Elève	NOM	STEPHANE SEIGNEUR
	STATUT	Stagiaire de la formation professionnelle

Cursus	BTS	Brevet de Technicien Supérieur
	SIO	Services Informatiques aux Organisations
	OPTION (A) SISR	Solutions d'Infrastructure, Systèmes et Réseaux

Phase	PPE	Projet Personnalisé Encadré en lien avec mon rapport de stage

---

Lieu de formation	ETABLISSEMENT	EPNAK ESRP ROUBAIX
	Adresse postale	35 rue du Général Sarrail - 59056 ROUBAIX
	Site internet	https://formation.epnak.org/roubaix/
	Téléphone	03 20 73 76 67
	Courriel	contact@crp-roubaix.epnak.org
	Fax	03 20 73 68 60

Lieu de stage donnant base de PPE	ETABLISSEMENT	Communauté de Communes CDC - Campagne de Caux
	Adresse postale	52, impasse du Lin, Rte de Bolbec, 76110 GODERVILLE
	Site internet	www.campagne-de-caux.fr
	Téléphone	02 35 29 65 85
	Courriel	accueil@campagne-de-caux.fr
	Fax	02 35 29 06 06

Sommaire

Auteur du rapport et son cadre d'exercice

Le présent document a été élaboré :

- par Monsieur Stéphane SEIGNEUR, stagiaire de la formation professionnelle
- dans le cursus préparatoire au diplôme de Technicien Supérieur référencé BTS SIO option SISR
- dans le cadre de son passage en entreprise rattaché aux exigences de sa formation diplômante
- sur une période réglementaire de stage de 12 semaines répartie en 2 fois 6 semaines
- sur des séquences de travail et des temps personnels au long des apprentissages de formation.

Remerciements

Je souhaite dès ce moment, adresser mes remerciements en direction des différents acteurs que j'ai eu à rencontrer tout au long de cette expérience professionnelle de formation.

Je tiens à remercier toutes les personnes, et elles sont nombreuses, qui ont contribué au succès de mon stage. Je ne peux être exhaustif, mais ils se reconnaitront sans le moindre doute.

Dans un premier temps, je profite immédiatement, en cette étape post-contextualisation de mon **rapport de stage et Projet Personnalisé Encadré**, pour remercier très vivement les primo-acteurs.

Sur site / en entreprise :

- Madame la DGS de la CDC, Madame Sandrine MIUS, Directrice Générale des Services qui a tout de suite compris mon action, l'intérêt de celle-ci et de ma présence et m'a adressé une très grande confiance et une marge d'action ciblée, mais très ouverte et libre, tout au long de mon passage dans l'établissement. Madame MIUS m'a confié les clefs du SISR à un degré important de confidentialité, de sécurité, d'intervention et de retour vers elle et l'entité. Sous son contrôle, je me suis immergé pleinement dans mon rôle d'administrateur systèmes et réseaux au niveau d'une direction technique adjointe, en fusion complète avec mon cursus de formation professionnelle. J'en retire une expérience valorisante, constructive, dans les domaines d'action et de connaissance applicables sur le terrain. Merci Madame.

- mes confrères de la société MSI2000, entreprise basée à Saint-Étienne-du-Rouvray (76 - Seine Maritime - Normandie, France), entité dont le cœur de métier et réside en l'administration et de services informatiques aux organisations, le conseil en solutions et réseaux informatiques, en développement de logiciels personnalisés et en externalisation.

  J'appui tout particulièrement mon salut, vers Messieurs :

  - Sylvain Fahy & David Rodriguez (Administrateurs systèmes et réseaux)
  - Régis Viger (Responsable Technique)
  - Plinio Piazza (Directeur)

  pour leur accueil, leur écoute et patience, leur qualité d'interaction avec moi, leur exactitude de réponse et leur bienveillance et pour m'avoir pleinement intégré professionnellement à leurs côtés. En coordination directe avec mes confrères, j'ai eu la possibilité de questionner, de participer, d'intervenir logiquement et physiquement sur les matériels et solutions, en interaction directe avec la réalité de terrains de mon entité d'accueil, la CDC. Enfin, plus largement, merci à toute l'équipe MSI2000.

En centre de formation :

J'adresse mes remerciements à mes formateurs et professeurs ainsi qu'à l'ensemble de l'équipe de suivi pluridisciplinaire présent tout au long des deux années d'étude et de formation au CRP de ROUBAIX.

- Je remercie vivement également Monsieur Ouadie Nejmi, mon formateur principal voué au domaine de la cybersécurité et des apprentissages informatiques généraux, pour son soutien, son écoute, son support logique et technique qui m'a servi de bagages et de références essentielles tout au long de ma formation et de mes périodes en entreprise.

- Je remercie également Monsieur Nicolas Maton, mon formateur en Infrastructure Réseaux et Administration des Systèmes dont l'intervention fut très importante au cours de mes apprentissages de seconde année.

- Je remercie chaleureusement l'équipe de suivi pluridisciplinaire et tout particulièrement Monsieur Pascal SAWARYN, professeur d'Algorithmie & de Mathématiques appliquées à l'informatique, qui fut mon référent de parcours à qui je dois un suivi permanent ainsi que Madame Méline BOUTOURY pour son haut degré de compétence, de compréhension et précision de réponse, avec un salut fraternel vers ses collègue Julie RODRIGUES et Justine KONIECZNY.

Leur suivi et leurs conseils m'ont permis de structurer mon parcours, de préciser mon action, de réaliser ma formation dans ce cheminement de deux années intenses en le NORD et la NORMANDIE, entre centre de formation et entreprise.

Dans un second temps, plus général mais tout aussi important, mes remerciements vont à l'ensembles des acteurs liés à mon environnement de travail au sein de ma structure d'accueil, à savoir :

- l'ensemble des élus du bureau exécutif de l'établissement public, avec une attention particulière vers Monsieur Franck Rémond, président de la communauté de communes Campagne de Caux (en exercice au moment de mes passages), Monsieur David FLEURY, 3eme Vice-Président, maire de la commune de Bornambusc pour leur accueil, les échanges, questionnements, l'écoute et la compréhension, sur des sujets techniques et technico-règlementaires dans un cadre technico-juridique complexe et une situation extrêmement complexe de restructuration de l'entité. Merci pour votre confiance concernant mon action, mes propositions et la compréhension de l'importance des systèmes d'information et systèmes réseaux au sein de l'EPCI, me permettant d'agir professionnellement au sein de la structure.

- Je remercie Madame Angélique GADONNA, assistante de direction administrative en interaction avec les pôles situés sur le site dit du « DOJO », qui fut un véritable éclairage, « mon projecteur longue portée » dans des moments d'investigations techniques et humains servant à établir les rôles, les actions, et bons nombres d'autres facteurs d'ingénierie sociale, moments très importants associés à la compréhension, à la gestion et bonne tenue et pratiques du et sur le SISR de la ComCom.

- Je remercie Madame Adeline GODEFROY, assistante de direction & de gestion administrative, notre charmante rédactrice territoriale aux multiples compétences…

- Je remercie Madame Audrey ESTIVAL, notre Directrice Générale Adjointe (DGA) en charge du Pôle Environnement… (votre sourire avant mon départ fut une belle récompense…)

- l'équipe communication et évènementiel, Madame Julie LIVER-CARLES, responsable de service et assistante du président de la ComCom, Madame Océane LE GOFF, assistante de communication

- L'équipe Finances, Mesdames Djamela SLIMANI, responsable financière (pour sa grande compréhension, son écoute et sa bienveillance) et Anne-Lise TALBOT, assistante

- le pôle Ressources Humaines, madame Angélique PIERRE, responsable RH, pour son aide, son humour, les échanges techniques liés entre nos deux domaines et expériences

- Je remercie également l'ensemble des personnels techniques et administratifs pour leur accueil, leur esprit d'équipe et en particulier Mesdames Éloïse LECANU, Béatrice GUÉRARD, technicienne Rudologie et SPANC ainsi Lydie DELALONDE, secrétaire de pôle, qui m'ont beaucoup aidé à comprendre les problématiques liées au fonctionnement de la structure et à comprendre le fameux « qui fait quoi et où ?»

Je ne peux vous citer tous, mais pêlemêle, un grand merci à :

- l'équipe « Voirie et Travaux » et « Environnement » en les personnes de Messieurs Didier LACHÈVRE, Didier PITTE (bonne retraite !), Marc DUVAL, Jean DEHORS, Wesley TOUROUL, Mickaël CANTREL et de leur responsable Monsieur Claude LEMERAY (toujours sur le terrain auprès de ses effectifs), Monsieur Daniel BOUBERT, Directeur Technique Adjoint, mon référent de stage sur place, durant ma première période de stage (relai fut pris par madame MIUS), Nicolas RICHOMME, responsable travaux, Julien GOUVAZÉ, responsable Cycle de l'Eau, Jean-Baptiste LEROUX, animateur Cycle de l'Eau

- l'équipe « Rudologie et Déchetterie » en les personnes de Madame Anastasia VATINEL & Messieurs Patrick LORCHER, Vincent ARGENTIN responsable d'équipe déchetterie, Madame Sandrine SAILLARD du service REOM, et Monsieur David VARIN en qualité de responsable du Service Déchets

- à notre réception, Madame Anne-Sophie HANIN, agent d'Accueil et Secrétaire… spécialiste de la méthode «en douceur et bonjour avant tout…»

- l'équipe Urbanisme, monsieur Pascal CHENEAU, Responsable Chargé de mission au côté de mesdames Lise BREDEL et Anne-Claire FRESNEAU, instructrices en urbanisme et Ludivine FLEURY, assistante

- l'équipe dite CIAS, Mesdames Christine MARTINEZ, Responsable Résidence La Chênaie et Caroline MAUTALENT sa collaboratrice

- l'équipe EFS (Etablissement France Services) Mesdames Séverine DESHAYES, responsable et Claire CLAEREBOUDT, Conseillère EFS, Marie BERTIN animatrice et conseillère Culture / Tourisme

- l'équipe Animatrice RAM / LAEP / Piscine / Entretien des locaux, Mesdames Valérie LE HÉRISSÉ, Coordinatrice Petite Enfance, Anna EZEQUEL, Armelle BAUDOUIN Animatrice, Stéphanie FAUVEL & Laëticia EBRAN, agentes polyvalentes

Projet Personnalisé Encadré (PPE) / Cadre de réalisation

Inscrit dans mon cursus de formation, le projet personnalisé encadré (PPE) est une modalité d'enseignement et de formation possédant une cohérence thématique ancrée dans la pratique professionnelle.

En tant qu'élève, le PPE prévoit que je sois amené à y assumer des fonctions de la maîtrise d'ouvrage ou de chefs de projet dans leurs relations d'encadrement[1].

Contextualisation de mon PPE / du projet : Idée directrice de mon action - Précautions et avertissements concernant l'utilisation du présent document

L'idée directrice de ce document consiste à poser une première image de la situation existante du SISR au sein de la CDC, d'en relever les principaux points fort et faibles[2], pour en tirer les principaux enseignements permettant d'en définir les principales mesures correctrices et actions d'amélioration, à prendre et mettre en œuvre, avec en parallèle l'idée de donner des éléments permettant de faciliter l'harmonisation de la méthodologie d'usage du système d'information et de son infrastructure.

Mon objectif premier consiste :
- à réponse aux exigences imposées par les impératifs de formation
- à réaliser un projet théorique inscrit dans mon cursus de formation au plus proche du réel

En réponse à cet énoncé, j'ai fait le choix d'aborder mon PPE sur les bases d'un contexte existant et inspiré de situations factuellement vécues en entreprise. Ainsi orientée, l'expression de mon exercice est en mesure d'être utile et propre à être mise en œuvre dans un but de sauvegarde, de développement, de sécurisation et de pérennisation du Système d'Information et du Système Réseau de l'entité concernée, environnement réel d'apprentissage ou j'ai évolué de manière effective.

Par extension, mon travail consiste en ce que ce projet puisse être utile à l'amélioration de la situation de départ au moment de son relevé s'il devait être mis en œuvre concrètement. **Ainsi, ce document a pour objectif associé, de fournir une aide** à l'entité et à ses décideurs afin qu'ils identifient les points utiles pour créer les conditions de bases minimales, les conditions de départ incontournables, lui permettant de tendre à respecter les obligations règlementaires et législatives liées à son statut et à ses domaines d'activité, ce qui lui permettra, ensuite, de vivre et d'évoluer de façon pérenne par un suivi sérieux à partir de cette base.

Ce rapport ne peut pas être exhaustif. Mon travail à la participation de l'audit est le fruit de plusieurs semaines de travaux individuels et collaboratifs sur place au sein de la structure, de rencontre, d'échanges, d'investigation, de synthèse et de rédactions.

Pour qu'il soit exhaustif, il faudrait un temps d'exécution beaucoup plus long, sans interruption, avec une équipe à minima en binôme, dédiée spécifiquement à la problématique autour de moyens d'investigation plus avancés.

Il est évident qu'un tel travail, un début d'audit, et à fortiori une action complète, nécessitent des moyens humains et techniques plus poussés que je n'en puisse disposer durant une période de 2 fois 6 semaines de stage réglementaire et dans les difficultés temporaires actuelles de la structure pour finaliser et rendre exhaustif.

Par **mon action ponctuelle, je souhaite établir les éléments utiles d'un prime audit non exhaustif,** du Système d'Information et Système Réseau présent, permettant à l'établissement de reprendre en main

son SISR, qui **permet à l'établissement de disposer des bases de compréhension** constitutives des **premières actions indispensables à mener, sur le principe simple du 3QPOCC autrement appelé QQOQCCP (Qui, Quoi, Où, Quand, Combien, Comment, Pourquoi)**.

Précisions concernant le cadre législatif, technique, technico réglementaire, et les facteurs, sur lesquels s'appuie la compréhension de ce document en sa technicité et sa légitimité

L'attention du lecteur est appelée sur le fait que, même une fois devenu définitif, le présent document ne pourra en aucun cas être considéré comme le seul référentiel à la lumière duquel les auditeurs, les intervenants futurs, les décideurs, la direction et directions adjointes, auront à former leur opinion globale et porter leur jugement professionnel dans le domaine considéré. Toutefois, il sera utile de lui prêter crédit et intérêt. Il s'agit de bien saisir qu'en terme de SISR, l'entité doit impérativement commencer un travail et une évolution technique, organisationnelle, budgétaire et humaine de fond, de longue haleine, nécessitant des compétences et des qualifications en interne aussi bien que l'appel de compétences et qualifications en externe.

Il ne s'agit pas d'un choix de bon vouloir, il s'agit de besoins réels sur la base d'obligations légales[3]. **Mon document ne juge pas. Mon document ne critique pas. Il porte aux lecteurs un regard objectif.** Il met en évidence des faits constatés lors d'actions concrètes. Il a pour but d'**aider ma structure d'accueil, l'EPIC CDC, et ses acteurs, à progresser. La volonté clairement affichée est d'aider le collectif, ses intervenants et son action en leur « prêtant main forte » vers l'amélioration.** Il n'est pas rédigé pour faire comprendre autre chose que ce qu'il contient.

En termes de réalisation, l'essentiel de ce travail d'audit relatif au système d'information et système réseau de la ComCom CDC, nécessite une connaissance et une formation a minima professionnelle en informatique ainsi qu'une maîtrise minimale des pratiques d'audit. **Dans sa lecture, ce document s'adresse à la fois à un auditoire dit « non-avertis » et à des intervenants dits « avertis / sachants ».**

Ce document n'a pas vocation à être rendu public et se doit de conserver un certain caractère de **discrétion et de confidentialité dans sa diffusion.** Il peut donc « circuler » mais en prenant la précaution qu'il soit transmis avec discernement et pondération à des personnes dument identifiées et en lien avec son objet. C'est un document d'étude préparé dans le cadre d'un exercice professionnel lié à ma formation.

Fort de ces précisions, la lecture ce document s'adresse plus précisément :
- à mes formateurs et enseignants, à mon centre de formation, à l'académie et autorités examinatrices
- aux instances et personnes en relation avec la préparation et la délivrance du diplôme que je vise
- les élus de la Communauté de Communes Campagne de Caux en ce qui est de son bureau directeur
- les personnels habilités de et par la ComCom Campagne De Caux (EPCI CDC)
- des intervenants internes ou externes habilités et désignés par la ComCom

Il est important de prendre en considération l'importance de ce document et des pièces qui y sont jointes, d'y prêter une écoute ouverte avec la volonté de s'y intéresser**, d'en comprendre le sens positif,** au service du SISR de la ComCom, des utilisateurs et acteurs, qu'ils soient directs et indirects.

Dans son exploitation il en va de même. L'important réside dans le fait que ce document serve de point de départ et d'aide aux personnes comprenant l'intérêt légal, règlementaire, juridique, stratégique, sociétal et économique de son propos ainsi que d'aide aux lecteurs dans la **compréhension que, le et les sujets qui y sont traités, relèvent des niveaux législatifs et règlementaires et par conséquent portent à responsabilités techniques et pénales de l'établissement et de ses représentants.**

Contexte général du projet en termes de structure d'accueil

Par définition, un contexte se détermine par l'assemblage de multiples facteurs, données, éléments, plus ou moins liés, dont l'agrégation crée un ensemble des circonstances appelé «une situation» au sein de laquelle se produisent « des faits ».

En cela, le contexte général du projet en termes de structure d'accueil se définit en ce que l'entité concernée dispose de ses propres infrastructures d'hébergement (en termes de locaux), de ses propres personnels et matériels et qu'elle inclut en son sein un ensemble de moyens définissant son propre Système d'Information (S.I) et sa propre infrastructure réseau autrement appelée Système Réseau (S.R), d'où l'abréviation « S.I.S.R », le tout nommé « SISR » en ce document.

Ciblage / bornage du présent rapport

Dans ce document, sont seuls concernés, le Système d'Information et le Système Réseau, l'infrastructure et les équipements constitutifs propres à l'entité dite « EPCI Communauté de Commune Campagne de Caux ». Il n'en débordera pas afin de réaliser un travail ciblé.

Exposition de l'entité servant de base contextuelle à ce projet

Communauté de Communes Campagne de Caux 52, impasse du Lin, Route de Bolbec - Zone d'activités 76110 GODERVILLE	
Tél : 02 35 29 65 85 Fax : 02 35 29 06 06	Courriel : accueil@campagne-de-caux.fr Site internet : www.campagne-de-caux.fr

L'entité que j'ai choisi pour ce projet est la Communauté de Communes Campagne de Caux.
Il s'agit d'une administration publique fondée en 1997 pour répondre à des besoins de mutualisation de moyens humains et techniques mais également pour répondre aux impératifs règlementaires et législatifs.

Toutefois, si la structure est une entité de sein publique, elle n'est toutefois pas une collectivité territoriale. C'est un E.P.C.I : un Etablissement Public de Coopération Intercommunale.

Ainsi, par son statut d'E.P.C.I, la communauté de Commune Campagne de Caux, obéit au principe de spécialité, c'est-à-dire que, à la différence d'une collectivité territoriale qui assume un rôle et des missions de plein droit par ses attributions législatives et règlementaires, un « E.P.C.I » est une entité morale qui ne dispose pas d'une vocation générale au sens «global » du terme, sur son territoire.

Sa vocation est d'être une structure de coopération et de mutualisation des moyens techniques et des compétences humaines mais pas une structure de fusion, de remplacement, de subrogation ou d'absorption des communes en une supra-entité.

En ce PPE, l'E.P.C.I, la communauté de Commune Campagne de Caux, sera dès lors, nommée dans ce document « La CDC ».

Contextualisation réglementaire et législative

Ma rédaction, mon action, ce document, se basent sur les principes et préconisations des principales entités vouées au domaine des SISR (Systèmes d'informations et Systèmes Réseaux) dans le cadre d'un exercice pratique vers l'activité professionnelle d'administrateur SISR. Mon exercice s'appuie sur les domaines législatifs et règlementaires français et européens.

D'un point de vue national

En termes de références françaises, de façon non exhaustive, nous pouvons citer :

- L'**A.N.S.S.I**, l'Agence Nationale de la Sécurité des Systèmes d'Information, qui est un service à compétence nationale, rattachée au Secrétaire Général de la Défense et de la Sécurité Nationale (**S.G.D.S.N**) qui assiste le Premier ministre dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale.
Documents de références :

> - *ANSSI Collectivités - Guide - Sécurité numérique des collectivités territoriales*
> --> *https://www.ssi.gouv.fr/uploads/2020/01/anssi-guide-securite_numerique_collectivites_territoriales-reglementation1.pdf*
>
> - Les collectivités face aux enjeux de cybersécurité dans le cadre juridique applicable
> --> https://www.ssi.gouv.fr/uploads/2020/01/anssi-infographie-les_collectivites_face_aux_enjeux_de_cybersecurite.pdf

- La **C.N.I.L**, la Commission Nationale de l'Informatique et des Libertés, entité créée par la loi Informatique et Libertés du 6 janvier 1978, chargée de veiller à la protection des données personnelles contenues dans les fichiers et traitements informatiques ou papiers, aussi bien publics que privés, chargée de veiller à ce que l'informatique soit au service du citoyen et qu'elle ne porte atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques. La CNIL est une autorité administrative indépendante (AAI) organisme public qui agit au nom de l'Etat, sans être placé sous l'autorité du gouvernement ou d'un ministre. Elle joue un rôle d'alerte, de conseil et d'information vers tous les publics et dispose d'un pouvoir de contrôle et de sanction.

- le **C.H.A.I.E**, Comité Interministériel chargé de coordonner, de soutenir et de suivre le développement de l'Audit Interne dans l'administration de l'État. Le CHAIE a été créé dans le cadre de la réforme de l'audit interne de l'État, prévue par le décret n° 2011-775 du 28 juin 2011, visant à généraliser l'audit interne à l'ensemble des fonctions et métiers des ministères et par ruissellement vers les administrations et structures rattachées qui en dépendent et y sont rattachées de façon directe ou indirecte.

Mon travail s'appuie également sur la **« loi pour une République numérique »** promulguée le 7 octobre 2016, (LOI n° 2016-1321 du 7 octobre 2016 pour une République numérique) loi dont l'objectif est de préparer la France aux enjeux des évolution techniques, technologiques liés à transition numérique et préparer le pays à l'évolution de son économie à venir. Cette loi, je cite : « promeut l'innovation, le développement de l'économie numérique, une société numérique ouverte, fiable et protectrice des droits des citoyens. Elle vise également à garantir l'accès de tous, dans tous les territoires, aux opportunités liées au numérique. »

D'un point de vue supra-territorial et extraterritorial

Ce prime audit s'appuie également sur les domaines législatifs et règlementaires européens
Simultanément aux multiples contextes technico-législatifs et technologiques nationaux, il est important d'intégrer à la démarche les échelons supra-territoriaux.

Le règlement général sur la protection des données (RGPD)
Le contexte continental européen est donc un des éléments à prendre en compte en se basant sur les principes et préconisations du RGPD, acronyme et sigle du Règlement Général sur la Protection des Données (en anglais « GDPR - General Data Protection Regulation »). Le RGPD encadre le traitement des données personnelles sur le territoire de l'Union Européenne.

Le RGPD est entré en application le 25 mai 2018. Il harmonise les règles et les pratiques européennes, applicables en matière de protection des données à caractère personnel. Il concerne les entités publiques ou privées, établies dans l'UE ou touchant des personnes dans l'UE. Toute structure, quelle qu'elle soit, de toutes taille, privée ou publique, administration ou collectivité, qui traite des données à caractère personnel est concernée sans exception. Tout organisme quelle que soit sa taille, son pays d'implantation et son activité, peut être concerné. En effet, le RGPD s'applique à toute organisation, publique et privée, qui traite des données personnelles pour son compte ou non, dès lors :
- qu'elle est établie sur le territoire de l'Union Européenne,
- ou que son activité cible directement des résidents européens.

A titre d'exemple :
- une entité, une administration, une société public ou privée, un prestataire de service, quel que soit son statut, du moment où elle est établie en France ou sur le sol européen, qui exporte l'ensemble ou partiellement ses actions, ses productions, ses services au Maroc, en Chine, ou toute autre localisation, pour et vers ses clients, fournisseurs, intervenants, aux Moyen-Orientaux, en Océanie, sur le continent américain ou autre, doit respecter le RGPD.
- de même, une entité, société, administration établie en Chine, proposant un site de service, d'hébergement, de e-commerce, etc… en français ou dans une langue européenne au sein de l'union, ou sur le sol français, ou sur le sol européen dans un autre pays membre de l'Union Européenne, livrant des produits et/ou services en France ou sur tout autre territoire de l'Union, doit respecter le RGPD pour agir légalement et protéger les données et les citoyens membres de l'Union Européenne.
- Le RGPD concerne aussi les sous-traitants qui traitent des données personnelles pour le compte d'autres organismes. Ainsi, si vous traitez ou collectez des données pour le compte d'une autre entité (entreprise, collectivité, association), vous avez des obligations spécifiques pour garantir la protection des données qui vous sont confiées.

TEXTES OFFICIELS via la CNIL : --> *https://www.cnil.fr/fr/reglement-europeen-protection-donnees*

En parallèle, adoptée par les institutions européennes le 6 juillet 2016, mon exercice tend à s'appuyer sur « **La directive Network and Information Security » (NIS)** datée de Juillet 2016, dont le texte garantit la protection des services essentiels au sein de l'Union Européenne par la définition d'un objectif majeur : assurer un niveau de sécurité élevé et commun pour les réseaux et les systèmes d'information de l'Union Européenne, le SISR de la ComCom Campagne de Caux se situant sur le territoire européen et dans son périmètre juridique, l'entité est partie prenante.

DIRECTIVE (UE) 2016/1148 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, texte adopté et decreté par le Parlement Europeen et le conseil de l'union européenne. Document et textes de références : --> *https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016L1148&from=EN*

Le système d'information et système réseaux (SISR) de la communauté de Commune Campagne de Caux face aux responsabilités juridiques

Statutairement, la ComCom CDC est un EPCI, un établissement public de coopération intercommunale, dont le statut définit qu'il est **une personne morale de droit public** qui est créée par l'Etat et qui tire son pouvoir de l'acte juridique de délégation de compétences par les communes-membres qui le composent. En droit, cette personne morale est une entité dotée de la personnalité juridique, ce qui lui permet d'être directement titulaire de droits et d'obligations en lieu et place des personnes physiques ou morales qui la composent ou qui l'ont créée. L'EPCI Campagne de Caux a donc les compétences qui lui sont déléguées et transmises. Il exerce les compétences en tant que personne morale, entité morale par délégation.

Au titre de la Loi Informatique et Libertés et du RGPD en application le 25 mai 2018, l'EPCI CDC, est concerné au premier chef, en tant que propriétaire de données, qu'elles soient créées, reçues, collectées ou stockées, de quelque nature qu'elles soient et d'autant plus qu'elles concernent des données dites à caractères privés. A titre d'exemple, la ComCom CDC reçoit, traite, transmet et stocke des renseignements fiscaux, territoriaux, d'urbanisme, d'identité, contenant des informations et données à caractère personnel, privé, confidentiel, etc… la liste est longue…

Dans tous les cas, au terme des lois et règlementations en vigueur, l'EPCI est propriétaire et demeure responsable des usages, du traitement, du stockage, de la sécurité, de la confidentialité, de la pérennité, de l'intégrité, de l'authenticité, des dites données, même s'il en délègue partiellement ou entièrement l'administration, le stockage, l'hébergement, le transit, la communication à un tiers. Si ses missions sont confiées à un tier, le propriétaire ne se voit en rien affranchi de ses responsabilités juridiques et pénales.

En termes d'exploitation et d'usage des Systèmes d'Information et Systèmes Réseaux, les maires et les présidents d'établissements publics de coopération intercommunale sont responsables des traitements informatiques et de la sécurité des données personnelles qu'ils contiennent. Ils peuvent ainsi voir leur responsabilité, notamment pénale, engagée en cas de non-respect des dispositions de la loi.

Je cite la CNIL : - « Les informations que les collectivités traitent informatiquement pour remplir leurs missions de service public, qu'elles agissent comme représentantes de l'État ou comme entités locales, doivent être protégées parce qu'elles relèvent de la vie privée et parce que leur divulgation est susceptible de porter atteinte aux droits et libertés des personnes concernées. La Loi Informatique et Libertés, créée en 1978 et modifiée en 2004 par la Loi n°2004-801 du 6 août 2004 - art. 4 (publiée au) JORF 7 août 2004, concerne l'ensemble des traitements automatisés de données personnelles, stipule un certain nombre de droits pour les personnes dont les données personnelles ont été recueillies, dont l'obligation d'informer les individus concernés de la collecte de leurs données, liée au droit à l'accès, la modification et la suppression des données en question. Y sont définis les principes à respecter lors de la collecte, du traitement et de la conservation de ces données. La loi prévoit également que le respect, par les collectivités locales, des règles de protection des données à caractère personnel est un facteur de transparence et de confiance à l'égard des usagers. C'est aussi un gage de sécurité juridique pour les élus qui, responsables des fichiers mis en œuvre, doivent veiller à ce que la finalité de chaque traitement informatique et les éventuelles transmissions d'informations soient clairement définies, les dispositifs de sécurité informatique précisément déterminée et les mesures d'information des administrés appliquées. »

Pour préciser, l'établissement public est, de plein droit et de plein exercice, dans sa responsabilité et sa charge face au traitement, à la collecte, au stockage, à l'exploitation, à la sécurisation, à la confidentialité, des données dont elle a la charge et l'usage, et qu'il en est de même face à l'usage, à la sécurisation, la confidentialisation de son SISIR.

Le système d'information (SI) et système réseaux (SR) de la CDC doit s'appuyer sur quels objectifs de base ?

Dans le cadre de son évolution et de ses responsabilités en matière d'usages numériques, de Systèmes d'Informations et Systèmes Réseaux, L'EPCI Campagne de Caux doit s'inscrire dans les objectifs visant à **tendre vers la sécurité informatique dont les cinq principaux objectifs de base** sont les suivants :

1 - Disponibilité

- La disponibilité au sens où elle doit permettre de maintenir le bon fonctionnement du système d'information et garantir l'accès à un service et/ou à des ressources.

2 - Intégrité

- 2.1 - Intégrité du système qui est le prime support à l'intégrité des données

L'intégrité d'un système est la prime condition et le prime support à l'intégrité des données qu'il collecte, reçoit, traite et conserve. Il consiste à définir et mettre en œuvre les moyens physiques et logiques, garantissant un principe selon lequel un système informatique est protégé de la façon la plus sûre et stable contre les dysfonctionnements, les agressions et les attaques et en garantissant que le traitement effectué par le système d'information et système réseau soit complet, exact, rapide et autorisé.

- 2.2 - Intégrité des données

Elle permet de vérifier l'exactitude, l'exhaustivité et la cohérence globales des données, vérifier si les données n'ont pas été altérées durant la communication que ce soit de manière imprévue, involontaire, ou intentionnelle, garantir que les données sont bien celles que l'on croit être. L'intégrité des données désigne également la sûreté des données concernant la conformité à la réglementation, par exemple la conformité au RGPD et la sécurité.

3 - Confidentialité

- La confidentialité consiste à rendre l'information inintelligible à d'autres personnes que les seuls acteurs de la transaction. Elle consiste à assurer que seules les personnes autorisées aient accès aux ressources échangées.

4 - Authentification

- L'authentification consiste à assurer l'identité d'un utilisateur, c'est-à-dire à garantir à chacun des correspondants que son partenaire est bien celui qu'il croit être. Un contrôle d'accès peut permettre (par exemple, par le moyen d'un mot de passe qui devra être crypté) l'accès à des ressources uniquement aux personnes autorisées. Consiste à assurer que seules les personnes autorisées aient accès aux ressources.

5 - Non-Répudiation

- La non-répudiation de l'information est la garantie qu'aucun des correspondants ne pourra nier la transmission, nier l'échange d'information, nier la transaction, etc…

Tous ces aspects doivent faire l'objet d'une **stratégie logique et physique mise en place par l'ensemble de l'entité, tant humainement, que techniquement et budgétairement sous la conduite d'une direction dédiée au SISR.**

La CDC doit prendre en compte une approche globale de son système d'information, infrastructure et système réseau (SISR) Stratégie logique et physique

La sécurité d'un système informatique est une chaîne ou chaque maillon est en relation avec d'autres maillons du SISR interne et des systèmes périphériques.

Dans l'objectif de la réalisation des points précédemment notés, l'établissement se doit de s'inscrire dans une démarche globale, fondée sur des actions courantes aussi bien que ponctuelles, mais également sur le long terme, la continuité et la pérennisation de ces actions, matériels et infrastructures.

Le niveau de sécurité d'un système est caractérisé par le niveau de sécurité du maillon le plus faible, le principe étant : - « Qui peut le plus peut le moins »,
mais « qui peut le moins ne peut pas nécessairement le plus »

- « en protégeant le plus faible, je protège de facto le plus fort »
ainsi, « en dimensionnant ma démarche pour sécuriser le point le plus faible, je sécurise de facto tous les points plus forts »

A titre d'exemple, sur un bâtiment, une maison, un local, une porte blindée est inutile si les fenêtres, les dispositifs d'évacuation d'urgence, les systèmes de ventilations, etc… de ce même bâtiment sont NON sécurisées, ouvertes sur la rue OU laissent en tout état de cause une possibilité d'accès à un/des potentiel(s) acteur(s) malveillant(s) ou malintentionné(s).

En abordant la sécurité du SISR dans un contexte global, il faut prendre en compte les aspects suivants, fonder sur **trois principales ressources** :

1 - Les facteurs humains et ressources humaines :

- Les facteurs humains, associés à la maitrise des outils, aux procédures techniques d'utilisation, à la sensibilisation des utilisateurs aux problèmes de sécurité, etc…

- Principales ressources de cet aspect : les ressources humaines, individuelles ou en équipe, dans des milliers de fonctions directes et indirectes tels que des administrateurs, des développeurs, des programmateurs, des web designers, des usagers, des créateurs, des cartographes, des géomètres, mais aussi des utilisateurs ou conducteurs de machines connectées, etc… une liste tellement immense qu'il est impossible d'être exhaustif à moins d'y consacrer tout son temps, tous ses moyens et toutes ses possibilités…

2 - La sécurité logique et les ressources immatérielles :

- La sécurité logique, c'est-à-dire la sécurité au niveau des données, la et les stratégies informatiques, les stratégies conceptuelles notamment dans la conservation et protections des données de l'établissement, les logiciels, les applications ou encore les systèmes d'exploitation, la conception ou l'appropriation de procédures, etc…

- Principales ressources de cet aspect : des ressources immatérielles, comme des brevets, des algorithmes, des formules, des graphismes, des assemblages d'idées, créés et exploités pour mettre en œuvre des services, des calculs, des créations, applications, des logiciels, des divertissements, des communications…

3 - La sécurité physique et les ressources matérielles

- **La sécurité physique,** c'est-à-dire la sécurité des matériels, la qualité des matériels et leurs qualités conceptuelles, au niveau des infrastructures matérielles : salles sécurisées, lieux ouverts au public, espaces communs de l'entreprise, postes de travail des personnels, etc…

- **Principales ressources de cet aspect : les ressources matérielles**

Des ordinateurs, des équipements, des ressources et des matériels internes ainsi que des périphériques, serveurs, caméras, satellites sont utilisés pour acquérir, stocker, acheminer les données cartographiques ;

Des matières, des matériaux, sont extrais, transformés, recyclés, inventés, découverts, etc… pour créer, fabriquer tous les éléments, équipements et pièces qui interviennent dans le fonctionnement et l'usage d'un SI…

La sécurité des télécommunications des SISR, regroupe l'ensemble de ces points sans exception, tous en interaction et interconnexion par la technologie réseau, les serveurs de l'entreprise, les réseaux d'accès, etc…

Contexte de situation du S.I.S.R de la CDC au départ du projet : situation relevée Moment zéro du projet

L'image de la situation que je choisis de fixer comme point de départ de mon PPE est la situation rencontrée au terme de mes périodes de stage en entreprise au sein de la CDC.

La source première de ce projet est fixée à l'issue de ma première période en entreprise.
Elle sera évolutive et complétée au terme de la seconde période effectuée.

Au moment de la réalisation de mon projet :

1 - Le SISR en lien avec les sites opérationnels de la CDC

Le SISR de la CDC concerne et se trouve répartie sur plusieurs sites, physiquement et géographiquement séparés et indépendants. Ces sites physiques sont répartis ainsi :

1.1 - Site unitaire :

1.1.1 - « le siège» en tant que site bâti du siège social de l'EPCI incluant les services généraux administratifs et le centre des services techniques au sein de la même infrastructure bâtie

1.1.1.1 - Ce site physique bâti est le lieu d'hébergement physique du serveur central du SISR de la CDC.

1.2 - Site adjacent au siège :

1.2.1 – « la déchetterie » site intercommunal de collecte des déchets, situé à proximité immédiate du siège. Peu informatisé, il est sous équipé et ceci uniquement par des matériels informatiques obsolètes.

1.3 - Sites dispersés géographiquement séparés :

1.3.1 - « le Dojo » en tant que site incluant un ensemble d'infrastructures bâties vouées à des activités et équipements sportifs :

1.3.1.1 – Le « pôle social » au sein du « Dojo », ensemble de bureaux avec un secrétariat d'accueil, lieux d'exercice des personnels en charge du pôle social de la CDC et des activités sportives et extra-scolaires locales.

1.3.2 - « l'Espace France Services » local d'accueil et d'information du public en lien avec les administrations territoriales, départementales, régionales et d'Etat.

2 - Statut descriptif et mode de gestion et d'administration du SISR, F.A.I et imbrication du F.A.I dans le SISR de la CDC

Le SISR de la CDC est géré par trois têtes de pilotage. La CDC a recours à :

2.1 - dans un premier temps, son propre personnel interne en la personne unique de son directeur général adjoint en charge du pôle action sociale, équipements et infrastructures.

Ce point révèle une vulnérabilité qui amplifie la fragilité du SISR de la CDC.

Il n'est pas normal, ni tenable dans le temps, qu'en interne, une personne seule, soit à la fois :

- directeur technique adjoint en charge du SISR, dédiée à l'administration et gestion et à un ensemble de tâches et responsabilités vouées au SISR de la CDC

- la personne dédié à des activités de directeur technique adjoint en charge du « pôle social »

- en charge du service « Infrastructure »

- en charge de la direction du S.I.G, Système d'Information Géographique

Il ne peut pas être raisonnable de laisser cette situation perdurer, dans une volonté de bon fonctionnement du SISR de la CDC, à son niveau actuel d'importance stratégique, croissant et vital. Cette situation entraîne des failles extrêmement importantes en termes de fonctionnement, de pérennité, de sécurité, de confidentialité du SISR et à terme, des risques majeurs sur ses données.

Le risque zéro n'existe pas et n'existera jamais, mais cette situation et cet état de faits, créent un terrain propice à augmenter les risques et à rencontrer de très grandes difficultés aux conséquences multiples et très dommageable tant techniquement, qu'économiquement et juridiquement.

Dans une telle situation, le personnel concerné ne peut que se diriger vers une situation de surcharge et de saturation morale, créant des situations propices à amplifier les risques de disfonctionnement du SISR.

Un SISR demande une hyper spécialisation et une concentration vouée à ce seul domaine regroupant à lui seul, un panel déjà important de champs opératoires.

Un SISR demande du temps, des moyens et de la concentration, les situations de surcharges par dispersion d'activités et de rôles et la non-spécialisation, y créent une situation globale détériorée qui, à terme, aboutissent toujours et par retour d'expérience à la mise en difficulté profonde de l'ensemble du système d'information.

Dans ces cas, les difficultés de fonctionnement et de gestion sont et seront croissantes et les conséquences d'erreurs possibles dues à des impondérable ou impossibilités temporelles, techniques, humaines, sur l'ensemble des tâches à réaliser trouveront des effets démultipliés à court, moyen et long terme.

Le SISR de l'établissement doit se doter d'une tête spécifique constituée d'une équipe spécifique et uniquement dédiée au SISR. La création d'une D.S.I (Direction des Systèmes d'Information) au

sein de la ComCom est une condition incontournable dans la mise en place d'une stratégie, d'une évolution, d'une protection efficace et d'un usage et d'une pérennisation sécurisée.

Une direction du SISR de la CDC doit être créée.

A ce niveau de développement et d'importance du SISR de la CDC, une administration spécifiquement dédiée, basées sur un service spécifiquement dédié doit être créée, allouée, planifiée et pérennisée pour un service dédié, spécialisé, structuré, budgétisé et souverain qui doit, par simple logique, voir le jour.

Il faut impérativement que la structure saisisse **l'importance stratégique de son SISR**, cet **outil que la CDC a créé par elle-même via le courage et l'engagement de ses différents acteurs par leurs actions au sein de l'entité**, en réponse aux multiples impératifs structuraux, techniques, budgétaires et sociétaux présents et à venir.

Cette direction aura la mission d'administrer, superviser et piloter la sécurité, la confidentialité, l'intégrité, la pérennisation et la disponibilité du SISR dans son entièreté.

Cette direction se doit d'être détachée de tout autre domaine. Elle doit être un service autonome d'administration du SISR uniquement vouée à sa seule mission à la tête du SISR.

Cette direction, doit être en prise directe avec les réalités de terrain dans ce qui fait la vie et l'usage du SISR et donc, par conséquent, doit avoir un droit de regard sur l'ensemble des activités et pratiques informatiques pour en connaître les usages, les besoins présents et à venir, les faiblesses techniques et d'usage, pour intervenir ponctuellement et périodiquement, pour assurer les actions de maintenance, d'administration et de gestion.

Elle devra avoir les autorisations et les possibilités d'intervenir de façon autonome et décisionnelle en tout point et tout moment au sein de l'établissement, de ses infrastructures et équipements et d'entrer en contact à distance ou physiquement avec ses agents et intervenants, utilisateurs ou acteur interne et externe du SISR.

L'ensemble de la mise en œuvre doit faire l'objet d'un projet global. Il doit inclure, entre autres aspects non exhaustifs, l'ensemble des facteurs tant humains que techniques, de sécurité, d'usage, de développement et de pérennisation à court, moyen et long terme du SISR de la ComCom.

Cette démarche se doit d'être continue et réalisée par cette direction mais en lien direct avec la DGS et l'ensemble des DGA, de façon neutre, objective, indépendante, hors contexte de la vie politique de l'établissement.

Le SISR et sa direction sont à considérer comme un outil majeur, socle de l'infrastructure et de l'ensemble des activités, dont l'objectif est d'assurer la stabilité , la continuité et la sécurité des moyens d'information de l'établissement en dehors de toute influence.

2.1.2 - Le SIG et le SISR au sein de la CDC : la confusion des professions et des rôles associés.

En effet, un autre point de difficulté dans la définition des intervenants réside en la confusion permanente entre le SIG et le SISR.

Face aux nombreuses difficultés, il est important de relever qu'une confusion de fonction et de profession est faite au sein de la CDC en ce qui concerne le SISR et le SIG.

Cette confusion est en partie due :

- à une croissance très rapide de l'EPCI
- à un manque d'information des décideurs n'ayant que peu de sources de renseignements et d'aides
- à la volonté louable mais inappropriée de contraction budgétaire face aux réalités de financement.

Un S.I.G, Système d'Information Géographique, est un système d'information conçu pour recueillir, stocker, traiter, analyser, gérer et présenter tous les types de données spatiales et géographiques de l'établissement. L'acronyme SIG est parfois utilisé pour définir les « Sciences de l'Information Géographique ». Un SIG est un outil numérique constitué de l'ensemble des outils des cartographes permettant le croisement et la superposition des données multidisciplinaires pour un tirer les informations utiles et les utiliser.

Pour faire simple :
- un S.I.S.R relève de l'intervention d'un administrateur informatique.
- un S.I.G relève de l'intervention d'un cartographe.
Les deux métiers, les deux professions, n'ont strictement RIEN A VOIR. Le seul point commun de ces deux domaines, c'est que le SIG est une évolution du métier de cartographe en ce qu'il s'est numérisé et donc permet au cartographe, la superposition et le recoupement des données d'activités diverses, mises en parallèle et en superposition avec les cartographies pour en comprendre encore plus les enjeux, mieux comprendre les réalités de terrains et mieux agir ou anticiper sur les actions à mener.
Au bilan :
- Un technicien S.I.G n'est pas un technicien SISR
- Un technicien SISR n'est pas un technicien S.I.G
- Un **informaticien** spécialisé en Système d'Information, Solutions d'Infrastructure, Systèmes et Réseaux n'est pas un **cartographe**, spécialiste des Systèmes d'Informations Géographiques

2.2 - en parallèle, une externalisation d'appuis, dans la gestion et l'administration

2.2.1 - Cette externalisation se concrétise par l'intervention, après réponse à appel d'offre, de l'entreprise MSI2000, pour deux aspects que sont :

2.2.1.1 - aspect premier : administration, support et intervention sur l'administration logique et physique du SISR de la CDC

2.2.1.1.1 - le support et l'intervention logique et physique concernant l'administration des système et réseaux internes et de pleine propriété à la CDC

2.2.1.1.2 - le support et l'intervention logique et physique concernant le maintien et la délivrance de services, la disponibilité, la sécurité, la sauvegarde et l'intégrité des systèmes et réseaux internes et de pleine propriété de la CDC

2.2.1.1.3 - avec un cadre d'intervention défini en amont de mission par appel d'offre nécessitant une réévaluation et une redéfinition profonde sur les bases des services réellement délivrés.

Il est à noter que le prestataire (MSI2000) va fréquemment au-delà de sa mission contractuelle par soucis et par forte conscience professionnelle et commerciale sans forcément que la CDC en soit pleinement consciente de ce fait.

Il est à noter que souvent, m'est revenu aux oreilles, le doute sur les compétences et la probité de notre prestataire de service. Ces critiques ne sont pas justifiées mais il faut comprendre qu'elles sont émises dans un contexte extrêmement difficile d'un point de vue technique et humain au sein de l'entité, situation vécue maintenant depuis une très longue période, entrainant une perte de repère des acteurs « utilisateurs » du SISR de la CDC sans pour autant qu'ils n'aient le niveau technique professionnel en la matière système et réseau adéquat pour juger de la qualité ou non de la prestation de nos prestataires actuels.

Je le redis, avec un regard et une démarche parfois très sévère de ma part, il est à noter la très bonne qualité de prestation délivrée au-delà des obligations contractuelles par la société MSI2000 et principalement face à la situation dégradée. De plus, je le répète, rien n'est parfait, la perfection n'existe et n'existera jamais. Le but est de tendre à l'amélioration et au développement sérieux, pragmatique, efficace, du SISR.

Les actions à mener sont extrêmement nombreuses et s'imposeront quoi qu'il arrive, quelques soient les modes et systèmes logiques et physiques et stratégies déterminées dans le temps et l'avenir du fonctionnement du SISR.

Le rythme des régies qui prévoient comme la CDC, 1 journée d'intervention tous les deux mois est clairement un frein à l'amélioration même lente de la situation du SISR ainsi qu'un risque extrêmement élevé de sécurité du système d'information.

Ce rythme et l'organisation actuelle sont inadaptés et imposent à tous que ce soit en interne et en externalisation via le tenant du marché, de ne gérer que les urgences et les demandes ponctuelles des utilisateurs.

Avant mon départ de fin de période en entreprise, fort de l'écoute de Madame la DGS et des prestataires eux-mêmes demandeurs de progression dans le sens que j'indique, la fréquence des interventions avec visites sur place a été actée à une fois tous les quinze jours, avec en alternance, une intervention à distance approfondie, une fois tous les quinze jours également. **Ceci est loin très loin d'être suffisant mais c'est un début de prise de conscience.**

2.2.1.2 - évolution de l'aspect premier : administration, support et intervention sur l'administration logique et physique du SISR de la CDC

Le seul aspect satisfaisant, actuellement existant, du SISR de la CDC est ce principe d'externalisation d'appuis avec un prestataire extérieur.

Il est à noter qu'il a été créé par « force de nécessité de survie du SISR », qui est en outre, le seul aspect répondant aux préconisations d'usage et de mise en fonction des autorités de tutelles que sont la CNIL et ANSSI.

Le principe réside dans le fait que la redondance de pilotage se doit d'être effective et assurée par un administrateur en interne et une entreprise d'administration de systèmes et réseaux externe.

Cette redondance par externalisation, est un point fort du SISR de la CDC.
Réglementairement et conformément aux recommandations nationales émises par CNIL, un SISR d'une collectivité locale, d'une entité administration, d'un service public, d'une entité intercommunale doit disposer d'une DOUBLE TETE d'administration, une direction et capacité d'administration et d'intervention en interne par des personnels en interne et son pendant en EXTERNE dans le but d'assurer la redondance sécuritaire, de supervision et de suivi logique, physique et procédural.

Ce point fort doit subir une évolution et une précision plus approfondies du rôle de l'intervenant externe en parallèle d'une véritable création de poste d'administration et de direction du SISR en interne, à temps plein et uniquement dédiée. **Actuellement, l'ensemble des points sont soit inexistants (administration en interne) soit insuffisants (administration externalisée).**

L'évolution de l'administration du SISR de la communauté de communes doit donc évoluer de la façon suivante :

- mise en place d'une administration en interne de plein temps, de plein droit et de pleine autorité sous la direction unique de la DGS (Direction Générale des Services) et détachée de toute autre donneur d'ordre.

- mise en place d'une administration externe de soutien et de redondance sous l'autorité exclusive de la direction d'administration interne du SISR et la DGS.

Afin de comprendre le dimensionnement utile de cette administration externe venue en soutien de l'administration interne, je préconise qu'elle se fasse à hauteur d'un volume d'activité égal à un mi-temps réparti sur des demi-journées dédiées.

Pourquoi ce choix ? Explication :
La durée légale du travail pour un temps complet est fixée à 35 heures par semaine, qui débute le lundi à 0 heure et se termine le dimanche à 24 heures, sauf si une convention ou un accord collectif d'entreprise ou d'établissement ou, à défaut, une convention ou un accord de branche, fixe une autre période de 7 jours consécutifs.
Ce qui définit 151,67 heures par mois et avec les congés, porte la somme à

1 607 heures par an (151.67x12 = 1820.04/ans - 30 jours ouvrables (5 **semaines**) portant à l'équivalent de 6.08 semaines de congés à 35h) mais dans notre cas nous parlons d'une prestation de service annuelle donc sur un temps de répartition annuel global hors salariat ou traitement d'agent et donc nous prendrons en compte 1820.04 h/ans pour un plein temps.

Explication de mon calcul :
--> Temps plein hebdomadaire = 35 heures/semaine
--> Temps plein mensuel = 151.67h/mois
[(Temps plein hebdo x 52 semaines)]/12 mois = [(35×52)]/12 =151.67/mois
--> Temps plein TECHNIQUE de disponibilité annuelle = 1820h/ans
Temps plein mensuel x 52 semaines par an = 151.67h×12= 1820h/an

Donc, pour notre besoin prospectif, je me base sur un volume d'heures tel que :
- un mi-temps annuel = (1820h/an)/2 = 910h/an
- un mi-temps mensuel = (1820h/an)/2/12 = 75.83h/mois
- un mi-temps hebdomadaire = (1820h/an)/2/52= 17.5h/semaines

Ainsi, le prestataire de service externe devrait être disponible et intervenir en parallèle de l'action de l'administration interne :
- sur un volume d'heure globalisé
- à hauteur de 910 heures par an
- reparti sur 75.83h par mois et 17.5heures par semaine

Ce volume d'heures devra bénéficier à la direction interne du SISR par la possibilité de modulation de cette répartition d'heures d'intervention en fonction des besoins pour regrouper les heures d'intervention en fonction des besoins réels prévisibles, des besoins planifiés et des besoins d'interventions imprévus et imprévisibles.
Ce volume d'heure et sa répartition entre temps planifiés et temps non-planifiés devra faire l'objet d'une évaluation et précision en interne pour être traduite au sein de l'appel d'offre mais en prenant soin de laisser la pleine maitrise de l'évolution de cette répartition aux services internes en faisant bien prendre en compte au prestataire de service qu'il s'agit d'une répartition évolutive et non définitive car adaptable plusieurs fois dans l'année en fonction des réalités et besoins planifiés ou non qui seront exposés ou rencontrés.

- Ce choix permettra de disposer d'une redondance et d'un appui technique, technologique, règlementaire, continu et efficient, dimensionné à la juste mesure des besoins de l'entité, permettant d'assurer une évolution, une continuité technique, une progression physique et logique du SISR et de son équipe dédiée.

- Ce dispositif permettra en outre de maîtriser le coût de la masse salariale engagée, permettant ainsi de disposer d'une continuité d'administration du système d'information et réseaux de la CDC en toutes circonstances y compris lors des périodes de vacances pour congés annuels, formation, évènement familial ou vacances pour événements graves comme la maladie ou un décès, une hospitalisation, etc.., concernant le ou les acteurs de la direction et de l'administration interne du SISR.

2.2.1.3 - aspect second : acquisition, délivrance, fourniture, intégration, mise en service, exploitation, pérennisation, historique, archivage, des solutions logiques et physiques des composants du SISR de pleine propriété de la CDC,
sur demande par commande ponctuelle.

A cette étape de son exploitation, le SISR de la CDC n'a pas le choix que de mettre en place, sur la durée, une planification matérielle et une planification logique, avec en face, une planification budgétaire.

A terme, matériellement et logiquement, sans réforme complète de fonctionnement, sans création d'une direction dédiée en interne, sans mise en place d'une stratégie adaptée, sans investissement dans des mises à jour physiques et logiques, sans réorientation et pérennisation des solutions composant le SISR de la CDC, le SISR finira par « tomber », c'est-à-dire, qu'il subira des pertes graves d'intégrité, de fonctionnement et de sécurité, ce qui entrainera la perte grave de données et de fonctionnalités et engagera la responsabilité de l'établissement.

Il existe plusieurs façons de planifier budgétairement le renouvellement, la pérennisation, l'entretien et la modernisation des systèmes d'information et réseaux. Il est souvent envisagé d'établir des plans quinquennaux.

Toutefois, je fais le choix, pour ce sujet d'une stratégie en 2 phases :

-**une phase d'amorce** pour permettre la remise à niveau primaire du SISR permettant de sortir de la situation actuelle par une action massive et unitaire de consolidation et remplacement des bases du système.

Par cette phase d'amorce, il s'agira de reprendre en main tout ce qui ne va pas. Il s'agira de remplacer tous les matériels obsolètes et de remplacer tous les matériels en fin de vie ou dégradés. Il s'agira également d'acquérir, de mettre en service les matériels et solutions indispensables pour sortir de la situation actuelle.

- puis d'évoquer **la mise en place d'une stratégie adaptée à court, moyen et long terme** soit en 3, 6 et 9 ans pour pérenniser et faire évoluer le SISR de la CDC. Cette stratégie de répartition permet de s'orienter vers un investissement plus doux car plus étalé et réparti, demandant un effort plus constant mais mieux planifiable créant un roulement, un renouvellement physique des matériels et des solutions logiques plus évolutif et serein.

C'est la technique dite des « petits pas réguliers ».
Effectués l'un après l'autre, chaque pas étant consolidé et consolidant l'étape et l'action suivante, le tout s'inscrit dans un cheminement doux et permanent et permet une intégration également douce et permanente des nouveaux éléments matériels, logiques et humains qu'ils soient constitutifs du SISR ou simples utilisateurs de celui-ci.

Il y a l'impératif de quitter le mode de fonctionnement actuel qui débouche involontairement sur une situation globale anarchique, dans un déroulé

saccadé, amenant à un ressentir brutal, pour diriger le SISR et ses acteurs vers une démarche d'intégration correcte et efficace.

Plutôt que de choisir la stratégie du coureur de vitesse qui court très vite mais s'arrêtera tout aussi vite et qui fournit un effort violent mais dont l'arrêt est tout aussi violent, un SISR voué à une collectivité est en quelque sorte un marathonien qui doit tenir sur la durée dans un effort continu.

Il n'est pas là pour épater la galerie, il est présent pour garantir une efficacité de disponibilité, de performance et de sécurité dans le temps ; il est un élément de stabilité des services et de l'infrastructure de l'état à son échelon dédié. Ce n'est pas un élément de compétition, c'est un élément de pérennisation.

Ce second aspect devra faire l'objet de multiples choix en interne et devra être intégré à la passation d'un marché vers des prestataires externes chargés de nous appuyer, de nous conseiller et de nous fournir sur les besoins matériels et logiques dont nous aurons le besoin avec un total pouvoir décisionnel de notre part.

Il faudra, en tout état de cause, que la CDC mette en place des sources d'approvisionnements logiques et physiques clairement identifiées, intégrées et disponibles, en lien avec nos contraintes règlementaires comme par exemple la loi n° 85-704 du 12 juillet 1985 relative à la maîtrise d'ouvrage publique et à ses rapports avec la maîtrise d'œuvre privée, dite loi MOP, fondue dans le code de la commande publique (CCP) et qui est une spécificité et souvent une difficultés car souvent inadaptée aux réalités de terrain.

Pour exemple, cette loi française qui met en place, pour les marchés publics, la relation entre maîtrise d'ouvrage et maîtrise d'œuvre, loi qui est propre aux établissements publiques comme la CDC, nécessite un temps de latence et une inertie parfois incompatible avec les difficultés du réel.

Pour pallier au mieux à cela tout en s'assurant du respect de la et des lois, il faut que l'entité sorte de sa situation actuelle où la moindre commande fait l'objet d'une difficulté systématique, lourde et floue, résultat de sa grande souffrance sur une très longue période et qui paradoxalement ne fait que la maintenir et l'enfoncer.

La CDC doit prendre le temps de mettre en place un système de commande qui ne soit plus « improvisé » par la mise en place, avec les services financiers, comptable et légaux, des moyens permettant de développer l'identification et l'automatisation des solutions permettant de s'approvisionner et acquérir les moyens matériels et logiques et d'en effectuer la commande au niveau le plus adapté.

Diverses solutions sont à étudier.

Par rapport au contexte actuel, il n'est pas normal que nous n'ayons pas mis en place un accord, une procédure clarifiée et le plus possible automatisée de commande des matériels informatiques en lien direct avec nos prestataires de service d'administration externalisé, actuellement la société MSI2000.

Nous devrions être en mesure de budgétiser, y compris prévisionnellement, par des « accords-cadres » les approvisionnements logiques et physiques de notre SISR.

Nous avons grand besoin de sécuriser, clarifier et identifier nos démarches et notre visibilité, en termes de fourniture de solutions logiques et matérielles par des prix identifiés, cadrés et dont la réactualisation est périodiquement planifiée pour des types et gammes de matériels donnés.

Cela peut également passer par des prestataires de service **complémentaires et/ou entrer dans la mission d'appuis et d'administration du prestataire externe** pour la mise en place d'un tel système.

Cette solution devrait permettre à l'établissement :

- de façon automatisée
- ergonomique et efficiente
- d'émettre une demande
- d'en préciser rapidement les critères et caractéristiques
- de s'intégrer à nos systèmes et services de suivi et vérification comptable
- d'en automatiser les procédures et l'édition
- d'en vérifier la bonne conformité face aux contraintes réglementaires, normatives et légales et d'en faire la bonne publicité
- nous donner la possibilité d'intégrer tous les fournisseurs potentiels, y compris des fournisseurs ou prestataires locaux et parfois très pacifiques, petits ou grands, jusqu'aux centrales d'achat.

L'établissement doit se structurer sur le long terme et automatiser ses processus pour sortir de lourdeurs et des difficultés actuelles qui encrassent la collectivité et ses personnels. La CDC doit identifier ses sources pour ne plus s'étouffer à chaque besoin.

2.3 - son prestataire F.A.I, fournisseur d'accès internet, seconde externalisation du SISR de la CDC

2.3.1 - la fourniture d'accès Internet est actuellement attribuée à la S.A. ORANGE pour les aspects suivants :

2.3.1.1 - la fourniture, mise en service et délivrance d'accès au réseau public général de télécommunication via abonnement professionnel dédié

2.3.1.2 - la fourniture, mise en service et délivrance des services téléphoniques, des standards de répartition et service VoIP associés (répartition, routage, sécurisation)
VoIP : Voice Over Internet Protocol, c'est-à-dire transmission de la voix par Internet. C'est une technologie qui permet la communication par la voix ou multimédia, vidéo ou flux audio, par le réseau Internet (IP).

2.3.1.3 - la liaison filaire, la répartition et le routage des liaisons de télécommunication physiques (liaison au format Ethernet RJ45) de l'ensemble des postes depuis les routeurs et switch en propriété d'ORANGE sur le serveur de pleine propriété de la CDC.

Cet aspect exprime une aberration technique plaçant l'ensemble de la CDC dans une situation d'ultra dépendance face à son F.A.I en termes de confidentialité, d'intégrité, de fonctionnement et de délivrance des services entrainant un risque prévisible d'effondrement de son SISR en cas de désengagement de la CDC vis-à-vis de son F.A.I., par exemple, suite à un appel d'offre pour étude et renouvellement du contrat de fourniture d'accès et des services associés.

2.3.2 - Liaison filaires externes dédiées à l'accès au réseau de télécommunication public

2.3.2.1 - F.A.I (Fournisseur d'Accès Internet) S.A ORANGE
Pour l'apport et la connexion au réseau de télécommunication externe public, la CDC a choisi la S.A ORANGE par un abonnement et un accès externe au réseau de télécommunication via une box professionnelle.

La S.A ORANGE est titulaire des missions héritées de la défunte entité « France Télécom » par attribution et délégation de mission de service public des missions d'entretien, de réparation et d'aménagement des réseaux publiques et communs d'Etat, mis à disposition des opérateurs de télécommunication et dont ORANGE perçoit les taxes, rétributions et redevances dédiées.

Ceci est une donnée importante à prendre en compte en ce qui concerne l'alimentation, l'apport des liaisons de télécommunication externe au niveau du NAT.

Toutefois, il est anormal que seule l'entité S.A ORANGE soit le F.A.I. exclusif de la CDC.

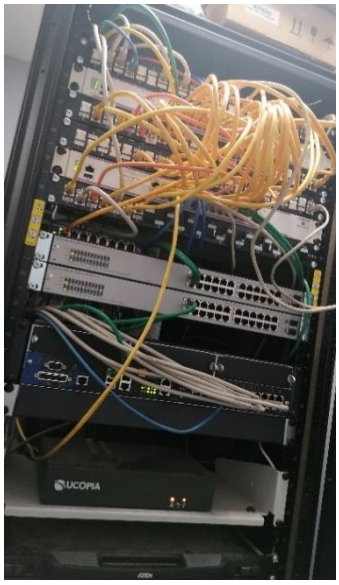
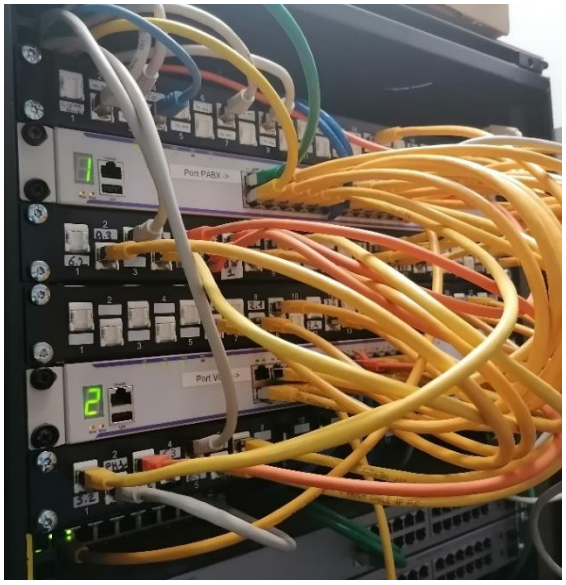
En termes de sécurité et de pérennité des liaisons de télécommunication, l'EPIC CDC se doit de se doter d'une double connexion au réseau public pour assurer une sécurisation par redondance de son SISR.

Il conviendra de déterminer le choix d'un second acteur FAI de la CDC en complément de la S.A. ORANGE.

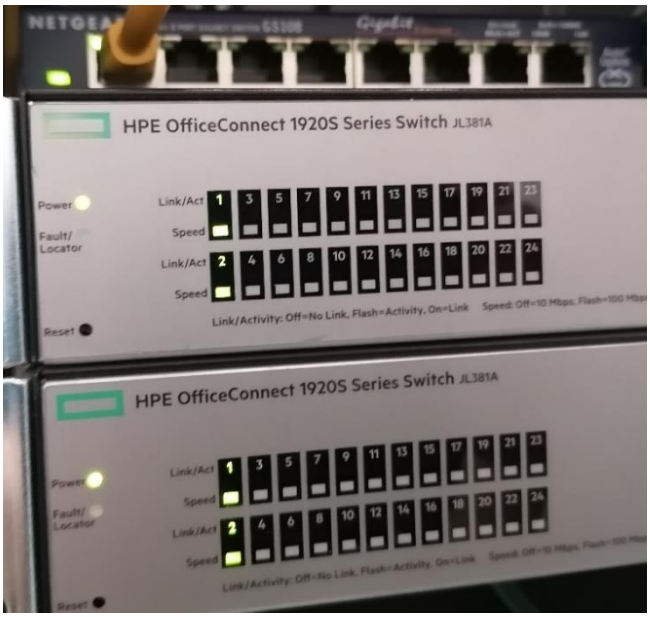
2.3.2.2 - Liaisons physiques des locaux
L'ensemble des sites de la CDC sont chacun et respectivement reliés au réseau public par une ligne unique. Ces points de connexion sont des points classiques, partagés, mutualisés, non dédiés. Ces accès au réseau public sont gérer par le F.A.I. de la CDC, la S.A. ORANGE.

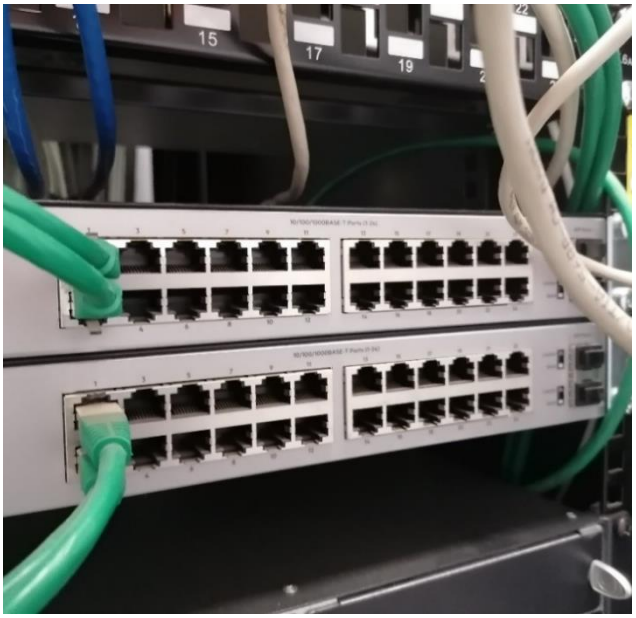
L'ensemble des sites de la CDC reliés aux serveurs du SISR ne disposent pas d'une liaison physique filaire (cuivre ou fibre optique) unitaire spécifiquement dédiée.

2.3.2.2.1 - le siège de la CDC qui héberge le cœur du SISR de l'EPCI, est également concerné par une connexion classique, par un point d'accès, mutualisé, non dédié, non réservé.

Photos ci-dessus et ci-dessous :
- Switchs (commutateurs programmables) de type : HPE OfficeConnect 1920S Series Switch JL381A





3 - Statut physique et logique du SISR de la CDC

3.1 - Le SISR, dans une optique de regard macro-globale, dans l'ensemble de ses domaines régaliens, tant logiques (au sens « logiciels » du terme) que physiques, présente un état d'insécurité et de faiblesse très prononcé :

3.1.1 - le SISR ne dispose que d'un seul serveur physique divisé en plusieurs machines virtuelles. Il est donc central et unitaire ce qui, de facto, entraine le fait que s'il « tombe », l'ensemble de la délivrance des services du SISR de la CDC « tombe ».

3.1.2 - le SISR ne dispose pas d'un serveur de réplication, permettant la sauvegarde, la redondance, la sécurité, la disponibilité, l'intégrité et la pérennité des services informatiques, des données et du réseau de la CDC.

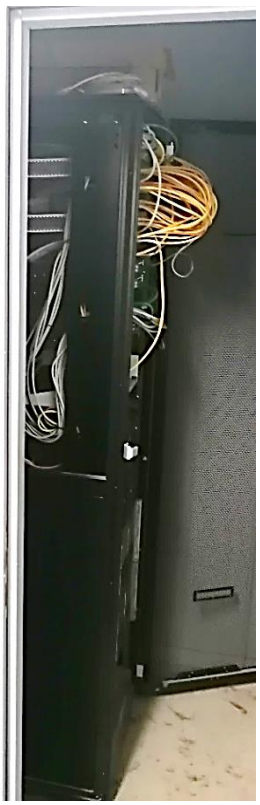
3.1.3 - le SISR, en l'ensemble de ses outils, machines et postes constitutifs, y compris au niveau serveur, ne dispose d'aucune ondulation électrique assurant la protection, la

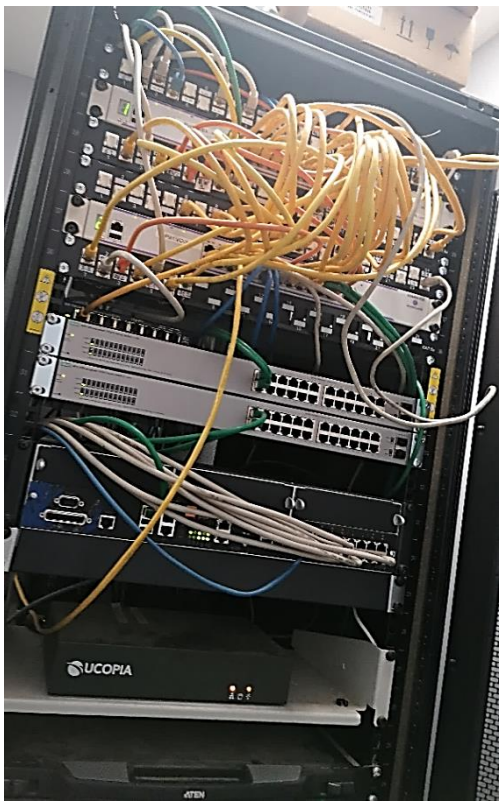
régulation et la sauvegarde spécifiquement dédiées.
Sur l'ensemble des équipements du SISR, les seules « protections» existantes mises en œuvre sont les dispositifs basiques des TGBT (Tableau électriques Généraux Basse Tension) et tableaux électriques individuels de protection des surtensions à disjonction différentielle basse tension classique de type « habitation individuelle ».

Le seul élément présent sur des dispositifs qui n'a jamais été entretenu, ni maintenu consiste en un élément d'ondulation déconnecté, hors service, installé en rack métal.

3.2 - Serveur principal du SISR de la CDC

3.2.1 - le serveur principal du SISR de la CDC est un serveur modulaire constitué de racks amovibles constitutifs d'un ensemble techniquement identifié sous l'appellation « Rack Metal Server »





3.2.2 - le serveur principal du SISR est une unité centrale de marque et type :
- HPE prolient type ML350 Gen9

3.2.2.1 - constituée de :
- deux processeurs sur une architecture CPU Intel Bi Xeon E5-2620v4 à refroidissement par dissipateur de chaleur et ventilation AIR/AIR

- soutenus par une mémoire vivre de 4 barrettes de RAM (Randon Access Memory en 4 x 16 GO) en 16 Go RDIMM Smart Array P840 4GO FBWC

- sur carte mère multi slot de RAM

- 2 fois 2 cages (2x1x2) de 8 emplacements de type SFF de disques soit 4 emplacements de 8 disques (32 disques)

- originellement, chaque disque de marque HPE de 300Go de capacité SAS 12G Enterprise 10K SFF

- le tout alimenté électriquement par une double alimentation en 2 x 500 watts Platinum soit 500 redondés

3.2.2.2 - périphériques incorporés

3.2.2.2.1 - un ensemble de commutateurs (switch) composé de 2 commutateurs montés en Rack l'un sur l'autre, de type Ethernet HP OfficeConnect 19205 24 G 2SFP de 24 ports, commutateur gérable en 24 ports Gigabit Ethernet Réseau et 2 2 x Gigabit Ethernet Uplink, commutateurs connectés via des liaisons câbles en une paire torsadée et fibre optique, 3 couches supportées, 1U Haut

Ces deux « switches » paramétrables sont à ce jour non opérés, non utilisés, alors qu'ils sont la base d'une indépendance réseau du SISR vis-à-vis du ou des F.A.I. possibles.

3.2.2.2.2 - La mise en service des commutateurs permettrait de mettre en place et exploiter le matériel présent, et de déclencher son développement en termes de moyens d'exploitation indépendants, acte qui permettrait principalement à la CDC de redevenir pleinement propriétaire et maître de son SISR et de s'affranchir de l'emprise de l'opérateur F.A.I., permettant ainsi à la CDC de mieux maîtriser et planifier ses techniques et coûts d'exploitation.

Le fait qu'une partie de l'infra soit gérée et dépende entièrement du F.A.I. Orange Business est un élément qui interdit aux administrateurs l'accès et le contrôle à des fonctions vitales et propriétaires du SISR de la CDC ; cela empêche les administrateurs d'avoir à 100% la maîtrise du SISR de la CDC et j'insiste, cela rend la CDC prisonnière et ses administrateurs tributaires de l'opérateur F.A.I. pour certaines fonctions importantes.

Il faut entièrement revoir la topologie interne du SISR de la CDC et envisager sur le long terme les actions utiles à une reprise complète de l'infrastructure réseau et ne laisser à l'opérateur F.A.I. que la gestion des liens internet.

3.2.2.2.3 - ESET Mail Security for Microsoft Exchange Server
L'ensemble de l'infrastructure du SISR de la CDC est placée sous solution de protection identifiée sous l'enseigne « ESET Mail Security ».

3.2.3 - le serveur principal du SISR en termes de contexte physique d'hébergement

3.2.3.1 - Situation physique d'hébergement du serveur principal du SISR de la CDC

Le serveur de la CDC est physiquement situé en RDC du Siège Social de la CDC.
Il se situe dans un local dédié « par défaut ».

Ce local serveur est constitué d'un simple « local de débarras ».

Les caractéristiques de ce volume sont les suivantes :

- un volume unique
- ce volume est fermé par une porte isoplane non verrouillable
- ce volume est exigu~~,~~ confiné, clos, non ventilé, non régulé thermiquement
- ne présente aucun dispositif d'alerte incendie

--> le serveur, ses équipements constitutifs et ses équipements périphériques sont, par nature, des sources de chaleur issues de leur fonctionnement normal.

3.2.3.1.1
Le RDC du bâtiment présente deux niveaux zéro distincts.
Ce double niveau de RDC est dû au mode constructif et aux choix architecturaux effectués lors de sa conception.

Le mode constructif choisi est lié à :

- la configuration naturelle du terrain sur lequel l'édifice bâti a été apporté et qui, originellement, présente une pente importante.

- la suspicion et le devoir de précaution face à la possible (mais non avérée) présence de cavités souterraines créées par la présence historique de marnières, sortes de carrières anciennes dédiées à l'extraction de la marne (abondement des sols agraires) dont l'existence et la localisation ne sont pas forcément connues ou révélées et dont la détection entraine des coûts importants, y compris en termes de techniques de détections par forages et analyses de carottages.

Ainsi, le serveur principal du SISR se situe au point le plus bas de l'infrastructure bâtie, point zéro de niveau de l'ensemble de la construction, qui lui-même est en contrebas du niveau zéro de l'atelier technique du service technique qui le surplombe.

Cette position au sein des bâtiments expose le cœur du SISR face à de multiples facteurs de dysfonctionnement et de risque d'endommagement, y compris au travers des risques divers liées à des épanchements ou inondations dues à des fuites de matières ou de liquides de toute nature, par exemple, par rupture de canalisations d'apport de fluide comme des conduite d'eau ou robinets, ou douches des vestiaires des personnels juxtaposées, propices à laisser s'écouler des liquides vers le serveur, son local dédié et ses dispositifs électriques ; écoulements de liquides qui pourraient également trouver leurs origines via la perte ou la rupture de contenant (ou autres événements) entrainant l'épanchement de matières ou fluides corrosifs ou irritants, inflammables ou volatils, stockés ou utilisés par les personnels, les machines-outils et véhicules thermiques dans les volumes directement en liaison avec le local abritant le serveur.

3.2.3.1.2
Ce local serveur est un volume unique par une porte isoplane non verrouillable, sans indentification d'accès, sans surveillance, ne présente aucun dispositif anti-intrusion. Ceci constitue une faille de sécurité importante.

Cette faille permet un accès au serveur par n'importe quelle personne, en quasiment tout temps, sans la moindre traçabilité, sans le moindre filtrage, sans la moindre identification, ni horodatage.

En cas d'intentions malveillantes, de volonté délibérée de nuire, de voler des données ou toute autre action entreprise vouée à porter préjudice au SISR et à la CDC, aucune précaution, ni aucune protection n'existe et les actes malveillants peuvent être menés dans l'anonymat le plus complet.

3.2.3.1.3
Le local présente un volume exigu et non ventilé.

Bien que non verrouillée, la porte isoplane en place permet de le clore. Cette possibilité de fermeture et de configuration de volume font que ce local serveur constitue un volume confiné en termes de ventilation et d'aération.

La chaleur dégagée par le fonctionnement des matériels, les températures admissibles dans la plage de fonctionnement des équipements prévue par les constructeurs, nécessite une ventilation et une aération régulée, performante, assurant le filtrage des poussières et la dessiccation par régulation hygrométrique de l'air.

3.2.3.1.4
Le Local Serveur ne dispose d'aucun équipement de détection et d'alerte incendie.

Le serveur et ses équipements périphériques sont des machines fonctionnant via un ou des alimentations d'origine électrique, assurant des fonctions variées telles que le redressement, la régulation, la transformation, la distribution et répartition des charges, de travail, des courants forts et faibles, des tensions, des ampérages, etc…

Le fonctionnement du serveur et des périphériques associés entraîne des variations et principalement des hausses de température ainsi que des risques (mêmes maitrisés à la conception) d'échauffement pouvant déboucher sur des points chauds, propices à des départs de feu en cas de panne, de défauts ou d'usures entraînant un fonctionnement anormal.

L'absence de système de détection et d'alarme incendie adaptée et dédiée au serveur, à ses périphériques et à son local sont un risque majeur de perte d'intégrité, de détérioration des équipements et des données stockées.

3.2.3.2 - Bureau, locaux de la direction, de l'administration du SISR de la CDC et accès aux solutions logiques et physiques du SISR

Les bureaux et locaux destinés à l'usage du ou des administrateurs du SISR se doivent d'être d'un accès et d'un usage très surveillé et restreint.

Ces espaces sont des lieux stratégiques dans tous les cas de figure sans exception. Ils sont les volumes qui hébergent les outils, dispositifs, solutions et personnels qui pilotent l'infrastructure et en garantissent la stabilité, la disponibilité, la continuité, la sécurité, l'intégrité et la confidentialité.

Ces accès doivent faire l'objet de toutes les attentions, horodatages, verrouillages et maîtrises.

Concernant les accès aux solutions logiques et physiques du SISR qui y sont liées, il en va exactement de même !

Il est capital de sécuriser et de contrôler les accès administrateur au sein de l'établissement et de ses locaux annexes liés au SISR. Il est également indispensable que les personnels hors administrations qui se verront la possibilité d'y accéder soient clairement identifiés et habilités dans et par des procédures et règlements précis et clairement établis.

Au sein d'une organisation, un SISR et ses administrateurs système occupent un rôle majeur. Les administrateurs sont responsables de l'installation, de la maintenance, de la configuration des ordinateurs, réseaux, serveurs ou bases de données, etc… Ils sont en charge de l'administration des bases de données, des infrastructures réseau, de la sécurité informatique des ordinateurs, des sites web, des logiciels, ou encore des télécommunications, etc…

Les administrateurs ont davantage de droits d'accès que les autres collaborateurs. Ils ont et doivent avoir accès partout, à tous les échelons utiles à leur mission et ceci parfois au-delà et par-delà les « habitudes, positions et rôles, mêmes hiérarchiques ». Ils ont un rôle d'ingénierie sociale qui est une composante incontournable de leur action.

Les administrateurs sont et doivent être en mesure d'accéder aux fichiers et aux données sensibles, de créer ou de supprimer des comptes, d'assigner des droits d'accès aux différents utilisateurs, de télécharger des logiciels, ou encore de modifier les systèmes internes.

Les comptes administrateurs et les comptes à privilèges élevés ont une importance capitale. Ils jouent un rôle essentiel, mais peuvent également représenter une faille pour la cybersécurité si leurs rôles et actions, moyens et prérogatives sont négligés et s'ils ne disposent pas des outils utiles et proportionnés.

D'une part, les droits d'accès quels qu'ils soient, y compris et surtout ceux des administrateurs, sont des droits stratégiques qui peuvent attirer la convoitise des hackers et autres cybercriminels. D'autre part, un administrateur peut lui-même abuser de ses privilèges à des fins mal

intentionnées… (N.B. : Les fuites de données internes ont augmenté de 61 % au second trimestre 2021). Selon les organismes de tutelle tels que la CNIL, l'ANSSI, etc... Plus de 64 % des entreprises de services financiers ont plus de 1 000 fichiers sensibles accessibles à tous les employés… ce qui est le cas de la CDC. En moyenne, 50 % des comptes utilisateur sont obsolètes, situation que la CDC connait bien malheureusement ! Par ailleurs, 58 % des entreprises possèdent plus de 1 000 dossiers dont les droits sont incohérents… la CDC n'y échappe pas… Malgré ces chiffres alarmants et le danger permanent, de nombreuses entreprises négligent encore la sécurité des comptes administrateurs, ce qui est le cas de la CDC.

Actuellement, la sécurité du SISR de la CDC ne tient que par la qualité des interventions des prestaires administrateurs externes qui, là encore, vont au-delà de la mission dont ils ont la charge contractuelle actuellement.

C'est pourquoi, il est important de sécuriser, confidentialiser et contrôler les accès des administrateurs, de sécuriser, confidentialiser et contrôler les accès à leurs bureaux et chacun des locaux en lien avec les équipements, solutions et composantes du SISR, ce qui, à ce jour n'existe pas au sein de la CDC.

La CDC se doit de doter son administration interne des moyens adaptés, à ce jour inexistants. Plusieurs machines et solutions sont à acquérir et à mettre en place. L'effort humain, matériel et physique à envisager sera sans autre choix, d'une dimension importante.

Le principe sera de tendre vers une séparation et un cloisonnement des usages, des accès et de développer une solution pérenne de sécurisation, de gestion, de supervision, d'écoute et de monitoring, d'alerte, de redondance et de sauvegarde.

S'il est à cette étape très difficile d'être précis alors qu'aucun plan n'est établi à court, moyen et long terme, il est toutefois possible de stipuler que plusieurs solutions logiques et physiques liées seront indispensables comme :

- la mise en place d'une machine et de ses périphériques multiples, dédiés à la supervision du SISR (coût estimatif 4000 euros HT)

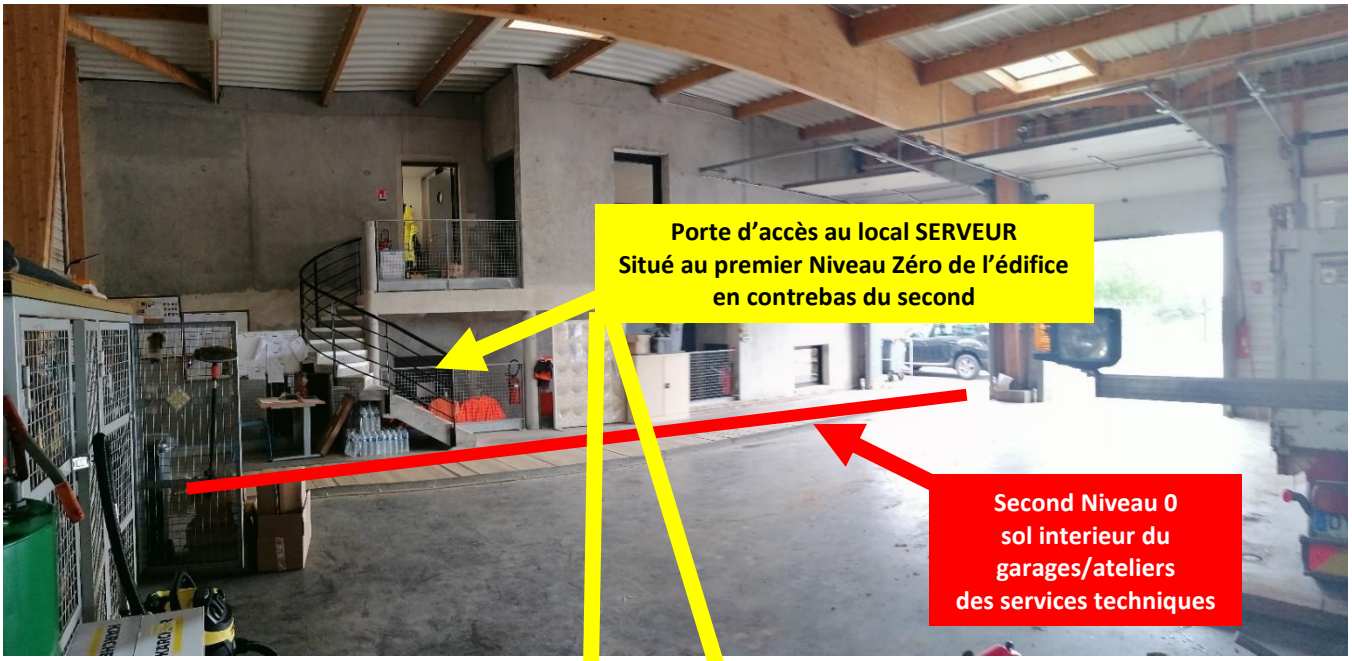
- la mise en place d'une machine et de ses périphériques multiples, dédiés au pilotage de la partie « pare-feu » évoquée précédemment (coût estimatif 3000 euros HT en complément de la solution proprement dite)

- la mise en place et l'affectation d'un bureau adapté et spécifiquement dédié aux administrateurs

- la mise en place et l'affectation de deux locaux séparés, adaptés, sécurisés et spécifiquement dédiés aux différents serveurs et types de machines utiles aux SISR

-Etc…

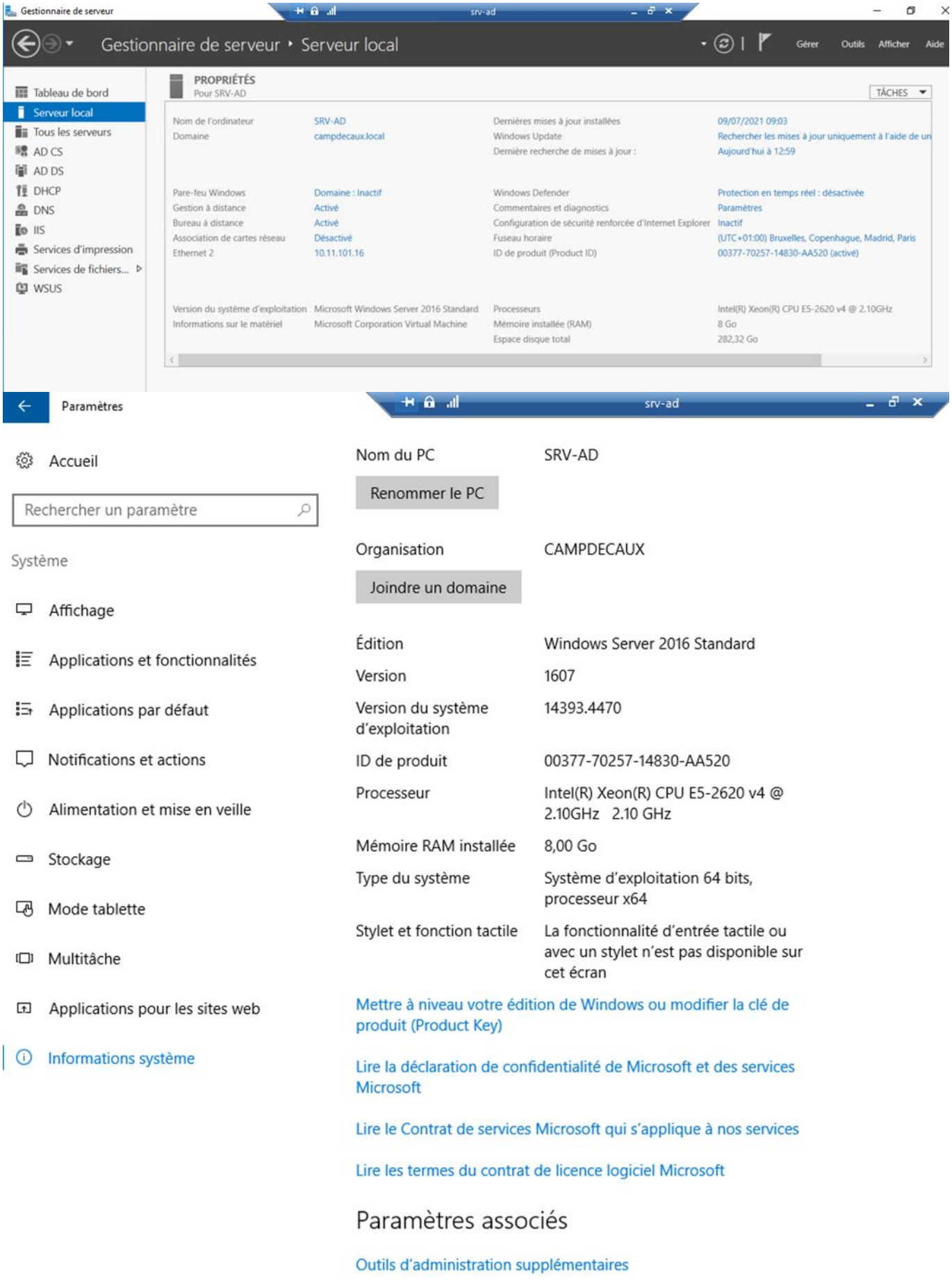
Illustration du contexte physique de situation du serveur rack de la CDC :
- Le serveur principal et son local se situent en point bas de bâtiment exposé à de multiples risques.



Local du Serveur principal :

3.3 - Visuels et analyse explicative sur les solutions logiques du SISR de la CDC

3.3.1 - Visuel sur le Server Active Directory (SRV-AD)



3.3.2 - Topologie des Ressources Serveur de l'infrastructure de la CDC
- répartition de ressources logiques et physiques du serveur rack

Le serveur de la CDC consiste en un serveur rack métal assemblé et constitué de ces différents équipements.

3.3.2.1 - les ressources de départ

L'ensemble des ressources matérielles physiques sont regroupées principalement sur la même machine et utilisées par une affectation et répartition de charge sur des machines virtuelles qui simulent une « séparation des usages ».

A l'implantation et au déploiement d'origine, cet équipement se définissait en un serveur aux caractéristiques suivantes :

- désignation HPE Proliant ML350
- à bi processeur de 9ème Génération Intel Bi Xeon E5-2620v4
- appuyé par :
  - une mémoire vive en 4x16Go RDIMM Smart Array 4Go FBWC
  - 2 compartiments superposés de lecteurs de support de stockage
    - chaque compartiment divisé en 2 x 8 cages
      Pour 8 Disques SFF hard drive cage
      type HPE 300GB SAS 12G Entreprise 10K SFF
      (8 DDR - disques durs mécaniques interchangeables)
  - une alimentation théorique en 2 x 500W Platinium

3.3.2.2 - les ressources actuelles

Un cloisonnement est implémenté pour restreindre les conséquences possibles de comportements inattendus d'un composant, qu'il s'agisse d'un bogue ou de son détournement par un attaquant, mais également pour permettre un nombre croissant de dispositions de sécurité.

Le cloisonnement et la séparation des usages se veulent aussi bien logique que physique. Le but est le suivant :

--> si un matériel ou une solution est détruite, détériorée, volée où attaquée, etc… les cloisonnements et séparations font que :

1- au mieux, les sécurités agissent et protègent

2- au pire, la destruction ou la perte de données et d'intégrité soit partielle et limité et ses conséquences également.

Une des faiblesses actuelles du SISR de la CDC, c'est que l'ensemble de séparations et cloisonnements est uniquement réalisé sur le même rack métal, au même endroit physique et de façon inadaptée.

En effet, il n'y a pas une réelle séparation physique des usages et des machines, tout dépendant actuellement de ce serveur rack et des deux périphériques serveur de données NAS dans les situations critiques évoquées ci-après.

3.3.2.1.1 le serveur virtuel N° 01 --> SRVHYPERV1

Descriptif : HP PROLIANT ML 350 GEN 9
Processeur 2 x Xeon E5-2620 V4 2.10 GHz – 8 Processeurs – 16 Thread
Mémoires 64 Go UDIMM ECC
Stockage 8 x 300 Go SAS 10000 Tr/mn 2,5 '' Raid
Alimentation 2 x 500 W (redondante)
OS Windows 2016 Standard
Cals nombre non précisé
Détail Stockage HPE VSA via iSCSI
LAN - Equipe TEAM-ISCSI composé de NIC1 & NIC2
- Equipe TEAM-LAN composé de NIC3 & NIC4
Rôles de ce serveur :
- serveur membre du domaine campdecaux.local
- serveur HYPER-V pour
- SRV-AD + SRV-APP + SRV-EXCH + SRV-FILE + SRVRDS + SRV-SV1
- serveur pour Services de fichiers
Applicatifs sur serveur :
- Outils de gestion HPE & maintenance informatique
- Gestionnaire de cluster de basculement
& MAJ adapté au cluster / MPIO / Service pour NFS

3.3.2.1.1.1 répartition des services et rôles sur ce serveur HYPER-V 1

--> serveur HYPER-V pour : --> SRV-AD
+ SRV-APP
+ SRV-EXCH
+ SRV-FILE
+ SRVRDS
+ SRV-SV1

Voir précisions des services/rôles de serveur ci-après…

3.3.2.1.1.1.1 - SRV-SV1
Descriptif : VM HYPER-V sur SRV-HYPERV1
Processeur 2 x Processeurs virtuels
Mémoires 5120 Mo
Stockage Contrôleur IDE 0 / Contrôleur iSCSI 0
Détail Stockage
IDE0 = D:\Hyper-V\Virtual Hard Disks\HVSA_Original.vhd
iSCSI0 = D:\Hyper-V\Virtual Hard Disks\Store1.vhdx
LAN LAN-ISCSI

Rôles du serveur :
- Serveur HP StoreVirtual VSA 2014 (Hyper-V)

- Applicatifs sur serveur : HP StoreVirtual VSA 2014

- Ce serveur et ce service font Autorité de Certification (AD CS) pour remote.campagne-de-caux.fr et mail.campagne-de-caux.fr
- AD DS migré à partir d'un SBS 2008, sans nettoyage du SBS. Pas d'approbation (normal).
- Site & service : Présence de l'ancien contrôleur CDCSRV.
- SRV-AD est bien catalogue global.

Script de démarrage en logon.bat

Plusieurs stratégies définies dont une pour les lecteurs réseaux qui fait doublon avec le script logon.bat
Stratégie de UAC disable Stratégie de compte par défaut.

DNS : 5 redirecteurs (3 suffisent) /
Zone directe sur campdecaux.local et campagnedecaux.fr
Le Nettoyage des enregistrements obsolètes est non actif.

Zone indirecte sur 101.11.10.
DHCP : Etendu sur 10.11.101.0 pool de 120 à 170
Deux réservations : Compta-MC et AD-PLUI
Pas d'option d'étendue supplémentaire
IIS : site = administration WSUS

Service d'impression : 4 imprimantes Sharp déployées via une stratégie par imprimante.

Pare feu Windows désactivé [Domaine / Privé / Public]

MAJ a avril 2018 + WSUS pas du tout à jour,
aucune approbation depuis avril 2018.

Fonction de rapport non installé.

Configuration de sécurité renforcé inactive pour les utilisateurs.

3.3.2.1.1.1.2 - SRV-APP

Descriptif : VM HYPER-V sur SRV-HYPERV1
Processeur 4 x Processeurs virtuels
Mémoires 8192 Mo
Stockage Contrôleur iSCSI0 = 80 Go & iSCSI1 = 200 Go
OS Windows 2016 Standard
Détail Stockage
iSCSI0 : C:\ClusterStorage\Volume1\SRV-APP\Virtual Hard Disks\SRV-APP.vhdx
iSCSI1 : C:\ClusterStorage\Volume1\SRV-APP\Virtual Hard Disks\SRV-APP-D.vhdx
LAN LAN-VM

Rôles du serveur :
- Serveur membre du domaine campdecaux.local
- Service de fichiers
Applicatifs sur serveur :
- DADSU
- COLORIS (Métier) Editeur COSOLUCE
- SQL serveur 2014 sp2
- Pare feu Windows désactivé [Domaine / Privé / Public]
- MAJ à avril 2018.
Configuration de sécurité renforcé inactive pour les utilisateurs.
Partages :
_cosoluce / coloris$ / cosoluce$ / defi / Donnees076CCCampagnedecau$

3.3.2.1.1.1.3 - SRV-EXCHANGE

Descriptif : VM HYPER-V sur SRV-HYPERV1
Processeur 4 x Processeurs virtuels
Mémoires 12288 Mo
Stockage Contrôleur iSCSI0 = 120 Go & iSCSI1 = 200 Go
OS Windows 2016 Standard
Détail Stockage
iSCSI0 : C:\ClusterStorage\Volume1\SRV-EXCH\Virtual Hard Disks\SRV-EXCH.vhdx iSCSI1 : C:\ClusterStorage\Volume1\SRV-EXCH\Virtual Hard Disks\SRV-EXCH-D.vhdx
LAN LAN-VM

Rôles du serveur :
- Serveur membre du domaine campdecaux.local
- Service IIS
- Service de fichiers
Applicatifs sur serveur :
- Microsoft Exchange 2016 serveur CU9
- Symantec Endpoint protection (n'a plus lieu d'être)

Pare feu Windows désactivé [Domaine / Privé / Public]
MAJ à avril 2018.
Configuration de sécurité renforcée inactive pour les utilisateurs.
Information relative à EXCHANGE :
Version de Exchange 2016 serveur actuelle : CU17
Reste 30 Go de libre sur le HDD d:\ pour la banque d'information.
Enregistrement du domaine sur OVH
MX = mail.campagne-de-caux.fr

Enregistrement SPF :
v=spf1 include:_spf.orange-business.fr ~all
Enregistrement DMARC = v=DMARC1; p=none
Pas d'enregistrement DKIM trouvé. A vérifier.
Envoie via smtp.relay.orange-business.fr
Domaines acceptés : campagne-de-caux.fr
Une seule base de données : DB1
Certificat autosigné campdecaux
Nombre de BAL = 103

3.3.2.1.1.1.4 - SRV-FILE

Descriptif : VM HYPER-V sur SRV-HYPERV1
Processeur 2 x Processeurs virtuels
Mémoires 4096 Mo
Stockage Contrôleur iSCSI0 = 80 Go & iSCSI1 = 800 Go
OS Windows 2016 Standard
Détail Stockage
iSCSI0 : C:\ClusterStorage\Volume1\SRV-FILE\Virtual Hard Disks\SRV-FILE.vhdx
iSCSI1 : C:\ClusterStorage\Volume1\SRV-FILE\Virtual Hard Disks\SRV-FILE-D.vhdx
LAN LAN-VM
Rôles du serveur :
- Serveur membre du domaine campdecaux.local
- Service de fichiers
Applicatifs sur serveur :
- VEEAM Backup et Réplication console
- SQL serveur 2012 sp2
Pare feu Windows désactivé [Domaine / Privé / Public]
MAJ à avril 2018.
Configuration de sécurité renforcé inactive pour les utilisateurs.
Partages :
- Plusieurs partages ont été mis en place pour la migration en 2018. Certain de ceux-ci ne doivent certainement ne plus être d'actualité. Voir pour contrôle et suppression des partages obsolètes.

Nom du partage	Chemin du dossier	Type
ADMIN$	C:\Windows	Windows
Brique	D:\CampdeCaux\Cosoluce\Donnees076CCCAMPAGNEDECAUX\Brique	Windows
C$	C:\	Windows
Cil	D:\CampdeCaux\Cil	Windows
COLORIS$	D:\CampdeCaux\Cosoluce\COLORIS	Windows
Cosoluce$	D:\CampdeCaux\Cosoluce	Windows
D$	D:\	Windows
Donnees076C...	D:\CampdeCaux\Cosoluce\Donnees076CCCAMPAGNEDECAUX	Windows
IPC$		Windows
Partage	D:\CampdeCaux\Partage	Windows
Pole Action So...	D:\CampdeCaux\Pole Action Sociale	Windows
Scan	D:\CampdeCaux\Scan	Windows
SEP	C:\Sources\SEP	Windows
Services	D:\CampdeCaux\Services	Windows
SI2G	D:\CampdeCaux\SI2G	Windows
Users	D:\Users\Shares	Windows
VBRCatalog	D:\VBRCatalog	Windows

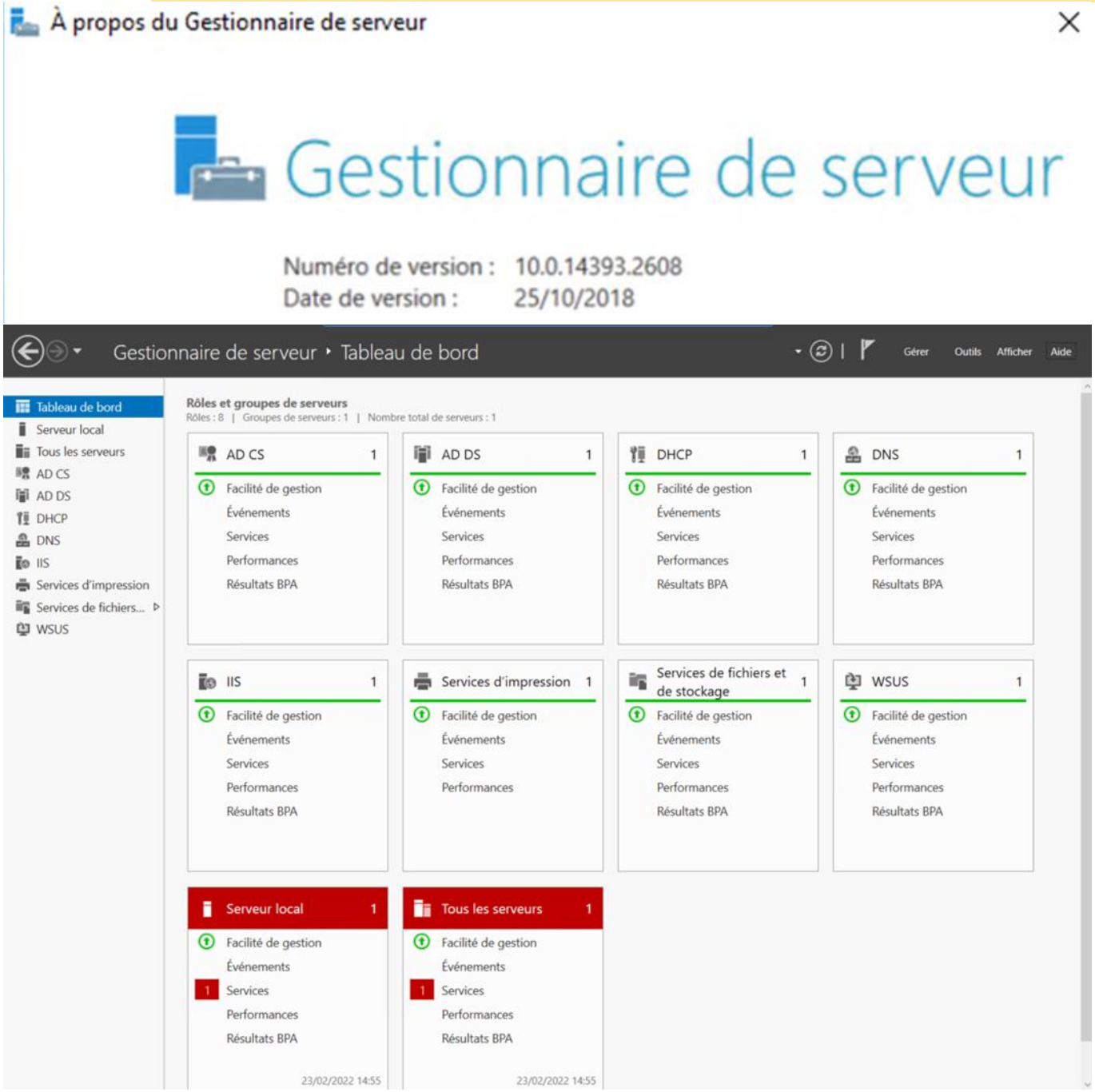
3.3.2.1.1.1.5 - SRV-RDP

Descriptif : VM HYPER-V sur SRV-HYPERV1
Processeur 2 x Processeurs virtuels
Mémoires 4096 Mo
Stockage Contrôleur iSCSI0 = 90 Go & iSCSI1 = 100 Go
OS Windows 2008 R2 Standard
Détail Stockage
iSCSI0 : C:\ClusterStorage\Volume1\SRVRDS\Virtual Hard Disks\SRVRDS.vhdx
iSCSI1 : C:\ClusterStorage\Volume1\SRVRDS\Virtual Hard Disks\SRVRDS-D.vhdx
LAN LAN-VM
Rôles du serveur :
- Serveur membre du domaine campdecaux.local
- Service de fichiers
Applicatifs sur serveur :
Symantec Endpoint Protection (n'est plus d'actualité)
Pare feu Windows désactivé [Domaine / Privé / Public]
Windows serveur non activé.
Fonctionnement RDS (Service de bureau à distance) semble ne pas être utilisé. C'est en lien avec le service RDS de bureau à distance. Il faut donc décider de le supprimer ou de l'utiliser pour définir l'utilité de mobiliser ou non les ressources associées et les réaffecter ou non.

3.3.2.1.2 le serveur virtuel N° 02 --> SRVHYPERV2

Descriptif : HP PROLIANT ML 350 GEN 9
Processeur 2 x Xeon E5-2620 V4 2.10 GHz – 8 Proc – 16 Thread
Mémoires 64 Go UDIMM ECC
Stockage 8 x 300 Go SAS 10000 Tr/mn 2,5 '' Raid
Alimentation 2 x 500 W (redondante)
OS Windows 2016 Standard
Cals nombre non précisé
Détail Stockage HPE VSA via iSCSI
LAN Equipe TEAM-ISCSI composé de NIC1 & NIC2
Equipe TEAM-LAN Composé de NIC3 & NIC4
Rôles du serveur :
A/ - serveur membre du domaine campdecaux.local
B/ - serveur HYPER-V pour : SRV-SV2
Descriptif : VM HYPER-V sur SRV-HYPERV2
Processeur 2 x Processeurs virtuels
Mémoires 5120 Mo
Stockage Contrôleur IDE 0 / Contrôleur iSCSI 0
Détail Stockage
IDE0 = D:\Hyper-V\Virtual Hard Disks\HVSA_Original.vhd
iSCSI0 = D:\Hyper-V\Virtual Hard Disks\Store1.vhdx
LAN LAN-ISCSI
Précision de rôles du serveur :
- Serveur HP StoreVirtual VSA 2014 (Hyper-V)
- Applicatifs sur serveur : HP StoreVirtual VSA 2014
- serveur pour Services de fichiers
Applicatifs sur serveur :
- Outils de gestion HPE & maintenance informatique
- Gestionnaire de cluster de basculement
& MAJ adapté au cluster / MPIO / Service pour NFS

3.3.2.2 Details / Focus sur le serveur SRV AD



Nom du système d'exploitation Microsoft Windows Server 2016 Standard
Version 10.0.14393 Numéro 14393
Autre description du système d'exploitation Non disponible
Fabricant du système d'exploitation Microsoft Corporation
Ordinateur SRV-AD
Fabricant Microsoft Corporation
Modèle Virtual Machine
Type PC à base de x64
Référence (SKU) du système None
Processeur Intel(R) Xeon(R) CPU E5-2620 v4 @ 2.10GHz, 2095 MHz, 4 cœur(s), 4 processeur(s) logique(s)
Version du BIOS/Date Microsoft Corporation Hyper-V UEFI Release v1.0, 26/11/2012
Version SMBIOS 2.4
Version du contrôleur embarqué 255.255
Mode BIOS UEFI
Fabricant de la carte de base Microsoft Corporation
Modèle de la carte de base Non disponible
Nom de la carte de base Carte de base

Rôle de la plateforme Bureau
État du démarrage sécurisé Activé
Configuration de PCR 7 Non disponible
Répertoire Windows C:\Windows
Répertoire système C:\Windows\system32
Périphérique de démarrage \Device\HarddiskVolume2
Option régionale France
Couche d'abstraction matérielle Version = "10.0.14393.3297"
Utilisateur CAMPDECAUX\adminmsi
Fuseaux horaires Paris, Madrid
Mémoire physique (RAM) installée 8,00 Go
Mémoire physique totale 8,00 Go
Mémoire physique disponible 870 Mo
Mémoire virtuelle totale 13,7 Go
Mémoire virtuelle disponible 3,53 Go
Espace pour le fichier d'échange 5,75 Go
Fichier d'échange C:\pagefile.sys
Sécurité basée sur la virtualisation de Device Guard Désactivé
Un hyperviseur a été détecté. Les fonctionnalités nécessaires à Hyper-V ne seront pas affichées.

3.3.2.3 - Details / Focus sur le serveur SRV AD
Explication des services et rôles présents sur le serveur SVR-AD, le serveur determinant de la CDC

3.3.2.3.1 - Service AD CS :
autorité de certification racine sous Windows Server

Avec une autorité de certification, vous pourrez gérer vos certificats numériques, de la délivrance d'un certificat à sa révocation. Cette couche de sécurité offre notamment les avantages suivants :

- intégrité
- authentification
- non-répudiation
- et confidentialité.

Ceci est possible grâce à l'utilisation à la fois de certificats, mais aussi de clés, c'est pour cela que l'on parle souvent de : - PKI : Public Key Infrastructure
en français de : - IGC - Infrastructure de gestion de clés.

Sous Windows Server, la mise en œuvre d'une autorité de certification s'effectue par l'intermédiaire du rôle ADCS : Active Directory Certificate Services. Il existe des outils open source pour mettre en place une CA sous Unix/Linux.

Une autorité de certification s'avère utile et sollicitée dans le cadre de nombreux projets :

- mise en place d'un serveur NPS (Network Policy Server) pour obtenir un certificat valide pour utiliser le 802.1X
- mise en place des flux sécurisés et chiffrés pour votre serveur WSUS, ou votre Active Directory,
- authentification renforcée sur des applications, accès VPN, etc…

Autant de projets et besoins pour lesquels vous pourriez avoir besoin de la solution AD CS.

Cette autorité de certification Microsoft sera capable également de signer vos scripts PowerShell pour que leur exécution soit autorisée sur les serveurs et les postes clients de votre entreprise.

Ceci vous évitera de modifier la politique d'exécution des scripts et d'exposer vos postes aux problèmes que ça implique.

L'autorité de certification est un vaste sujet, qui peut s'avérer complexe et nécessite a minima un serveur mais selon vos besoins et les rôles à déployer, plusieurs serveurs peuvent être nécessaires.

3.3.2.3.2 - Service AD DS - Active Directory Domain Services

Les AD DS (Active Directory Domain Services) constituent les fonctions essentielles d'Active Directory pour gérer les utilisateurs et les ordinateurs et pour permettre aux administrateurs système d'organiser les données en hiérarchies logiques. ADDS permet la mise en place des services de domaine Active Directory, autrement dit la mise en œuvre d'un domaine et d'un annuaire Active Directory.

Ce rôle permet de gérer au sein d'un annuaire les utilisateurs, les ordinateurs, les groupes, etc. afin de proposer l'ouverture de session via des mécanismes d'authentification et le contrôle d'accès aux ressources.

3.3.2.3.3 - Service DHCP

Le service et rôle DHCP est en fait un protocole DHCP (Dynamic Host Configuration Protocol).

C'est un protocole client/serveur qui fournit automatiquement un hôte IP (Internet Protocol) avec son adresse IP et d'autres informations de configuration associées, telles que le masque de sous-réseau et la passerelle par défaut. Les RFC 2131 et 2132 définissent DHCP comme norme IETF (Internet Engineering Task Force) basée sur le protocole Bootstrap (BOOTP), un protocole avec lequel DHCP partage de nombreux détails d'implémentation. DHCP permet aux hôtes d'obtenir les informations de configuration TCP/IP requises à partir d'un serveur DHCP.

A la CDC, sur son Windows Server 2016 qui comprend le serveur DHCP, c'est un rôle de serveur de mise en réseau (facultatif) qui est déployé sur votre réseau pour allouer des adresses IP et d'autres informations aux clients DHCP de façon automatisée.

Il est à noter que tous les systèmes d'exploitation clients basés sur Windows incluent le client DHCP dans le cadre du protocole TCP/IP, et le client DHCP est activé par défaut.

3.3.2.3.4 - Service DNS

Le DNS pour « Domain Name System » est un service, un rôle de serveur, permettant de traduire un nom de domaine en informations de plusieurs types qui y sont associées, notamment en adresses IP de la machine portant ce nom.

DNS (Domain Name System) est l'une des suites standards de protocoles qui composent TCP/IP. Le client DNS et le serveur DNS fournissent ensemble des services de résolution de noms de mappage d'adresses d'ordinateur à IP aux ordinateurs et aux utilisateurs.

À la demande de la DARPA (Defense Advanced Research Projects Agency, « Agence pour les projets de recherche avancée de défense ») américaine, Jon Postel et Paul Mockapetris ont conçu le « Domain Name System » en 1983 et en ont rédigé la première réalisation.

3.3.2.3.5 - Service IIS / Serveur web IIS (Windows Web-IIS Alternatives)

Anciennement appelé Internet Information Server, IIS (Internet Information Services) est le serveur web de Microsoft disponible en tant que rôle sous Windows Server et en tant que fonctionnalité sur les versions clientes de Windows.

IIS est principalement utilisé en tant que dépendance pour d'autres services, comme le service RDS, (serveur RDS pour Remote Desktop Services / Service de bureau à distance) pour son portail web et l'autorité de certification pour obtenir des certificats depuis une interface web ou tout autre service (ou logiciel tiers) proposant une interface web ou utilisant le protocole HTTP ou HTTPS.

IIS est disponible depuis Windows NT et chaque version de Windows (ou sa version serveur) possède une version différente de IIS et donc des fonctionnalités différentes.

Exemple :
Le support du protocole HTTP/2 est disponible uniquement depuis la version 10 de IIS sous Windows Server 2016 et Windows 10.

Ce serveur Web est utilisé pour aider les utilisateurs de Windows à héberger divers types de contenu sur le Web, tels que des fichiers multimédias, des documents ou même des sites Web à part entière. À l'heure actuelle, Apache est le serveur Web Windows le plus populaire, suivi de près par IIS, ce qui est assez impressionnant.

L'interface graphique d'IIS facilite la conception, la personnalisation, la configuration et la publication de sites Web à partir d'un seul emplacement.

Il dispose d'un outil de gestion de site Web intégré appelé Gestionnaire IIS que vous pouvez utiliser pour ajuster des options telles que les paramètres de sécurité, les paramètres de performance, les préférences de journalisation, ainsi que les pages d'erreur ou les valeurs par défaut des sites Web que vous administrez.

D'un point de vue technique, IIS est assez polyvalent, car il peut servir des pages Web standard et dynamiques. Ainsi, vous pouvez l'utiliser pour créer et publier des pages Web HTML, mais c'est bien de savoir que vous pouvez également gérer des pages PHP et des applications ASP.NET.

3.3.2.3.6 - Service D'IMPRESSION

La console Gestion de l'impression est installée par l'intermédiaire du Gestionnaire de serveur et permet l'administration des imprimantes et serveurs d'impression.

Un serveur d'impression est un serveur qui permet de partager une ou plusieurs imprimantes entre plusieurs utilisateurs (ou ordinateurs) situés sur un même réseau informatique.
Sous le Windows Server 2016 de la CDC, il permet d'installer, configurer, déployer le service d'impression et de numérisation de document.

Le serveur d'impression est un rôle incontournable en environnement professionnel pour assurer une bonne gestion des imprimantes et des copieurs, pour plusieurs raisons :

- Faciliter le déploiement des imprimantes sur les postes clients
(listing dans l'annuaire Active Directory et déploiement par GPO).
- Gérer les autorisations d'accès aux imprimantes (par exemple, via des groupes de sécurité).
- Préconfigurer les imprimantes déployées sur les postes clients
(par exemple, par défaut en noir et blanc).
- Gérer des files d'attente centralisées : si un fichier bloque la file d'attente, vous pourrez le visualiser.

En matière de sécurité, il assure un rôle important, car il doit servir de relais entre vos copieurs/imprimantes isolés sur un VLAN et vos postes clients, isolés sur un autre VLAN.

3.3.2.3.7 - Service WSUS - Windows Server Update Services (WSUS)

WSUS (Windows Server Update Services) permet aux administrateurs informatiques de déployer les dernières mises à jour de produits Microsoft. Grâce à WSUS, vous pouvez gérer entièrement la distribution des mises à jour publiées par Microsoft Update sur les ordinateurs de votre réseau. C'est un rôle de serveur qui permet de déployer et d'assurer la maintenance des services liés au service WSUS. C'est un service auquel je suis très sensible et attentif également. Il ne paye pas de mine, mais il est inversement aussi important que discret.

3.3.2.3.8 - SERVICES de FICHIERS et de STOCKAGE

Par ce service qui est un rôle du serveur, vous allez pouvoir mettre à disposition en toute sécurité des fichiers sur votre réseau. Vous pourrez gérer des droits d'accès (lecture, écriture, modification…).

Fournir ce type de rôle dans un réseau permet de centraliser le point de stockage des fichiers, facilitant ainsi la sauvegarde, la restauration, et permettant à plusieurs personnes de travailler ensemble sur un même fichier. Il s'agit ainsi d'un outil de gestion déployé sur le serveur. Ce service est utilisé pour assurer la gestion de ressources pour serveur de fichiers autrement dit des « FSRM ».

Lorsque nous souhaitons partager des fichiers au travers de votre réseau, il faut mettre en place un serveur de fichiers, y compris comme à la CDC, sur Windows Server 2016.

Le Gestionnaire de Ressources du Serveur de Fichiers comprend les fonctionnalités telles que la gestion des quotas permettant de limiter l'espace autorisé pour un volume ou un dossier, pouvant être appliquée automatiquement aux nouveaux dossiers créés sur un volume, définition des modèles de quota qui peut être appliquée aux nouveaux volumes ou dossiers.
Cela permet également aux infrastructures la classification des fichiers et la fourniture des informations sur vos données en automatisant les processus de classification afin que vous puissiez gérer vos données plus efficacement.

Ce rôle, permet de multiples possibilités, pour classer les fichiers, appliquer des stratégies en fonction de cette classification. Les exemples sont extrêmement nombreux…

Pour simple illustration de stratégie, citons le contrôle d'accès dynamique pour restreindre l'accès aux fichiers, le chiffrement des fichiers et l'expiration des fichiers, il y a possibilité de :

- classer les fichiers automatiquement en utilisant des règles de classification de fichiers
- ou, les classer manuellement en modifiant les propriétés d'un fichier ou d'un dossier sélectionné.

Les tâches de gestion de fichiers vous permettent d'appliquer une stratégie ou une action conditionnelle à des fichiers en fonction de leur classification. Les conditions d'une tâche de gestion de fichiers incluent l'emplacement du fichier, les propriétés de classification, la date de création, de la dernière modification ou le dernier accès au fichier. Dans le cadre d'une tâche de gestion de fichiers, vous pouvez faire expirer des fichiers, les chiffrer ou exécuter une commande personnalisée.

La gestion du filtrage de fichiers vous permet de contrôler les types de fichiers que l'utilisateur peut stocker sur un serveur de fichiers. Vous pouvez limiter les extensions pouvant être stockées sur vos fichiers partagés. Par exemple, vous pouvez créer un filtre de fichiers qui interdit le stockage de fichiers dotés d'une extension MP3 dans les dossiers partagés personnels sur un serveur de fichiers. Les Rapports de Stockage vous aident à identifier les tendances d'utilisation des disques et la façon dont vos données sont classées. Vous pouvez également analyser un groupe sélectionné d'utilisateurs afin de détecter toute tentative d'enregistrement de fichiers non autorisés.

Les fonctionnalités incluses dans le Gestionnaire des Ressources de Serveur de Fichiers peuvent être configurées et gérées à l'aide de l'application Gestionnaire des Ressources Serveur de Fichiers ou à l'aide de Windows PowerShell en ligne de commande.

3.3.2.4 - Focus sur les problématiques des services précédemment décrit

3.3.2.4.1 - GLPI / inventaire du parc informatique

Il existe un début de mise en place d'une GLPI au sein du SISR de la CDC. Elle est actuellement basée sur un O.S. de type Ubuntu 20.04 LTS.

Cette solution logique est asservie à une configuration physique, une solution hardware, en souffrance. La maintenance et la solution d'hébergement physique sont inadéquates depuis une longue période.

La GLPI signifie Gestionnaire Libre de Parc Informatique.
C'est une solution logicielle de gestion des services informatiques siglée ITSM pour « IT Service Management » dont la définition réside en sa traduction de « Gestion des Services Informatiques ». C'est une approche stratégique des matériels physiques et des solutions logiques. Elle permet de bâtir et maintenir, de concevoir, distribuer, gérer et améliorer l'usage et la gestion des moyens et technologie de l'information utilisés au sein d'une entité comme la CDC. Cette solution est de droit d'usage libre. C'est une application web, éditée en PHP et distribuée sous licence GPL qui rend cette technologie librement exécutable, exploitable, modifiable et développable par toute personne ou entité qualifiée la mettant en œuvre

Dans le contexte relevé au moment de l'élaboration de ce projet, il est nécessaire d'étudier le remplacement des solution physiques existantes constitutives des supports de la GLPI en place par des matériels adaptés, sécurisés, protégés et d'y migrer les services GLPI dans une action concertée, combinée et synchrone entre la direction interne du SISR constituée de son administrateur et de son prestataire externe en ces administrateurs systèmes et réseaux, y compris dans ces aspect support de création, rédaction, mise au point, abondement et mises à jour synchronisées des procédures d'installations, de gestion, d'administration, de sécurisation et de pérennisation physiques et logiques des solutions logiques et physiques de la GLPI ainsi mise en place.

Lorsque la GLPI sera en place, elle permettra la mise en place de la gestion administrative de l'ensemble des matériels physiques et solutions logiques du SISR de la CDC. Elle permettra, à terme, de connaître avec exactitude la composition et de gérer plus efficacement le SISR :

- machine par machine
- solution par solution
- licence par licence

Dans son second aspect, elle permet de mettre à disposition un service de gestion des services d'assistance autrement siglé ITSM pour « Issue Tracking System et Service Desk). Cette fonctionnalité de gestion d'assistance (autrement nommée helpdesk) fournit aux utilisateurs un service leur permettant de signaler aux administrateurs, des incidents ou de créer des demandes d'intervention basées sur un actif ou non via la création d'une demande appelée « ticket d'assistance ».

Dans un troisième temps, les fonctionnalités de la solution GLPI, aident les Administrateurs Systèmes et Réseaux à créer une base de données regroupant des ressources techniques et de gestion, ainsi qu'un historique des actions de maintenance.

Dans un quatrième temps les caractéristiques de la GLPI permettent aux administrateurs de construire un inventaire de toutes les ressources de la société et de réaliser la gestion des tâches administratives et financières. Ceci permet, en liaison avec les services financiers et les décideurs de mettre en place des planifications financières de financement du SISR et de donner des outils propres à prévoir et planifier le plus possible les coûts prévisibles de fonctionnement, de renouvellement, de sécurisation et de pérennisation.

Au jour zéro du projet :
- seules les fonctions de suivi incident sont en place.
- un début d'information sur gestion administrative des postes est en création.
- un début de constat de sur utilisation des licences Microsoft Office est en service.

3.3.2.4.2 - VSA

3.3.2.4.2.1 - Licence VSA

La solution VSA présente au sein du SISR de la CDC est, à l'origine, une solution logique vouée à la surveillance à distance des terminaux de la CDC et qui avait pour but de générer également en parallèle l'infrastructure.

Cette solution pose actuellement un problème d'obsolescence car le produit n'a plus de commercialisation en l'aspect et version qui intéresse le SISR de la CDC. De plus, son support a pris fin en 2020.

L'objectif concernant cette solution logique, est de supprimer cette application qui permet la tolérance de panne entre deux serveurs et passer sur la solution native liée à Hyper-V.

Hyper-V est également connu sous le nom de Windows Server Virtualisation.

Hyper-V est un système de virtualisation basé sur un hyperviseur 64 bits.
Il connait son développement depuis et sur base de la version de Windows Server 2008.

Hyper-V permet à un serveur physique de devenir Hyperviseur et ainsi de gérer et héberger des machines virtuelles communément appelées VM (Virtual Machines).

Hyper-V est dit « natif » car issu et intégré au système

d’exploitation (OS) mis en place par et depuis la « maison mère ».

Grâce à cette solution et technologie, il est possible d’exécuter virtuellement plusieurs systèmes d'exploitation sur une même machine physique et ainsi d'isoler ces systèmes d'exploitation les uns des autres. Hyper-V permet à de nombreux systèmes d'exploitation de fonctionner en son sein.

Les ressources de l'hyperviseur sont alors mutualisées pour différentes VM, ce qui présente un intérêt économique car auparavant il fallait envisager une machine physique par serveur.

3.3.2.4.2.2 - Le volume de stockage VSA

Ce volume de stockage des données liées à la solution VSA est au bout de ces capacités en termes de disponibilité d’espace, il est plein et peut donc générer des incidents majeurs de production.

Suite à un second incident majeur lié à la solution VSA, les administrateurs externes ont fait en sorte d’intervenir sur l’ensemble des Machines Virtuelles en place (VM) pour qu’elles ne soient plus stockées sur ce service.

Il reste à mettre en place la tolérance de panne en Hyper-v puis à supprimer VSA.

3.3.2.4.3 - MAJ Serveur physique

Non effectué suite à risque potentiel de crash VSA.

Cet aspect génère un risque majeur dans le fonctionnement et la sécurité du Serveur Physique Principal du SISR de la CDC.

3.3.2.4.4 - Sauvegarde avec la solution et suite logiciel VEEAM + NAS

3.3.2.4.4.1 - VEEM - Solution logique de sauvegarde et clonage

VEEAM est une solution logique constituée d’un ensemble optionnel qui crée une suite logique de sauvegarde et réplication des systèmes et des données.

Cette solution logique crée des sauvegardes au niveau « image » des applications, c’est-à-dire des répliques parfaites et paramétrables, compatibles VSS en cours d'exécution.

Cela garantit une restauration efficace des applications, des services stratégiques et autorise des scénarios de restauration spécifique des applications.

En fonction des choix techniques et opérationnels des administrateurs du SISR, il est à noter qu’au moment du projet la question se pose de migrer ou non vers une solution concurrente comme « ACRONIS » pour des raisons purement techniques et

logiques de détermination et d'usage.

Il est à noter que lors du « crash » des volumes des disques du serveur de la CDC en juillet 2021, cette solution a permis de restaurer les services endommagés et perdus et d'assurer la survie du SISR via les interventions en interne et les compétences professionnelles des administrateurs externes directement en contact avec l'infrastructure sur place.

N.B : le Microsoft VSS (Microsoft Volume Shadow Copy Service).
Lancé à l'origine avec Windows Server 2003, l'API de snapshot de Windows, VSS, le service VSS de Microsoft est une infrastructure Windows intégrée conçue pour les sauvegardes d'application.
Service Windows natif, VSS simplifie la création d'un jeu cohérent des données applicatives lors d'une sauvegarde.
Il repose sur la coordination entre les composants VSS Requestors, Writers et Providers pour figer un volume de disque, dans le but d'obtenir des sauvegardes contenant des données intègres.
Telle en est la définition technique.
En termes plus simples, VSS informe les applications qu'une sauvegarde va avoir lieu. Il coordonne les opérations de sauvegarde entre l'OS et les applications en cours d'exécution.
Il informe également l'OS de la fin des sauvegardes en demandant aux applications d'exécuter des tâches post-sauvegarde importantes, comme tronquer les journaux et autres opérations de nettoyage propres à ces applications.
En dépit de l'utilisation de l'hyperviseur, l'utilisation de VSS s'avère généralement nécessaire pour sauvegarder les applications en cours d'exécution sur les serveurs Windows. Il peut s'agir d'Exchange, SQL Server, Active Directory, Oracle ou toute autre application nécessitant un accès continu au disque.

3.3.2.4.4.2 - NAS - Serveur de stockage en réseau dédié à la sauvegarde des données de la CDC

NAS et une abréviation issue de l'anglais :
- Network Attached Storage = Stockage En Réseau

La principale fonction d'un NAS est le stockage de données en un volume centralisé pour des clients réseau hétérogènes.

Il assure la cohérence et la cohésion d'une sauvegarde au sein d'un système même si celui-ci est disparate, hétérogène , c'est-à-dire un SISR qui est composé d'éléments de natures différentes et qui n'a pas ou peu d'unité à l'image du SISR de la CDC.

Un NAS, c'est également ce que l'on nomme un serveur de stockage en réseau type NAS. C'est un boîtier actif, autonome, contenant des disques durs de stockage de données (tout type de datas) que l'on fait fonctionner en volume de sauvegarde, c'est-à-dire que l'on fait fonctionner les disques durs qui le composent comme un seul disque.

Les avantages principaux sont :

- Atout 1er : La souplesse de détermination des capacités employées, l'utilisateur pouvant déterminer quel type et quelle capacité de disque il choisit d'utiliser en fonction des objectifs de sauvegarde, de pérennisation, de niveau d'intervention et de sécurisation qu'il est utile d'atteindre, tout en incluant dans le choix la notion de coûts, à court, moyen et long terme.

- Atout second : le NAS est un volume de disque. Ainsi, si un de ces disques durs s'abîme, est endommagé ou subi une destruction progressive due à divers types d'incident ou de disfonctionnement, les données du, ou des, disques concernés vont migrer de façon automatique vers les autres disques du volume et signaler l'anomalie pour procéder à l'analyse du problème et procéder au remplacement du disque dur défectueux ou en fin de vie.

3.3.2.4.4.3 - NAS originel situé en salle des archives

A l'origine du projet, seul un NAS unique existait et est toujours maintenu. Il s''agit du NAS premier de la CDC de marque « Synology ». C'est un matériel de qualité correspondant aux besoins premiers du SISR de la CDC.

Par manque d'infrastructure bâties adaptées, ce NAS se situe et fonctionne au sein de la salle des archives (archives de type « récentes » en opposition au stockage pour archivage longue durée actuellement en container dans le garage des services techniques).

Les risques sont :

- un risque d'incendie entrainant (outre un risque de feu au sein des locaux du siège) la perte du NAS et de ses données stockées en cas d'évènement imprévu, suite à divers disfonctionnements envisageables comme un court-circuit, une surchauffe matérielle, etc… Le fait que cet équipement électrique soit situé au milieu d'archives papier augmente la probabilité d'un risque incendie.

- un risque de dégradation involontaire ou de vol physique : En effet, la pièce concernée n'est pas sécurisée, pas fermée à clef, et de nombreux personnels sont appelés à y circuler plus ou moins temporairement.

- La configuration de disposition du NAS premier en salle d'archive, entraîne un risque de manipulation involontaire. Par exemple, s'il y a besoin de prendre un dossier adjacent à l'équipement, il faut déplacer le NAS.

De plus, il m'a été donné de constater sur place, et à plusieurs reprises, que l'exiguïté de la pièce fait s'installer des personnels de façon sommaire, assis sur une table placée au-devant du NAS, entrainant des coups de pieds involontaires en étendant fort légitimement leurs jambes.

Si ces à coups répétés peuvent être considérés, à tort comme insignifiants, ils peuvent être la cause par répétition, d'une usure jusqu'à une casse physique du matériel, entrainant, au moins, la perte de fonction du matériel, au pire une perte de données.

Ces risques de dégradations involontaires par la position du NAS qui se situe en étage inférieur du dispositif d'étagères qui l'accueil et lui servent « d'emplacement faute de mieux » sont corrigeables à peu de frais.

Par exemple, la mise à « hauteur d'homme » de l'équipement, le rend davantage accessible pour intervention et assure un moindre risque de choc.

De plus, la mise en place du dispositif au sein d'un espace dédié et sécurisé , peut commencer, par exemple, par l'installation d'une baie murale ou d'un support stable et fixe spécifique et réservé.

- Autre point, la configuration actuelle d'emplacement du NAS, entraine un risque de vol physique par la facilité d'accès.

De facto, un risque de vol du NAS entraine le vol des données stockées.

Pour exemple, un individu malveillant qui, par ruse, parviendrait à se fondre sous un prétexte fallacieux, parmi le flot des personnes approchant le dispositif… pourrait entrainer des conséquences très graves de disparition de la ressource.

De plus, si l'individus ci-avant évoqué, venait à bénéficier d'une connaissance de la data suffisante, cela le placerait en position d'exploiter les contenus illicitement, ce qui aurait des répercutions, des conséquences extrêmement graves en termes de sécurité, de confidentialité en lien avec l'ensemble des domaines et conséquences concernés.

Le NAS premier, ne présente pas de dispositif d'ondulation électrique, ce qui amplifie les risques d'endommagement de celui-ci et en particulier de ses disques de volumes et donc une perte de données. Il est à noter également que l'absence d'ondulation entraîne des risques également en terme de réseau et de

communication, de synchronisation et de déroulement des cycles de fonctionnement et donc de sauvegardes.

3.3.2.4.4.4 - NAS secondaire dit NAS de réplication originel situé en « pseudo salle serveur »

Depuis juillet 2021, la réplication du NAS premier, se fait sur un NAS identique, de même marque pour assurer en urgence un dispositif de sauvegarde par réplication efficace et donc améliorer la sécurité des données de la CDC.

Ce NAS est un Synology Station D5418 4 Baies, équipé de DDR, Disque Dur Mécaniques WD Western-Digital gamme RED pro de 2 TO de capacité chacun en 3.5 » (3.5 pouce standard) à 7200 tours minutes.

J'ai pu assister à la mise en place de ce dispositif en second en intervenant aux côtés de mes confrères Administrateurs Système et Réseaux de la société MSI 2000.

Ainsi, ce NAS second constitue avec le NAS premier, une réelle solution de sauvegarde et de sécurisation des données.

Toutefois, il reste des points à améliorer dès que possible.

Ce second NAS de réplication est stocké en « salle serveur », par manque de possibilités adaptées autres. Cet emplacement a été déterminé par défaut pour parer au plus pressé.

Pour la sécurité des données ainsi que pour une reprise d'activité dans des délais cours ou au minimum « acceptables » en cas d'incident grave, le second NAS ainsi que le second serveur ne devraient pas être ni dans la même pièce que le serveur principal, ni dans le même bâtiment. Chaque sauvegarde est autonome et envoyée sur le NAS stocké en salle archive.

3.3.2.4.5 - RDS sur Windows Server

Le sigle **RDS signifie « Remote Desktop Services »** que nous pouvons traduire par « Services de Bureau à Distance »

C'est une fonctionnalité, un service, inclus dans les versions de Microsoft Windows Server. C'est une architecture logique centralisée, qui permet à un utilisateur de se connecter sur un ordinateur distant utilisant Microsoft Terminal Services.

Il utilise le « Remote Desktop Protocol » pour permettre aux utilisateurs l'affichage des données et fonctionnalités sur le « Terminal Léger » ainsi que la communication des périphériques.

Sur le server du SISR de la CDC, la version en service trouve son environnement machine de fonctionnement sous un Microsoft Windows

2008 R2, une version obsolète n'ayant plus aucun de support de mise à jour et de correctif Microsoft. C'est une version « abandonnée » eu égard à l'évolution constante des technologies. C'est une faille importante de sécurité du SISR de la CDC.

Il est alors utile de faire un choix technico-financier important de sécurité :
- soit déplacer les services en déployant une version système récente et durable sur environ 10 ans,
- soit supprimer ce serveur, la machine en Windows 2008 R2 n'ayant plus de support Microsoft) Faille de sécurité.

Il est à noter qu'au sein de la CDC, le service RDS est encore utilisé par quelques personnes pour accès à l'application DEFI.

Toutefois, nous devons voir avec l'éditeur afin d'être en client-serveur si possible.
Les performances du lien internet, de la connexion externe, irrigant la CDC sont, pour le moment, trop faibles, ce qui constitue un frein au déploiement de cette solution.

3.3.2.4.6 - SRV (VM) Une machine virtuelle, ou « Virtual Machine », est « le client » créé dans un environnement informatique, ici le serveur de la CDC qui est « l'hôte ». Plusieurs machines virtuelles peuvent coexister sur un seul hôte.

L'équipe externe de MSI2000 à effectuer des mises à jour serveur concernant la mise à jour des services de Gestion des Machines Virtuelles avec le module Hyper-V. Dans la situation actuelle, il est difficile voire impossible de faire mieux pour développer ce service, cette fonctionnalité du serveur. Pour cela il faudra investir lors du développement des moyens du SISR pour acquérir les solutions physiques permettant d'aller plus avant. Plus de RAM, de puissance de calcul processeur et de stockage mémoire en volumes de disques seront nécessaires pour développer les capacités de services.

3.3.2.4.7 - WSBS pour Windows Small Business Server, autrement nommé SBS (Small Business Server) en sa version 2008, est une solution logicielle « Windows Server » de Microsoft, préconfigurée, légère et permettant la mise en réseau des PC, le partage de fichiers et imprimantes, la sauvegarde automatique des données et l'accès à une messagerie et des outils collaboratifs jusqu'à 75 postes.

Cette solution a été déployée au sein du SISR de la CDC en fonction de son évolution dans le temps et dans son histoire. Cette solution est aujourd'hui dépassée par son obsolescence.
Cet aspect du SISR de la CDC nécessite un nettoyage du SBS.

3.3.2.4.8 - AD - Windows Active Directory - WAD
Au sein des solutions logiques, du serveur de la CDC et du SISR plus largement, il existe un service nommé AD pour Active Directory.

L'Active Directory est une fonctionnalité Microsoft, un service d'annuaire installé sur les versions de système d'exploitation type « Microsoft Windows Server » à partir de la version 2000 et inclus sur les versions 2003, 2008, 2012 et 2016.

3.3.2.4.8.1 - **L'Active Directory (AD) présent actuellement au sein du SISR en son serveur résulte d'une migration depuis SBS 2008.** Par conséquent, beaucoup d'entrées sont à ce jour obsolètes.

Ceci constitue un risque de disfonctionnement important et crée des « risques» supplémentaires en termes de sécurité. Les administrateurs externes en ont déjà entamé une restructuration partielle, mais il reste beaucoup de travail sur ce sujet.

3.3.2.4.8.2 - La stratégie des mots de passe utilisateur en place actuellement au sein de la CDC et donnant les accès à chaque intervenant, n'est pas conforme à la RGDP. Elle doit faire l'objet d'adaptations pour être en conformité RGPD.

De plus, dans l'usage quotidien des comptes utilisateurs, il m'a été donné de constater quasiment tous les jours que les usagers entrent une confidentialité et une gestion des mots de passe qui ne fait l'objet d'aucune stratégie, d'aucune préconisation, ni aucune sécurisation ou confidentialité.

Pire, il m'a été donné de constater à de multiples reprises, une « très présente harmonisation » des mots de passe d'accès aux comptes et sessions utilisateur et une circulation de ceux-ci complètement anarchique.

En la matière, il est urgent de changer les habitudes, de clarifier les procédures et les usages.

3.3.2.4.9 - Microsoft Exchange
- service de messagerie professionnelle sécurisée

Au sein du SISR de la CDC, cette solution est déployée de longue date et présente une longue histoire, un lourd passif d'intervention.

Il est à noter que les administrateurs externes ont procédé au renforcement du serveur EXCHANGE :
- par la mise à jour du service.

- par l'apport de nouveaux disques ajoutés pour ne plus provoquer de problèmes dus au remplissage jusqu'à saturation des disques durs de stockage, dans la ligne droite du REx (retour d'expérience) des événements débouchant au plantage système courant début 2021 et des difficultés entrainées au cours des mois suivants.

- par le dédoublement des bases de données AGENTS et ELUS pour garantir des bases saines.

- par l'installation de certificats officiels d'authentification et de sécurité. Il est à noter que la mise en place des certificats de sécurité pour délivrer le service de liaison sous Protocol sécurisé HTTPS a été effectué par les administrateurs externes suite aux événements alors qu'ils avaient averti depuis un très long moment des difficultés qui se profilaient et qu'ils n'avaient eu aucun retour ni aucune autorisation d'acquisition.

Aussi, au bilan, les actions de protection vouées à la sauvegarde et à la messagerie ont été réalisées, de même que les CU (Cumulative Updates) afin de rester à jour (depuis la version CU 3).

Mais il est impératif de penser au développement de ce service, de cette solution, et de ne rien considérer comme étant soldé. Les capacité utiles et dimensionnées juste à propos sont à moderniser par l'apport de nouveaux matériels et sont à mettre à niveau régulièrement, leur volumes et importance d'usages, de stockage, allant constamment et logiquement de façon croissante.

3.3.2.4.10 - Gestion des dossiers / accès global FILES

Le SISR de la CDC présente une gestion des dossiers et de l'ensemble de sa data inadapté à son fonctionnement et présentant des risques majeurs de sécurité, de confidentialité et d'intégrité.

Une restructuration importante du système et de la stratégie d'administration doit être étudiée et mise en place concernant tous les aspects d'usages et en priorité concernant les droits d'accès, de partage, d'écriture et de lecture des dossiers et fichiers.

Une solution d'enregistrement, de supervision, de traçabilité et d'horodatage doit impérativement être mise en place pour garantir, identifier et sécuriser l'ensemble des fichiers et de la data du SISR, y compris sur les aspects concernant l'activité des personnels au quotidien, sur et via le SISR.

Actuellement, tout le monde à accès à tout, en tout temps et tout lieu, y compris vers et sur les fichiers les plus sensibles, confidentiels et stratégiques.

Aucun aspect ne répond a minima aux exigences minimum acceptables d'exploitation face à la RGPD.

A ce jour, seuls les dossiers et de la data des personnels, hébergés, stockés, sur le lecteur « U:\ », ont été remaniés et protégés en accès par les administrateurs externes.

L'ensemble de TOUTES les autres données restent en accès non contrôlé.

3.3.2.4.11 - Solution logicielle applicative « Cosoluce »

Cosoluce est une solution logicielle applicative dédiée à la gestion administrative financière des collectivités locales.

Cette solution logique est hébergée sur une solution physique interne au SISR de la CDC. Il y a besoin d'un nettoyage du serveur Cosoluce prenant en compte la présence de sauvegarde Cosoluce local d'anciennes versions nécessitant l'installation de la Version 6 de Cosoluce entrainant le besoin de prendre en compte la nécessité d'une optimisation du système support.

Il est à noter que les solutions « Cosoluce » ne seront plus maintenues à jours, ni patchées, en ce qui concerne les postes actuellement en service au sein du SISR de la CDC dont le système d'exploitation demeure sous Windows Seven (Win7).

Il est à noter que je suis intervenu pratiquement tous les deux jours sur des problèmes logiques et matériels liés à Cosoluce mais dont la source est très largement et majoritairement lié à l'obsolescence et à la dégradation du SISR de la CDC jusqu'au point de blocage ne permettant plus aux agents d'effecteur leur travail.

3.3.2.4.12 - WSUS - Windows Server Update Services

Ce service Microsoft System, permet aux administrateurs de déployer les dernières mises à jour de produits Microsoft par lien direct avec les services authentifiés de Microsoft. Ce service est actuellement non fonctionnel au sein du SISR de la CDC.

Cela constitue une faille MAJEURE de sécurité et de maintien dans le bon fonctionnement des solutions informatiques déployées en sein du SISR.

Le point d'origine de ce problème résulte et découle directement de la migration depuis le SBS (Windows Small Business Server) du SISR de la CDC ci-dessus évoqué et obsolète.

L'ensemble des postes du domaine est bloqué en termes de mise à jour (MàJ) car le service n'est pas opérationnel.

Il y a nécessité d'effectuer une suppression, suivie d'une recréation de ce service vital au bon fonctionnement du SISR. Les postes concernés sont bloqués depuis des mises à jour datée de 2018, soit plusieurs années de décalage par rapport aux dates actuelles. Les administrateurs externes ont identifié et remonté des actions à mener : elles sont en attentes parce qu'elles ne sont pas forcément possibles immédiatement à cause de l'état général extrêmes difficile du SISR de la CDC. Rien ne peut leur être reproché.

Précipitée et anarchique dans le temps, l'évolution du SISR de la CDC, a entrainé une accumulation de difficultés aux conséquences lourdes et extrêmement mal vécues, qui caractérisent les principales causes de dégradations et facteurs de perte de qualité, des rôles et services de serveur.

Faute de mieux, certains postes ont été mis à jour manuellement en direct lorsque cela fut possible, ce qui n'est pas forcément le cas sur les postes dont les versions d'OS (Système d'Exploitation) sont obsolètes, abandonnées depuis parfois plusieurs années.

3.3.2.4.13 - OS - Operating System - les systèmes d'exploitation en service

Au sein de la CDC, le SISR présente une disparité importante et dangereuse dans les versions des systèmes d'exploitation installés et en fonction sur les machines individuelles en service.

Un système d'exploitation (OS) est un ensemble de programmes qui dirige l'utilisation des ressources d'un ordinateur par des logiciels applicatifs, c'est l'âme d'une machine.

L'OS reçoit et traite les demandes d'utilisation issues et émises depuis et par les ressources de la machine, de l'ordinateur, en tout domaine y compris les ressources de stockage des mémoires comme l'accès à la mémoire vive (RAM), aux disques durs (DDR, SSD, HSSD, HDDR,etc…), les ressources de calcul du processeur central (unité centrale), les ressources de communication vers des périphériques, parfois en ayant recours aux ressources de calcul, au GPU (Graphics Processing Unit) par exemple, ou tout autre carte d'extension des capacités matérielles et logiques, ou via le réseau de la part des logiciels applicatifs. Le système d'exploitation gère les demandes ainsi que les ressources nécessaires évitant les interférences entre les logiciels.

Les versions disparates, obsolètes et non maintenues au sein du SISR, en particulier les machines sous système d'exploitation individuel Windows 7 pro sont une faille majeure de sécurité et de cohérence du SISR.

De plus, Windows Seven (Win7pro) n'est plus supporté par Microsoft, créant donc potentiellement des failles de sécurité. Certains postes ont été mis à jour vers Windows 10 mais nécessitent un upgrade (une monté en version et capacités) mémoire pour une effectivité, une stabilité, une cohérence de sécurité et un confort d'usage.
Par exemple Windows 10 dans ses versions actuelles, requiert 8Go de RAM a minima).

4 - Mon projet par une simulation évolutive - Etude prospective non exhaustive

Illustration de la Topologie du Système d'Information

Ce schéma de principe est la capture de la maquette de simulation que j'ai réalisé dans le cadre de mon PPE pour investiguer, tester et proposer des evolutions face aux problématiques soulevées précédement.

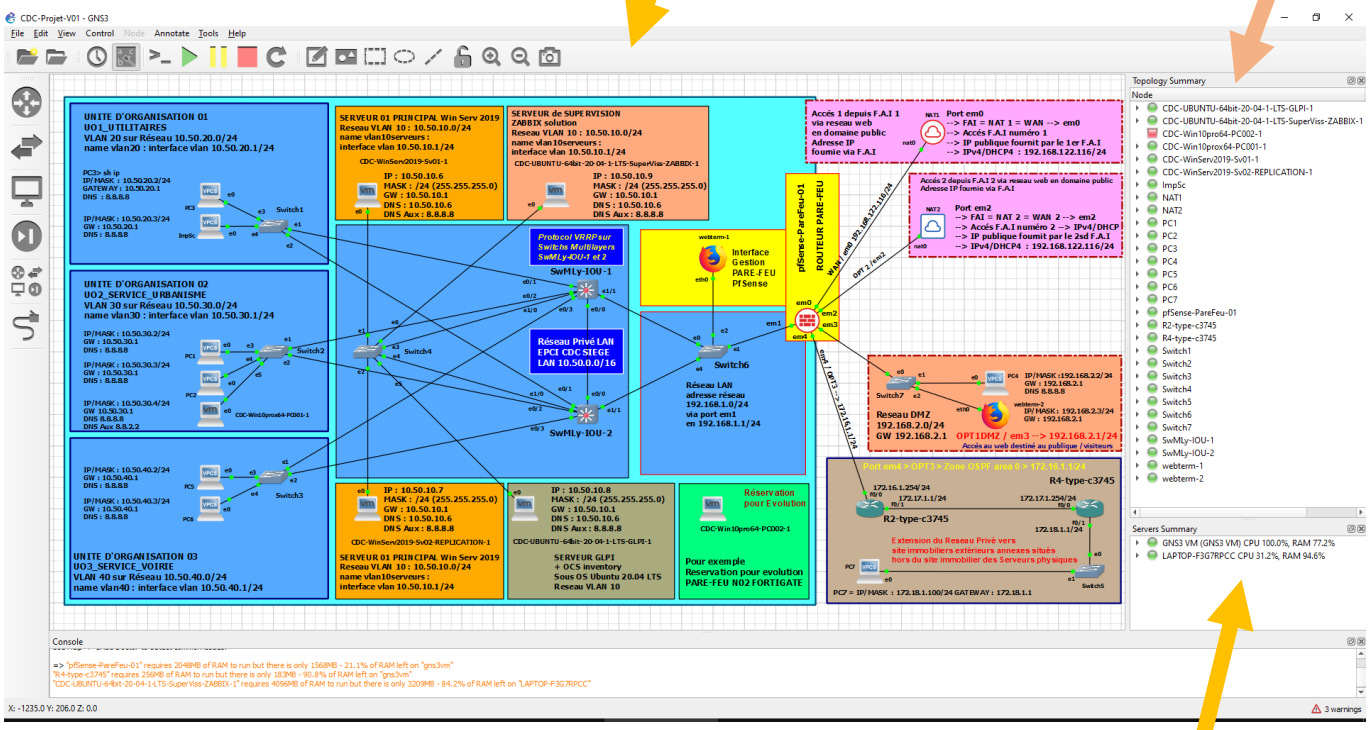
Exercice realisé sous logiciel GNS3 (Graphical Network Simulator) : logiciel libre permettant l'émulation ou la simulation de réseaux informatiques.

En arrière plan de GNS3, et synchronisé avec, je me suis appuyé sur le logiciel VMware, plateforme qui permet d'adopter la virtualisation des serveurs et de multiples types de machines informatiques.

Contexte visiuel de simulation (capture d'écran) / Plateforme de simulation

Espace de simulation
Maquette interactive du
Système d'information & infrastructure réseau

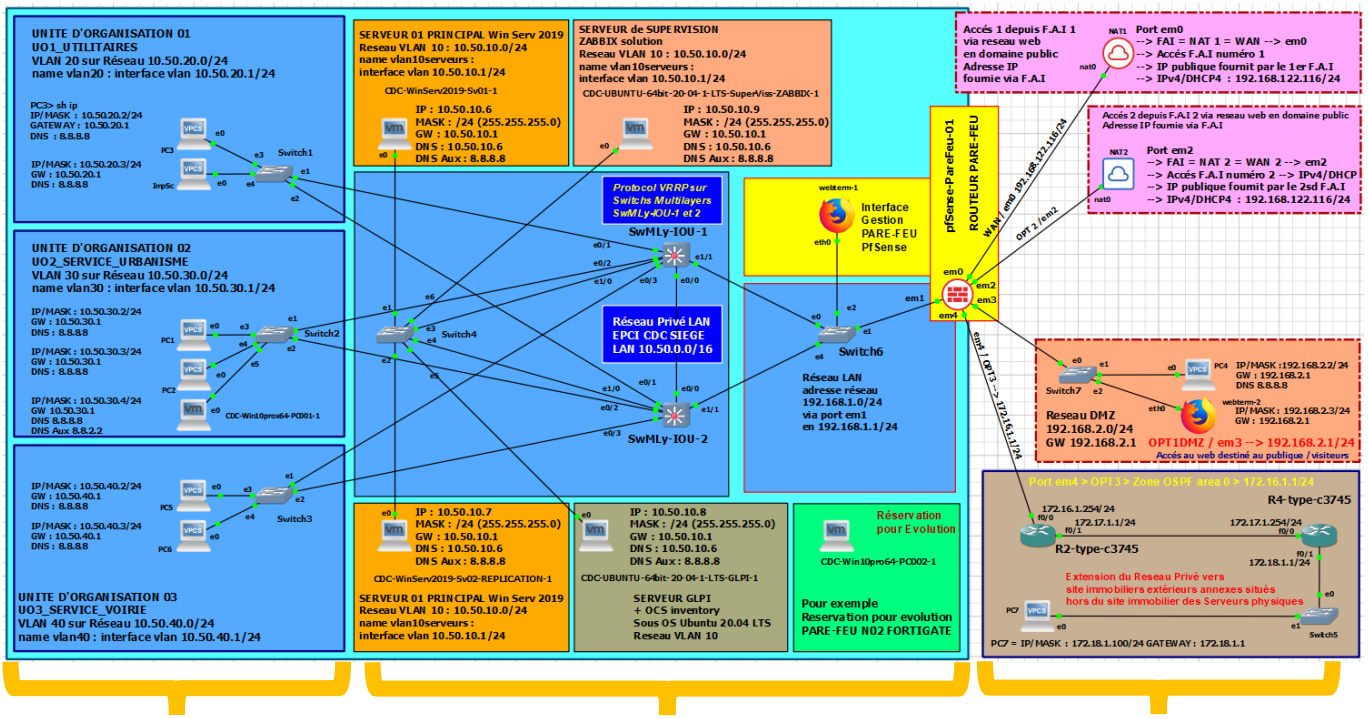
Fenêtre indicative des
activations & désactivations
des solutions physiques & logiques simulées



Fenêtre d'indication des niveaux d'utilisation des support physiques et logiques :

- **ligne 1 / GNS3 VM : indice de charge CPU & RAM de la solution logique de simulation**
- **ligne 2 Machine support : indice de charge CPU & RAM de la machine servant support physique de simulation**

4.1 - Topologie du système d'information - notice explicative



Secteur de Simulation des services internes de l'entité projet

Secteur de Simulation des solutions logico-physiques d'administration & de délivrance des services informatiques à l'organisation en pleine propriété de l'entité projet

Secteur de Simulation Des services externes et de délivrance des services hors site physiques des serveurs

4.1.1 - Serveur Pare-Feu

1 - Pare-feu Principal

Le pare-feu est un dispositif qui protège un système informatique connecté à Internet des tentatives d'intrusion qui pourraient en provenir. Ce dispositif est également nommé firewall.

C'est avant tout un outil de protection informatique matériel et/ou logiciel (les deux réunis sont nommés « solution pare-feu ») conçu pour protéger les données d'un réseau, assurer la protection d'un ordinateur personnel, professionnel ou individuel relié à Internet par exemple, ou protection d'un réseau d'entreprise.

Un pare-feu, comme tout autre outil est une solution. Cette solution n'est pas infaillible, mais elle constitue le premier rempart, le premier filtrage, la première ligne de défense, une solution professionnelle solide, une mesure de base, une mesure incontournable de tout SISR digne de ce nom.

Le pare-feu protège la totalité du trafic réseau et a la capacité d'identifier et de bloquer le trafic indésirable. Étant donné que, de nos jours, la plupart des ordinateurs sont connectés à Internet, les attaquants ont de nombreuses opportunités pour trouver des victimes.

Le pare feu est à l'image d'un aiguillage de voie, dirigé par l'administrateur qui le pilote et qui en est l'aiguilleur. Ce pare-feu est alors paramétré en fonction des besoins et objectifs

souhaités. Attention, le pare-feu a l'impérieuse nécessité d'être l'objet de mise à jour et d'une supervision attentionnée et régulière.

Un pare-feu fait souvent office de routeur et permet ainsi d'isoler le réseau en plusieurs zones de sécurité appelées zones démilitarisées ou DMZ.

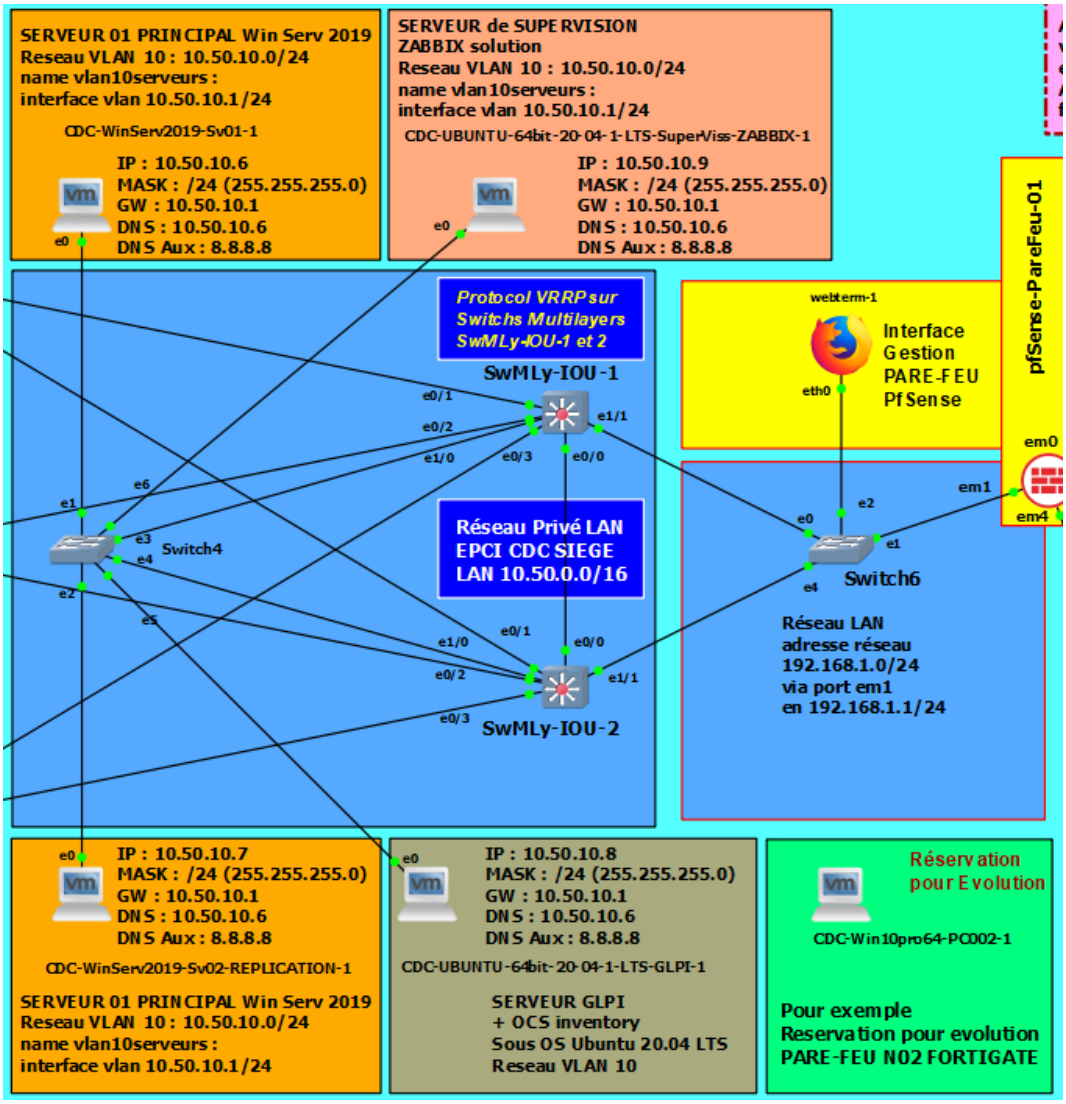
Ces zones sont séparées suivant le niveau de confiance qu'on leur porte. Enfin, le pare-feu est également souvent situé à l'extrémité de tunnel IPsec ou TLS.

Le pare feu (voir schéma de principe ci-en amont) se situe à la frontière du domaine public et du domaine privé du SISR de l'entité concernée, c'est-à-dire à l'exact interconnexion entre l'accès fourni par le F.A.I. (en amont) et le réseau privé du SISR ~~privé~~ (en aval).

Les solutions s'étalent sur une gamme de prix et des rapports qualité/prestation/prix très vastes pouvant (en généralité) s'étendre de 400 à 12000 euros.

Pour notre projet ici concerné, en posant un regard pragmatique sur les réalités et donc les contraintes de la CDC, je peux poser un estimatif prévisionnel de 4000.00 euros HT pour une solution proportionnée aux moyens et dimensions de l'infrastructure de la CDC avec une solution de type « Solution Logique et Physique » réunies mais sur une machine indépendante des serveurs : une solution autonome.

Concernant notre projet, je m'oriente vers une solution (pour exemple) Stormshield SN710 Pare-feu matériel UTM permettant 150 connexions VPN simultanées et disposant de 8 ports 10/100/1000 Mbit/s, etc… 3800 euros HT



4.1.2 - Serveur de supervision

Le serveur de supervision est une solution logique associée à une solution physique.

La supervision du SISR est le processus qui permet d'obtenir une visibilité sur l'activité de l'ensemble du système d'information, machine par machine, serveur par serveur, que ces équipement et solutions soient physiques ou virtuels.

Cette solution permet, via une machine, dont je fais le choix qu'elle soit spécifique et spécifiquement dédiée, réalisée sur mesure en fonction des besoins nécessaires, va permettre et consister à surveiller l'ensemble des comportements des processus et applications présentes au sein de l'infrastructure.

La supervision va dépendre de l'activité de l'entreprise, ici de l'établissement public, mais aussi de son besoin. On trouve rarement un même type de supervision d'une entreprise à l'autre. Elle est spécifique.

Concernant notre projet, je m'oriente vers une solution pour un somme de 3000 euros H.T pour une solution adaptée au besoin de la CDC, pour une machine indépendante et sa suite logique.

4.1.3 - Serveur Principal

1 - Serveur Principal

Le serveur est une machine spécifique, réalisée sur mesure en fonction des besoins nécessaires, des besoins de destination, constitués de différents éléments :

- à la fois matériel au sens physique du terme que l'on nomme Hardware
- et à la fois numérique au sens applicatif et logiciel du terme que l'on nomme Software.

Cet ensemble constitue le serveur auquel nous venons connecter d'autres équipements, machines et périphériques divers. C'est un ensemble technique évolutif, un assemblage d'équipements mis en corrélation avec des logiciels et un réseau de communication qui constitue une machine au cœur d'un système dit Système d'Information et Système Réseau (SISR).

Professionnellement, on considère qu'un serveur offre des services. Ces services sont extrêmes variés, variables, paramétrables, personnalisables, etc… tout comme la nature des services, qu'ils soient des services calcules, des services graphiques, audios, vidéos, multimédias, de données (data), en dur (c'est-à-dire directement hébergés, stockés, utilisés dessus) ou déportés, décentralisés, à distance, etc… en communicant, vers et avec d'autres machines.

Dans tous les cas, un serveur est un élément central, vital du système d'information et du système réseau qui y est attenant et connecté, auquel le serveur qui offre ses et des services accessibles via un réseau de communication.

Cet ensemble, constituant le serveur, est une machine qui exécute des opérations suivant les requêtes effectuées par un autre ordinateur appelé « client ».

Le mot « client » est ici dans sa définition pure hors du contexte mercantile habituel. Le « client » est la machine (ordinateur ou autre équipement connecté) qui communique et fait appel au cœur du système d'information auquel il est connecté que l'on nomme « le serveur ».

Concernant notre projet ici exposé, après investigation, je peux poser un estimatif de coût prévisionnel pour un somme de 22000 euros H.T pour une solution adaptée au besoin de la CDC avec serveur Rack métal sous OS Windows Server 2022 (le minimum étant d'évoluer sous version 2019).

Pourquoi un OS sous Win Server 2022 Datacenter ?

Dans le projet que je vous propose, je me suis servi d'une version Microsoft Windows Sever 2019 Standard pour des raisons logiques d'adéquation physique avec les matériels dont je disposais au moment de mon exercice, ayant financé seul l'ensemble de mes moyens de travail, puis pour des raisons de péréquation avec le programme d'enseignement suivi.

De plus, sorti très discrètement le 18 août 2021, Win Serv 2022 Datacenter, était disponible dans des limites de temps qui ne correspondait pas aux nécessités temporelles de notre projet ici présenté.

Il existe trois variantes :

- Microsoft Windows Server 2022 Standard.
- Microsoft Windows Server 2022 Datacenter.
- Microsoft Windows Server 2022 Datacenter : édition Azure.

Dans tous les cas, la version choisie devra être une version LTSC (Long Term Servicing Channel).

En effet, que cette version fasse partie du canal de service à long terme (LTSC - Long Term Servicing Channel) de Microsoft Windows est important car cela signifie que les entreprises peuvent bénéficier de 10 ans de support, 5 ans de support standard et 5 ans de support étendu.

Win Server 2022 Datacenter se situe au milieu des choix possibles pour la version récente et la plus ajustée en termes professionnels aux besoins et obligations de la CDC. Mais il y a également une raison législative importante : l'obligation de territorialité des données d'un établissement public français.

En Effet, la CDC est une entité publique française et fait partie de l'échelon territorial eu égard aux lois de décentralisation de l'état. Il n'en demeure pas moins que la CDC est une entité constitutive de l'état Français et l'EPIC à obligation de stockage, d'usage et d'archivage sur le seul territoire national de l'Etat Français.

Ainsi, sur les trois versions disponibles, la première présente le risque d'un sous dimensionnement dès le départ d'usage, la dernière présente la caractéristique d'être sous version Azure, c'est-à-dire Microsoft Azure: Services de cloud computing, une version dédiée aux services plateforme de cloud computing complètement inadaptée à nos besoins car vouée à l'externalisation sur des solutions aux dimensions continentales et extraterritoriales au territoire national avec une mainmise totale de Microsoft sur le stockage, le traitement et l'usage, ce qui n'est pas acceptable en l'état de nos besoins et prérogatives de souveraineté.

La version Win Server 2022 Datacenter, permet de mieux gérer l'ensemble des services et d'opérer plus largement en termes de nombre d'utilisateurs c'est-à-dire en termes de comptes, de machines et de sessions opérées.

Cette version dispose également de nouvelles fonctionnalités dont les anciennes versions ne disposent pas (cqfd : ce qui est logique puisque les technologies progressent, la délivrance et les possibilités liées progressent également).

Windows Server est une gamme de systèmes d'exploitation de serveur.
Les serveurs sont des systèmes conçus pour envoyer, stocker et recevoir des données vers d'autres ordinateurs. Windows Server 2022 a plusieurs nouvelles fonctionnalités. Selon Microsoft, les utilisateurs de Windows Server 2022 peuvent s'attendre aux nouvelles fonctionnalités suivantes :

- Protection multicouche avancée
- Serveurs centraux sécurisés, protection contre les attaques pour protéger les données et les informations

Les « serveurs sécurisés » reposent sur 3 piliers :

- la sécurité simple
- la sécurité avancé
- et la défense préventive.

Windows Server 2022 utilise TLS 1.3, un protocole bien connu mais dans sa dernière version, permettant une connectivité sécurisée.

TLS est le protocole de sécurité le plus récent et le plus largement utilisé.
TLS 1.3 crypte les données pour assurer une communication sécurisée entre deux points. Autre point, le client DNS dans Windows Server 2022 prend désormais en charge DNS-over-HTTPS (DoH).

Windows Server 2022 Datacenter bénéficie des dernières améliorations de configuration via une interface du Centre d'Administration Windows également plus précise et améliorée.

En termes de sécurité avancée, les serveurs à cœur sécurisé utilisent des capacités matérielles, micro logicielles et système d'exploitation pour protéger le système contre les menaces actuelles et celles qui viendront. Cela se fait via la racine de confiance matérielle, la sécurité du micrologiciel et la sécurité basée sur la virtualisation (VBS). La version ici choisie permet une meilleure délivrance de sécurité avancée.

Enfin au niveau de la Défense préemptive, Secured-core est un module, une fonctionnalité interne qui permet de mieux être défendu de manière proactive contre les attaquants qui tentent d'attaquer ou de perturber le système.

Autres précisions techniques concernant les différences entre les versions :

- L'édition standard de Windows Server 2022 est le package de base des trois. De nombreuses fonctionnalités sont disponibles, mais certaines options manquent, telles que l'option Storage Replica, Storages Spaces Direct et la prise en charge de Host Guardian Hyper-V. Il manque également des correctifs à chaud (application de mises à jour sans avoir à redémarrer tous les systèmes) et de mise en réseau définie par logiciel. Avec la licence Standard Windows Server 2022, vous avez la possibilité d'exécuter 2 machines virtuelles, avec un hôte Hyper-V par licence. L'édition standard contient les fonctions principales décrites dans la section sur les fonctionnalités, tels que les serveurs principaux sécurisés et le nouveau TLS. Ces précisions confirment le sous dimensionnement de cette version face aux besoins de la CDC.

- L'édition Datacenter de Windows Server 2022 est une avancée par rapport à l'édition standard. La mise en réseau définie par logiciel est incluse avec cette version de MS Windows Server 2022. L'édition Datacenter offre également une réplique de stockage illimitée et est également livrée avec la fonction Storage Spaces Direct.

  Hotpatching n'est pas inclus avec l'édition Datacenter. Microsoft a repensé le système de mise à jour et mis en place la technologie de "Hot Patching" qui permet l'application et l'activation immédiate de certains types de mises à jour sans avoir besoin d'un redémarrage. En bref, il s'agit d'une installation de mise à jour à chaud, mais techniquement, il est intéressant de conserver une installation

à froid pour garder la pleine vision de chaque mise à jour et de continuer des déploiements planifiés sous surveillance, le déploiement à chaud ayant tendance à « gommer » cette vigilance.

L'édition Datacenter permet, en termes de nombre de machines virtuelles, un nombre illimité de machines virtuelles et, tout comme l'édition standard, un hôte Hyper-V par licence. Cette édition (version) prend également en charge les machines virtuelles protégées.

- Microsoft Windows Server 2022 Datacenter : édition Azure.
L'édition Windows Server 2022 Datacenter : Azure est l'édition la plus fine des trois. Cette édition est prise en charge sur Azure et offre également de nombreuses fonctionnalités utiles que les autres éditions n'offrent pas. Par exemple, l'édition Azure propose SMB sur QUIC, Hotpatching et Extended Networking. Le Centre d'administration Windows a également été complété par les menus Azure suivants :

- Azure Hybrid Center
- Azure Kubernetes Services
- Azure Backup
- Azure File Sync
- Azure Monitor
- Azure Security Center

Comme l'édition Datacenter, cette édition est livrée avec un nombre illimité de machines virtuelles et un hôte Hyper-V par licence.

Mais comme précédemment évoqué, cette version est prioritairement conçue pour fonctionner avec les solutions externalisées et extraterritoriales de Microsoft.

Toutefois, laissons la porte ouverte en ce sens que cette version permet tout y compris ce que nous n'utiliserons pas… qui peut le plus peut le moins et non l'inverse…

4.1.3.1 - Les Serveurs de stockage en réseau dits Serveur NAS

- Serveur NAS principal et Serveur NAS de redondance

Les deux serveurs de stockage en réseau, également nommés « boîtiers de stockage en réseau » ou plus simplement « NAS » (de l'anglais Network Attached Storage), sont des machines constituant un serveur de fichiers autonome, relié au réseau interne privé de la CDC, dont la principale fonction est le stockage de données en un volume centralisé pour des clients réseau hétérogènes.

Les deux serveurs NAS déjà présents sont conservés et ne font pas l'objet de modifications spécifiques en ce projet.

Ils sont des machines spécifiques, réalisées sur mesure en fonctions des besoins nécessaires. Ils devront faire et feront l'objet d'une maintenance, d'une gestion et d'une mise à jour continue en fonction des évolutions du SISR et des besoins.

4.1.4 - Serveur de réplication du serveur principal

Un service de réplication se doit d'être intégré dans la stratégie de l'EPCI. Pour cela, un serveur de réplication se doit d'être mis en place. Ce serveur se doit d'être sécurisé et physiquement séparé du serveur principal.

Cette solution de réplication de serveur est destinée à permettre de sécuriser la production numérique de l'ensemble des domaines d'activités de la CDC. L'ensemble du processus de réplication informatique doit être automatisé par les administrateurs mais sous leur supervision permanente. La supervision humaine est ici également, indispensable.

Le fonctionnement du service de réplication de serveur consiste à créer un véritable clone de sécurisé permettant d'accroître la survivabilité des DATAS et le fonctionnent du SISR. Un serveur de réplication est à l'identique, le jumeau technique, logique et physique du serveur principal. Les mêmes applications sont installées sur le serveur source et sur le serveur cible.

Dans un premier temps, la mission d'un serveur de réplication est d'assurer la parfaite réplication primordiale des datas, c'est-à-dire les données les plus utiles, indispensables et stratégiques, puis, sont répliquées, les éléments définis comme secondaires.

Les réplications sont paramétrées selon des choix stratégiques établis par les acteurs du SISR, en corrélation avec les besoins face aux risques réels et potentiels relevés et envisagés ainsi que le degré de sécurité souhaité et les moyens disponibles.

La liaison physique de communication entre le serveur de réplication et le serveur principal se doit d'être réalisée via une connexion physique, filaire (Ethernet ou fibre) établie en direct, spécifiquement dédiée et protégée physiquement et logiquement. Elle se doit de faire l'objet d'une redondance afin de garantir en permanence la connexion et l'échange de données. Ces données répliquées se doivent d'être cryptées, compressées et transférées via le réseau interne.

En cas de défaillance du serveur source, la réplication de serveur effectue le basculement des services et ressources, soit de façon manuelle, soit d'une façon entièrement automatisée dont le paramétrage en amont a été préparé en lien avec les stratégies choisies et en tout état de cause toujours sous une supervision humaine qui peut reprendre la main.

Dès lors, les services, rôles et applications correspondantes sont lancées et, dans sa partie dite « de fichiers », le partage des dossiers est activé dans la foulée. La continuité, l'intégrité, la sécurité et la disponibilité sont assurées.

Selon l'application de réplication informatique choisie, un serveur cible peut aussi sécuriser plusieurs serveurs sources, ceci permettant d'économiser des ressources physiques, logiques et budgétaires.

Attention toutefois à ne pas oublier la séparation des usages domaine y compris physiquement. L'ensemble constitutif du serveur de réplication se doit d'être

alimenté électriquement via un dispositif d'alimentation, de régulation, de protection et d'ondulation électrique sécurisé et performant.

Concernant notre projet ici exposé, le coût de ce serveur de réplication sera nécessairement l'exact coût du premier et principal serveur, permettant ainsi de poser un estimatif de coût prévisionnel pour un somme de 22000 euros HT pour une solution adaptée au besoin de la CDC avec server Rack métal sous OS Windows Server 2022

4.1.5 - Au sein du SI, il y a le système réseau…

Le « Client » et le « Serveur » communiquent entre eux via un ensemble de dispositifs que l'on nomme « Système Réseau ». Plus précisément, le Système Réseau (SR) permet à l'ensemble des machines d'être interconnectées, par exemple de PC fixe à PC portable, de PC à imprimante, de PC à serveur dédié ou mutualisé, etc…
De façon complémentaire :

- un **« client »** désigne souvent la machine sur lequel est exécuté un logiciel, dit « programme client »,
- un **« serveur »**, est l'ensemble qui constitue l'ordinateur sur lequel sont exécutés les programmes, fonctionnalités et service dits « fonctionnalités serveur ».

Dans le cadre d'un fonctionnement en connexion et donc en liaison, avec un ou des réseaux, un serveur répond de façon automatique à des appels de services dits « requêtes » provenant d'autres dispositifs informatiques (machines dites « clients »), selon le principe dit client-serveur.

Le format des requêtes et des réponses obtenues est normalisé par des protocoles réseaux. Chaque service délivré peut être appelé, utilisé, exploité par le ou les clients qui mettent en œuvre le protocole propre à ce service, celui qui correspond précisément à ce service.

Les serveurs sont utilisés par les entreprises, les institutions et les opérateurs de télécommunication. Ils sont courants dans les centres de traitement de données (Datacenters) et sont au cœur des réseaux privés et réseaux Internet.

Dans le projet ici présenté, je fais le choix de mettre en œuvre deux routeurs multilayer de niveau 3 de marque Cisco pour permettre à la CDC de disposer d'une simulation et d'une proposition viable, durable et professionnelle adaptée, sans pour autant exclure d'éventuelles autres solutions.

C'est un sujet et une étape importante pour nous affranchir de la tutelle de la S.A. Orange qui, actuellement, gère également les aspects du SISR assurant une main mise complète sur le système.

Les deux dispositifs servant de routeurs dans ce projet, ici sous forme de deux Switchmultilayer de marque Cisco de niveau 3, en sont les cœurs et au cœur, des interconnexions du SISR.

Ils permettent de gérer ce que l'on nomme le routage, c'est-à-dire les actions qui consistent à faire passer des données à travers des routeurs, dans le but de les faire parvenir d'un point A à un point B. Ils sont les outils, les solutions, permettant de diriger les flux.

Un switch de niveau 3, également appelé commutateur de niveau 3, est un dispositif qui transmet le trafic (paquets et trames) en fonction des informations dites de couche 3 (principalement à travers l'adresse MAC).

Le switch multilayer de niveau 3 prend en charge toutes les fonctions de commutation et possède également des fonctionnalités pour le routage entre VLAN. Ces commutateurs sont conçus pour améliorer les performances de routage sur les grands réseaux locaux (LAN).

Sur un switch de niveau 3, la transmission de couche est effectuée par des ASICs (Application-Specific Integrated Circuit) spécialisés (celui-ci est plus rapide que les routeurs, mais manque généralement de certaines des fonctionnalités avancées des routeurs).

Contrairement aux routeurs, un switch de niveau 3 est moins susceptible de subir une latence de réseau puisque les paquets n'ont pas à effectuer des étapes supplémentaires à travers un routeur. Étant donné que ces switches remplissent des fonctions associées à la fois sur la couche 2 et couche 3 (mélange et assortiment de commutation de niveau 2/3), ils sont également appelés "switch multicouche", et certains switches 10GbE et switches Gigabit PoE correspondent à cette catégorie.

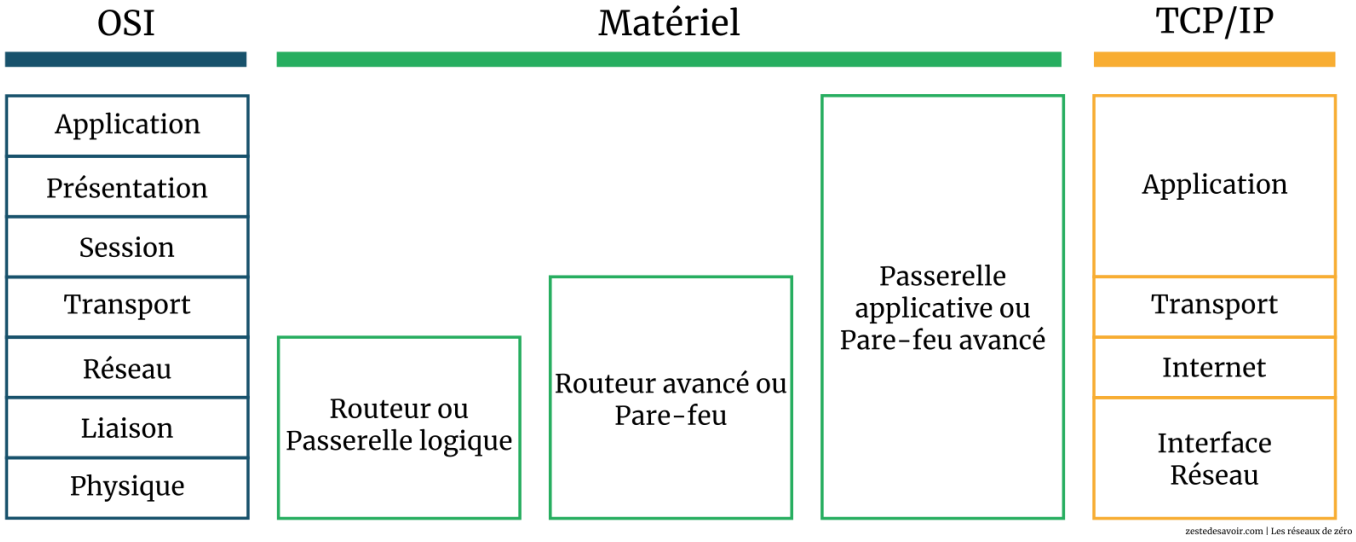
Le rôle de la couche réseau dite couche 3, du modèle OSI, qui correspond à la couche Internet du modèle TCP-IP, est responsable du routage. C'est par ailleurs la fonction principale de cette couche. Dans le modèle OSI à 7 couches (voir ci-dessous), la couche réseau est la couche 3. L'Internet Protocol (IP) est l'un des principaux protocoles utilisés au niveau de cette couche, avec plusieurs autres protocoles de routage, de tests et de chiffrement.

Une fois que la couche transport a assuré son rôle, les données sont envoyées à la couche réseau. Cette dernière se chargera d'ajouter toutes les informations en rapport avec le routage, dont notamment l'adresse IP du destinataire.

C'est la seule couche du modèle OSI qui utilise la connexion logique entre hôtes.
En fait, bien que cette couche ait pour rôle de déterminer le chemin physique à emprunter en se basant sur l'adresse IP du destinataire, les conditions du réseau et plusieurs autres facteurs, elle ne peut pas établir une connexion physique.

Son rôle se limite à la connexion logique.
Une fois qu'elle a ajouté à l'en-tête du paquet des informations qui lui sont spécifiques, ce dernier suit son cours et descend donc dans la couche 2, celle qui se chargera de la liaison des données. ;)

Illustration : le Matériel réseau à partir de la couche 3.



Précision sur ce qu'est un routeur :

- un routeur est un dispositif très répandu appliqué dans les réseaux domestiques et de petites entreprises.
- un routeur permet la communication entre les dispositifs auxquels il est connecté et le réseau internet.
- Un routeur peut transmettre le trafic (paquets) en fonction des informations de la couche 3, grâce à l'adresse IP, ce qui permet au réseau de fonctionner à travers différents protocoles.
- un routeur ou des routeurs servent également de première ligne de sécurité pour protéger le réseau contre toute attaque et intrusion.
- Un routeur analyse l'adresse de destination de la couche 3 de chaque paquet, et décide ensuite de la meilleure marche à suivre. Ce processus prend du temps et, par conséquent, chaque paquet subit un certain retard pour cette raison.

Dans notre projet, j'indique la présence de deux SWML de niveau 3 dont le coût prévisionnel peut être envisagé autour de 4000 euros HT par unité soit 8000 euros HT pour notre étude de cas.

4.1.5.1 - Mise en place d'un Protocole VRRP

Sur ces équipements, je fais le choix de mettre en place un protocole VRRP (Virtual Router Redundancy Protocol) qui est un protocole de sécurité de délivrance des services de routage et d'acheminement des communications par redondance.

Pour l'exercice, au sein de notre projet de développement de l'infrastructure, il y a plusieurs routeurs sous forme de switches multi layer de niveau 3, au nombre de deux dans cette simulation (mais qui peuvent être portés bien au-delà de ce nombre).

Cette multiplicité crée une redondance dite de « sécurité de délivrance des services de communication du SISR », créant les conditions d'une survivabilité accrue du réseau. Dans ce cas, le principe fait que si un matériel tombe en panne physique ou logique, son « double » prend automatiquement et quasi instantanément le relais de délivrance des services et permet l'intervention, le remplacement du matériel défectueux ou dégradé sans interruption de services.

Ainsi, le système en place sélectionne un ou plusieurs routeurs dans un groupe virtuel agissant en veille, amenant, en cas de défaillance, à ce que les routeurs dialoguent entre eux et, par le protocole VRRP, attribue dynamiquement la responsabilité d'un routeur actif à l'un des routeurs physiques d'un réseau local (LAN). Le système s'auto-attribue les rôles entre équipement sur le principe suivant --> routeur 01 tombe --> routeur 02 deux s'en aperçoit et prend le relais.

4.1.5.2 - Au sein du SI, au niveau du système réseau il y a une « relation » dite « client/serveur » :

La « relation client/serveur » est toujours un transit d'informations depuis une machine vers une autre machine. Ce transport d'informations se fait de multiples façons, par de multiples méthodes.

Mais à la base de toutes ces méthodes, il existe deux types d'architecture réseaux principales et dominantes, deux types de topologie via lesquelles un système d'information va communiquer via un système réseau :

1- La topologie physique
2- la topologie logique

1- La topologie physique (ainsi appelée architecture physique) définit la structure matérielle d'un réseau, c'est-à-dire, les câbles, les machines types ordinateurs, routeurs, switchs, etc… qui existent physiquement, que l'on peut toucher ou/et voir réellement. C'est l'expression concrète, visible, factuelle, d'un réseau. La topologie physique comprend elle-même, plusieurs types d'organisation : l'étoile (la plus utilisée), le bus, le mesh (topologie maillée), l'anneau, hybride, etc…

2- ***la topologie logique*** (architecture logique) qui se définit par le cœur, la programmation, la conception, l'administration numérique et virtuelle, qui fait fonctionner et commande la topographie physique.

Pour résumer :
- la topologie physique est constituée d'éléments matériels et concrets.
- la topologie physique est commandée par la topologie logique.
- La topologie logique, celle qui est virtuelle, numérique et conceptuelle est celle qui contient les « commandes » et qui définit ce qui doit se passer.

Dans tous les cas une architecture, une topologie, constitue un organigramme et une répartition, une organisation de fonctionnement… un réseau de communication.

Une topologie peut être composée, construite et mise en œuvre de diverses façons, par exemple :

- depuis un réseau public
vers un autre réseau public via d'autres réseaux publics
- depuis un réseau privé
vers un autre réseau privé via un réseau privé interne
- depuis un réseau privé
vers un autre réseau privé via un réseau privé externe
- depuis un réseau privé
vers un autre réseau privé via un réseau public externe
- depuis, via et vers un système réseau privé unitaire et/ou isolé dit « intranet »
- etc…

4.1.5.3 - Au sein du SI, le système réseau se décompose en 4 grandes catégories :

4.1.5.3.1 - Le réseau local dit réseau « LAN » :

L'acronyme « LAN », signifie en termes anglosaxons « Local Area Network ».
En français nous pouvons le traduire par **« réseau local » ou « réseau privé ».**

Le LAN est un réseau privé, interne, limité à une dimension géographique de site, c'est à dire, limité à un bâtiment, une zone d'activité précise, une salle, un étage, etc… Le réseau LAN se définit comme un **réseau interne, privatif, ultra localisé.**

Pour exemple :

- l'ensemble des ordinateurs et du réseau physique présent dans le bâtiment du siège social de la ComCom Campagne de Caux représentent des éléments d'une infrastructure de dimension typique d'un LAN.

- Ce type de réseau utilise généralement une configuration de type **« configuration au sein d'un domaine »,** ce domaine étant dit par défaut **« Domaine local ».**
C'est également ce que le langage commun nomme souvent comme étant un réseau privé interne dit **« intranet ».**

4.1.5.3.2 - le réseau local à transmission « sans fil » dit « WLAN » :
L'acronyme « WLAN » , signifie « Wireless Local Area Network » ou parfois « Wireless LAN ».
En Français « wire = câble », et « less = sans », donc « sans câble ».

Ce réseau est un ni plus ni moins qu'un « LAN » mais dont la différence réside en ce qu'il est exclusivement défini par un mode de transmission, de communication des informations de machine à machine par des moyens techniques dits **« sans fil »**.

Pour précision et exemple :

4.1.5.3.2.1 - le **Wi-Fi** est un mode de transmission « Wireless LAN », c'est-à-dire, sans câble, sans fil (« wire = câble », « less = sans »).

4.1.5.3.2.2 - un **WLAN public**, autrement nommé « hotspot Wi-Fi » est ainsi, en français, un point d'accès Wi-Fi public**.**
Il s'agit donc d'un réseau local sans fil public, d'où, WLAN public.

Au sein de la CDC :

- le « hotspot Wi-Fi » du local dédié à l'Espace France Services, en ses locaux de Goderville, est un point d'accès Wi-Fi public comme on en trouve dans des lieux publics. Là également, **c'est un réseau local sans fil public, donc un WLAN public.**

- le « hospot Wi-Fi » disponible à l'accueil de la CDC en son siège social, est lui également, un WLAN public (avec la particularité qu'il dépend de la connexion web et des services du SISR de la CDC en sa partie gérée par le F.A.I. et qu'**il serait bienvenu de reprendre en main par la création d'une DMZ pour des raisons de sécurité).**

4.1.5.3.3 - un WLAN privé :
Au sein de la CDC, le réseau WIFI privé, interne au siège social de la ComCom Campagne de Caux, dont l'usage est strictement réservé aux différents agents et personnels de l'EPCI, et qui, dans son rôle originel est uniquement réservé aux transmissions internes et privatives, est une forme de WLAN, un Wi-Fi, une liaison sans fil privative, donc un WLAN privé.

4.1.5.3.4 - le réseau local virtuel dit « VLAN »

Un VLAN signifie en termes anglo-saxons « Virtual Local Area Network ».
Nous pouvons traduire ce terme en Français par « Réseau Local Virtuel ».
C'est un type de réseau local :

- qui regroupe sur le même réseau physique

- un ensemble de machines informatiques

- qui fonctionnent sur des réseaux indépendants.

4.1.5.3.4.1 - Pour illustrer ceci, nous pouvons prendre l'exemple suivant :

--> imaginons plusieurs machines connectées sur le même switch et transitant, communiquant par un câble commun à toutes les machines et à tous les réseaux
--> mais, malgré tout, ces machines et réseaux ne doivent pas communiquer entre eux pour des raisons de sécurité et de confidentialité
--> une solution :
la mise en place d'un « réseau local virtuel » dit « VLAN » qui va permettre de disposer de plusieurs réseaux indépendants tout en se servant des mêmes câbles, des mêmes machines sur le principe « d'un câble unique pour plusieurs signaux distinctifs et séparés ».

Ainsi, plusieurs réseaux théoriques, donc virtuels et numériques, communiquent et transmettent de l'information, c'est-à-dire du signal, sur et via, un seul réseau physique.

Les réseaux virtuels dit « VLAN » améliorent la gestion du réseau en apportant plus de souplesse dans son administration et sa répartition logique, augmentent la sécurité du système d'information en imposant, entre autres exemples, le passage par un routeur pour la communication entre deux machines et donc l'utilisation de protocoles sécurisés.

Un VLAN permet d'optimiser l'usage des équipements de l'infrastructure du système d'information en optimisant l'usage de la bande passante, en séparant les flux des uns et des autres, en précisant, en ciblant la diffusion du trafic.

4.1.5.3.4.2 - 3 différents types de réseau locaux virtuels existent

4.1.5.3.4.2.1 - Les VLANs de niveau 1 :
--> les VLANs que l'on gère et que l'on affecte port par/vers port.

4.1.5.3.4.2.2 - les VLANs de niveau 2 :
--> les VLANs par adresse MAC, une adresse MAC étant l'adresse unique, l'identité unique détenue par une machine, son tatouage numérique unique.

4.1.5.3.4.2.3 - les VLANs de niveau 3 :
--> VLANs par adresse IP, que l'on gère et que l'on affecte par adresses IP par/vers d'autres adresses IP.

4.1.5.3.5 - le réseau étendu dit « WAN » :
L'acronyme « WAN », signifie en termes anglo-saxons « Wide Area Network ».
La traduction en français s'exprime sous « Réseau Etendu ».

Toutefois, il est à noter deux aspects possibles du concept de « WAN » :

4.1.5.3.5.1 - le WAN à grande échelle

C'est le réseau étendu dit « WAN » dans son aspect « internet », c'est-à-dire la vision « externe et globale » du réseau, dans la relation « client/serveur ».

Nous pouvons le préciser de façon suivante :

- un utilisateur via une machine (machine = client) va rechercher, faire appel, vers un site internet en utilisant un navigateur web.

- pour que ce navigateur puisse afficher le site web, il va effectuer une requête au serveur http qui est un serveur web (HTTPS si c'est un serveur web sécurisé).

- le serveur informatique destinataire de la requête du client va alors établir un dialogue, une relation « Serveur/Client et Client/Serveur » pour délivrer un service via le « Réseau Etendu » qu'est « internet ».

Ce type de relation et de fonctionnement constitue un des aspects du World Wide Web (le fameux www.https/... internet…) qui n'est qu'une face de ce qui est, ni plus ni moins un réseau étendu, **un WAN globalisé, interconnecté**, partie intégrante et constitutive du dispositif informatique (matériel et logiciel) qui offre des services de un à plusieurs dizaines de millions de clients (machines).

Les aspects, les services les plus courants, les plus communs en sont définit sous des milliers de formes dont, de façon non exhaustive :

- accès aux Systèmes d'Informations connectés au Systèmes Réseaux mondiaux constituant le « Système Mondial d'Interconnexion des Système d'Information » nommé « Internet » ou « la toile (d'araignée) mondiale »
- services de messageries différées, instantanées, courrier électronique
- usages, partages, stockages via des périphériques à distance
- gestion de l'authentification & du contrôle d'accès
- mise à disposition de logiciels, d'applications
- commerce électronique ou commerce en ligne
- constitution de base de données, de datas
- le gaming en ligne (jeu connecté)

- etc… la liste est immense, non finie, non terminée, en constante évolution…

De façon synthétique et résumée, le WAN, c'est le réseau que, principalement, gèrent et exploitent les acteurs du web, comme les hébergeurs, les agences et associations nationales et internationales et autorités de régulations de télécommunications et différentes entités telles que les F.A.I. (Fournisseur d'Accès à Internet).

4.1.4.3.5.2 - le « WAN réservé » ou « WAN privatif » à petite échelle
C'est le concept du « WAN » mais à l'échelle d'une entité clairement identifiée et sur un périmètre de cibles précisément circonscrites, par une liaison étendue mais privative ou privatisée.

En clair, il existe des cas où, à petite échelle, il y a besoin d'une infrastructure étendue, fonctionnant sur le même principe qu'un « WAN » mais sur une partie restreinte et réservée du réseau.

Cette « étendue d'infrastructure » ainsi utilisée, est alors « isolée », mais elle transite, circule, transmet et trouve sa source tout de même depuis le réseau extérieur, qu'il soit public, local, départemental, régional, national, étatique, supranational, international ou issue des liaisons et services internet mondial, etc…).

En quelque sorte, c'est une partie du « WAN » collectif que l'on paramètre logiquement (au sens logiciel du terme) pour devenir une partie « à usage réservé » mais qui fait physiquement partie du réseau global, du « WAN » étendu.

Nous créons alors une sorte de « Super VLAN » mais qui lui, s'applique et se considère sur le réseau étendu qu'est le « WAN ».

Pour exemple :

a --> Imaginons que le réseau LAN du siège social de la ComCom soit divisé en plusieurs réseaux LAN indépendants et privés pour des raison évidentes de confidentialité et de sécurité
b --> considérons que nous décidons arbitrairement que la répartition et la division de ce LAN, se fasse à hauteur d'un réseau privé par service, donc d'un LAN par service
c --> considérons uniquement pour la démonstration, 4 pôles/services = 4 LAN,
d --> Imaginons qu'il faille créer des possibilités de communication entre ces différents réseaux LAN

--> résultat / solution :
A --> pour cela nous allons mettre en relation, en communication, chaque **LAN** avec les autres, via des échangeurs de circulation de l'information que l'on **nomme « des switches » et des « routeurs »**
B --> chaque pôle dispose d'un switch pour connecter les machines du même pôle, donc 4 pôles = 4 switches
C --> on place un switch commun, qui reçoit la connexion du switch de chaque pôle
D --> le "raccordement ainsi effectué, d'un switch avec un autre et/ou ainsi de suite et/ou le branchement des 4 switch entre eux via un autre switch que nous pouvons considérer comme le switch de répartition commun, forme un réseau qui interconnecte les switches…

Au bilan, nous venons de mettre en place, nous venons de créer, la topologie physique d'un WAN, qui est l'association de plusieurs LAN entre eux, il permet d'obtenir un seul réseau virtuel en connectant plusieurs réseaux physiques distincts dans et sur plusieurs localisations géographiques différentes, plusieurs sites physiques séparés.

4.1.5.3.5.3 - Le « VPN » ou « Virtual Private Network

En français le VPN se traduit par « Réseau Privé Virtuel » ou « RPV ».
Le « WAN réservé » ou « WAN privatif » en version « simulée ».

Depuis que les infrastructures réseaux et ces acteurs sont en mesure de fournir des liaisons web, des liaisons Internet via un réseau WAN globalisé rapide, il existe des solutions technologiques et techniques nommé VPN, qui permettent de créer virtuellement un réseau privé virtuel.

C'est en quelque sorte une alternative, un autre moyen, pour disposer d'un « WAN réservé privatif » mais par un protocole de chiffrement indépendant et d'adressage par transit via des services cryptés et « délocalisés» et d'autres techniques, qui simulent le fonctionnement d'une infrastructure physique dédiée.

Les transmissions se font bien via la WAN étendu, mais le « trompent » pour donner l'impression que l'entité, l'entreprise, l'organisation, etc… dispose de son propre réseau privé alors qu'elles utilisent l'infrastructure commune, étendue et partagée du réseau public, collectif, support à internet.

Cette solution technique et logique, a toute sa raison d'être.
Toutefois, il faut être conscient qu'elle constitue une alternative.
Le « VPN » ne remplace en rien le WAN global collectif.
Le « VPN » repose physiquement dessus.
Le « VPN » confère à ses utilisateurs une solution palliative à usage et qualité de service moins performant à un taux de disponibilité inférieur qu'un véritable WAN physique.

4.1.5.3.5.4 - Mise en place d'un « VPN d'entreprise » propre à la CDC

Actuellement, la CDC utilise une solution VPN Business Everywhere de la S.A. Orange.

Cette solution est très coûteuse et rend la CDC et son SISR encore plus dépendants et aliénés à leur fournisseur d'accès, augmentant également les couts d'exploitations.

De plus, cette solution n'offre pas une meilleure protection que d'autres dont nous pourrions avoir la délivrance et il est de notoriété publique que la S.A. orange envisage de l'abandonner par suite d'un retour souvent négatif des usagers.

Il s'agit donc d'une solution qui sera rapidement obsolète et qui entraine des dépenses que nous ferions mieux d'utiliser pour développer notre

propre solution propriétaire.

La CDC doit utiliser ses propres matériels pour gagner son indépendance dans la ligne droite du présent projet. Pour cela, la CDC devra doter son SISR de son propre VPN, de plein usage et de pleine maîtrise, hébergé et géré sur sa propre infrastructure.

La mise en place d'une solution physique et logique de type « propriétaire » efficace est en lien avec le choix « 4.1.1 - serveur pare-feu » précédemment évoqué.

Pour rappel : je fais référence à la solution (pour exemple) Stormshield SN710 Pare-feu matériel UTM permettant 150 connexions VPN simultanées et disposant de 8 ports 10/100/1000 Mbit/s, etc… en estimatif pour un budget de 3800 euros HT.

5 - Topologie et plan d'adressage du SISR dans son évolution future face aux besoins de l'entité

5.1 - Etude pour proposition de Topologie et de plan d'adressage --> explications contextuelles et de principes

Afin de reprendre la maîtrise du SISR de la CDC, il faut établir une stratégie réseau incluant un « plan d'adressage réseau". Ce plan détermine :

1 - l'adresse IP du réseau, adresse principale de départ, base du réseau interne privé
2 - les adresses IP du sous-réseau qui en dépend et toutes ses ramifications.

C'est un peu comme le système physique du courrier postal, je m'explique :

- vous disposez d'une adresse d'expéditeur, ici l'IP de votre machine (exemple, le PC que vous utilisez)
- vous envoyer via les services postaux votre courrier ou colis en recommandé, pour cela vous utilisez le réseau postal de l'entreprise postale,
et donc ici, vous utilisez le réseau de transmission (quel que soit sa forme)
- donc dans le SISR, votre colis se nomme « des paquets » qui circulent dans le système d'information et l'infrastructure réseau :
    - le centre de tri oriente votre courrier ou colis, ici les serveurs, les routeurs, etc…
    - le facteur sait d'où le courrier vient grâce à l'adresse de l'expéditeur, ici l'adresse IP de la machine de l'expéditeur
    - le facteur sait où il doit délivrer le courrier ou le colis grâce à l'adresse postale du destinataire, ici, le SISR sait qu'il doit délivrer « les paquets de transmissions» vers l'IP du destinataire.

Et ainsi de suite, d'où le terme adressage réseau qui fonctionne, en résumé, à l'image de l'adressage postal.

Ce plan précise ainsi l'ensemble des adresses IP utilisées ou réservées et donc l'adresse de chacun des équipements, qu'ils soient des ordinateurs, unités centrales dédiées, stations de travail, imprimantes, scanners, copieurs, automates, machines-outils, etc…., qui composent le réseau de l'entité concernée.

Ce réseau IP, permet d'interconnecter les différents sites physiques et s'il y a, les réseaux de communication qui y sont reliés et prend en compte tout ce qui peut y être relié, connecté.

Etablir le plan d'adressage permet donc de définir pour chaque réseau physique (LAN et WAN)

une adresse de réseau IP permettant l'adressage, l'indentification et le bon déroulement, la bonne délivrance de l'information au sein du SISR.

Il est à noter que l'ensemble des adresses ici proposées sont, bien évidemment et forcément différentes de celles envisagées dans le cadre d'une véritable mise en œuvre, ceci pour des raisons évidentes de confidentialité, d'intégrité et de sécurité.

En cas de réalisation concrète de l'entièreté de ou des systèmes et stratégies d'adressage, de ou des topologies proposées en cet exercice et projet, le plan d'adressage, l'ensemble des adresses dédiées, seront à modifier, à adapter, à anonymiser, à ré-établir, à archiver et portés à l'usage exclusif, à la connaissance exclusive des seuls administrateurs du SISR et direction de l'établissement.

5.2 - Etude pour proposition de Topologie et de plan d'adressage - vision prospective

5.2.1 - Pour définir la ou les classes d'adresses que je choisi, je tiens compte :
- du nombre de réseaux physiques de votre réseau d'entreprise
- et du nombre de machines sur chacun de ces réseaux

Au sein de la CDC, il y a :
- des services existants
- et il y aura forcément des évolutions, des extensions, des créations… (même si elles ne sont pas encore connues ou identifiables à ce jour).

Ainsi, je m'oriente vers un dimensionnement qui me permet de rester évolutif tout en restant suffisamment restreint pour limiter ma surface d'attaque et de gestion à ce qui est indispensable, plus les marges que j'estime admettre dans mon rôle d'administrateur.

Je réunis l'ensemble de l'état-major technique, administratif et financier de la CDC, c'est-à-dire :
- La DGS - la Direction Générale des Services
- la DGA - la Direction Adjointe de chaque service (y compris le mien)
- la DF - la Direction Financière
- la DRH - la Direction des Ressources Humaines
- le SISR (moi-même), en qualité d'Administrateur Système et Réseau Interne
- les Administrateurs Système et réseaux prestataires extrêmes.

Ensemble :
- nous définissons, établissons prioritairement et très précisément
- nous redéfinissons entièrement et complétement le plan d'adressage en lien et les composantes des services et intervenants face au SISR :
- les rôles de chacun, son fonctionnement et administration
- les degrés, modalités et habilitations d'accès
- les degrés, modalités et habilitations d'intervention
- les degrés, modalités et habilitations de confidentialité
- les degrés, modalités et habilitations d'usages
- le recensement de tous les services
- le recensement et la pleine connaissance des tous les personnels
- établir qui a accès à quoi, quand, comment par où et quel moyen, par quelles conditions, etc… ?

- évaluer les besoins à mettre en place dans les domaines des procédures de sécurité, d'authentification, d'horodatage, de supervision, etc…
- recenser et recouper par tous les éléments possibles, comme en se servant de la GLPI ou autre, pour connaître, évaluer, le parc des machines asservies, connectées, en interaction avec le SISR, leurs caractéristiques, leurs localisations physiques, leurs destinations d'usage, etc…
- De-là, sur la base de l'ensemble des éléments collectés, vérifiés et corrélés, nous élaborons notre stratégie d'adressage correspondant à nos besoins présents et futurs.

5.2.2 - je prends en compte trois aspects et possibilités :

5.2.2.1 - Prospective 01 (P01) : La solution Globale

- je choisis des adresses réseaux IP totalement librement sur les plage et classe d'adresses conventionnelles de type « 1.0.0.0 », « 2.0.0.0 », « 3.0.0.0 », etc…
--> l'exercice consiste à ce que nous définissions alors, sur cette base, un plan d'adressage privé, mais sans s'assurer de l'unicité mondiale des adresses.

Cette solution n'est pas adaptée en l'état actuel du projet et au niveau actuel de l'exercice présenté. Il serait, à ce stade surdimensionné, de s'engager à un tel niveau de dimensionnement et d'intervention :

En effet, celle-ci, est, à l'échelle de mon simple projet, complétement et techniquement aberrant parce qu'il est évident que je connecte par nécessité, le réseau du SISR de la CDC au réseau à Internet.
Il y a donc de fortes chances de voir avec certitude que ces adresses sont déjà attribuées à d'autres sociétés, comme, par exemple, l'adresse 8.8.8.8, adresse qui, par exemple, correspond à l'un de serveurs DNS public de Google, souvent utilisée pour tester facilement et rapidement la connectivité d'un ordinateur à internet sans utiliser de résolution d'adresse, avec la commande "ping" ou sa variante TCP sur le port 53. C'est un grand classique car cette IP est facile à retenir et toujours active, c'est-à-dire "up".

Précisions techniques :
- le résultat du test ne sera cependant pertinent que sur un réseau domestique
- de plus, 8.8.8.8 est souvent utilisée pour pointer un autre serveur DNS public que celui mis à disposition par le FAI, 8.8.8.8 est souvent utilisée avec la commande "nslookup" ou "dig" pour vérifier un enregistrement DNS (public).
Autre exemple d'adresse de ce type, l'adresse 8.8.4.4, 4.4.4.4 etc…

Ainsi expliqué, je renforce ce choix logique, par le fait que dans ce cas, nous aurions de très sérieux soucis de routage vers Internet et nous serions dans l'obligation de corriger notre action par deux méthodes possibles en plaçant sur notre point d'entrée et de sortie depuis et vers Internet vous, un équipement de type routeur avec pare-feu (FireWall) qui va modifier, brutalement, arbitrairement et à la volée, nos adresses de machines pour les rendre compatibles avec le plan d'adressage Internet.

Cette méthode est appelée NAT : Network Adress Translation.
C'est une fonction de l'équipement mis en œuvre et cela consiste à réaliser une

translation d'adresse, ce qui est techniquement source de problèmes dans la maîtrise et la parfaite identification, administration du SISR.

5.2.2.2 - Prospective 02 (P02) : L'interaction du SISR vers et depuis internet La solution lorsque des services du SISR auront besoin de fournir des services informatiques et réseaux vers l'extérieur

Nous prévoyons l'interaction et interconnexion du SISR avec Internet et donc la façon dont il est et doit être compatible avec le plan d'adressage. Ceci dans le cas de figure où nous gérons directement, l'activité du SISR :

- entre les différents sites physiques distants et le siège social où se trouve les serveurs du SISR
- dans la fourniture de services internet dirigés vers l'extérieur, comme, par exemple, l'interconnexion avec interactions vers des mairies, des établissements, services et entités publiques départementales, régionales, étatiques, des services juridiques, les trésors publiques, les services de dématérialisation, les services d'archives, etc….

Dans cette perspective, l'exercice consiste à prendre en compte le fait que le SISR de la CDC, s'ouvre à offrir extérieurement des services numériques, des services d'information, des services d'interaction et interconnexion à des acteurs, individus, entité privées ou/et publiques.

Par cela, il faut considérer que nous serons alors en mesure de créer, mettre en place et en œuvre un ou des serveurs complémentaires pour offrir ces possibilités.

Mises en services, ces extension du SISR auront la faculté de créer des usages et services plus poussés tout en assurant la séparation des usages et service, facteur primordial en terme de cybersécurité, gage d'un meilleur niveau de sécurité, de confidentialité, d'intégrité, de disponibilité et de redondance des services.

Dans l'expectative d'une telle action, nous serons en mesure de définir un plan d'adressage conforme au plan d'adressage public, c'est-à-dire de demander aux organismes spécifiques NIC, AFNIC ou IAP (Internet Access Provider) des adresses IP publiques qui vous seront réservées, qui seront spécifiquement réservées au SISR de la CDC.

Ces adresses réseaux, nous permettrons de définir notre plan d'adressage interne vers les adresses IP de type IP V6 déjà en cours, dès le départ et y compris lors de notre évolution technologique programmée et budgétisée pour répondre au mieux aux conséquences dues à la pénurie d'adresses IP publiques de type IP V4.

Le SISR sera alors en mesure d'évoluer avec la redéfinition du protocole IP, une nouvelle version identifiée IP V6, qui propose un format d'adressage sur 16 octets extrêmement plus performante, le large, ouvrant le champ des possibilités d'adressages plus avant des possibilités de l'IP V4.

Actuellement cet aspect du SISR est toutefois partiellement présent, de façon embryonnaire, sans que l'entité en ait pleinement la conscience.

En tout état de cause, la CDC n'a aucune maîtrise sur ce sujet car tout passe par l'intermédiaire de son seul et unique F.A.I., ce qui est dommageable.

En effet, ce sujet crucial, concerne les liaisons établies :

- vers et entre les services hébergés physiquement au sein des édifices des différents sites de la CDC
- mais tous distants du bâtiment du siège de la CDC (exemple le « DOJO »)

Dans ces cas, le F.A.I. assure une liaison via ses propres services sans aucune possibilité d'intervention ou d'évolution maitrisée de la part de la CDC. La CDC est en situation de totale dépendance technique et financière avec son F.A.I.

5.2.2.3 - Prospective 03 (P03) :
Les adresses routables et la mise en place d'un adressage dits « adressage privé »

Cette solution est, pour la partie du SISR interne au siège social, une solution envisageable et connue. Elle consiste à utiliser des adresses dites non « routables ». Ce sont des adresses réseaux spécifiques qui ne sont et ne seront jamais utilisées sur Internet. Elles sont dites « adresses privées ». Elles garantissent que nous n'aurons pas de conflit d'adressage.

Ces adresses sont définies par une RFC spécifique, la RFC 1918, qui est une « Convention Technique Universelle » qui s'applique à tous, sous le titre de « Address Allocation for Private Internets », expression anglo-saxonne, qui se traduit en français par « Attribution d'adresses pour les Internet privés ».

Ces adresses ne sont pas routées sur Internet. C'est-à-dire qu'elles ne peuvent être qu'à usage « privé » et non public.

Ceci donne donc la possibilité d'adresser, de donner des adresses IP, donc de router en interne, sur un réseau privatif autrement appelé « un réseau privé ». Cette adressage interne peut donc être établi librement, et donc peut être « numéroté » librement avec les plages d'adresses privées prévues à cet effet et cadrées, bornées par la convention technique.

Par opposition aux adresses publiques d'Internet, ces adresses ne sont pas uniques, plusieurs réseaux pouvant utiliser les mêmes adresses, mais elle ne se connecteront jamais, ni ne se croiseront ou entreront en interaction ou conflit puisqu'elles sont sur des réseaux séparés, logiquement et physiquement.

Et si toutefois, deux réseaux internes, deux réseaux privés basés sur ces adressages IP V4 de type « adresses privées » venaient à être mis en communication et en fonction ensemble, la séparation des usages, la gestion et l'administration par routeurs et Vlan et la mise en place de protocoles associés, permettent de maintenir leur séparation et de gérer leurs interactions et compatibilités sans conflit d'adressage.

La RFC 1918, définit trois classes d'adresses, nommées « A », « B » et « C ». Pour chaque classe, il y a, par convention, un pool (autrement dit, une plage) d'adresses réservées pour l'utilisation de réseaux privés. Ces adresses ne sont pas routées sur internet.

L'usage de ces plages et donc de chacune des adresses qu'elles contiennent, est obligatoirement et exclusivement réservé à être utilisé sur, pour et au sein, d'un réseau local privé. Pas autre chose.

Les plages d'adresses réservées aux réseaux privés en IPv4 sont :

Classe	Préfixe	Plage IP	Nombre d'adresses
	adresse/masque de s-réseau	De l'adresse… --> jusqu'à l'adresse…	Nombre de possibilités
A	10.0.0.0/8	10.0.0.0 --> 10.255.255.255	$2exp^{32-8}$ = 16 777 216
B	172.16.0.0/12	172.16.0.0 --> 172.31.255.255	$2exp^{32-12}$ = 1 048 576
C	192.168.0.0/16	192.168.0.0 --> 192.168.255.255	2^{32-16} = 65 536

Ainsi, je vais orienter mon exercice au sein de ce projet par une administration interne mettant en œuvre l'adressage privé sur les plages suivantes :

Classe	Plage d'adresse
A	10.0.0.1 à 10.255.255.254
B	172.16.0.0 à 172.31.255.254
C	192.168.0.0 à 192.168.255.254

En effet, la première et la dernière adresse d'un adressage réseau ne sont jamais affectées.

Le nombre maximum d'adresses d'hôtes disponibles correspond à l'espace d'adressage du sous-réseau moins deux, parce que :

- la première adresse désigne le réseau
- la dernière est l'adresse de diffusion, en anglais, « Adresse de Broadcast », dirigée vers tous les hôtes du réseau.

Au sein de mon plan d'adressage, les adresses indiquées figureront sous le format dit « notation CIDR » qui est la convention d'écriture universelle, établie sous la forme, « Adresse / masque de sous réseau » ce qui donne pour exemple que j'auto détermine, ceci, pour un choix d'adresse type « 172.22.0.1/24 », dans ce cas :

- « 172.22.0.0 est l'adresse réseau
- « 172.22.0.1 » est l'adresse réseau privée
- « /24 » le masque de sous réseau il y a 24 bits qui le constituent le net ID

De plus, lorsque sur ce projet, je vais décider de déterminer et d'administrer mon réseau, j'y placerai des « VLANs » afin de mieux séparer les usages, cloisonner les réseaux, ce qui donnera, sur la base de mon exemple, ceci :

- Vlan 10 = 172.22.10.0
- dont la première machine sera la 172.22.10.1
- dont la dernière machine sera la 172.22.10.254

Et ainsi de suite…

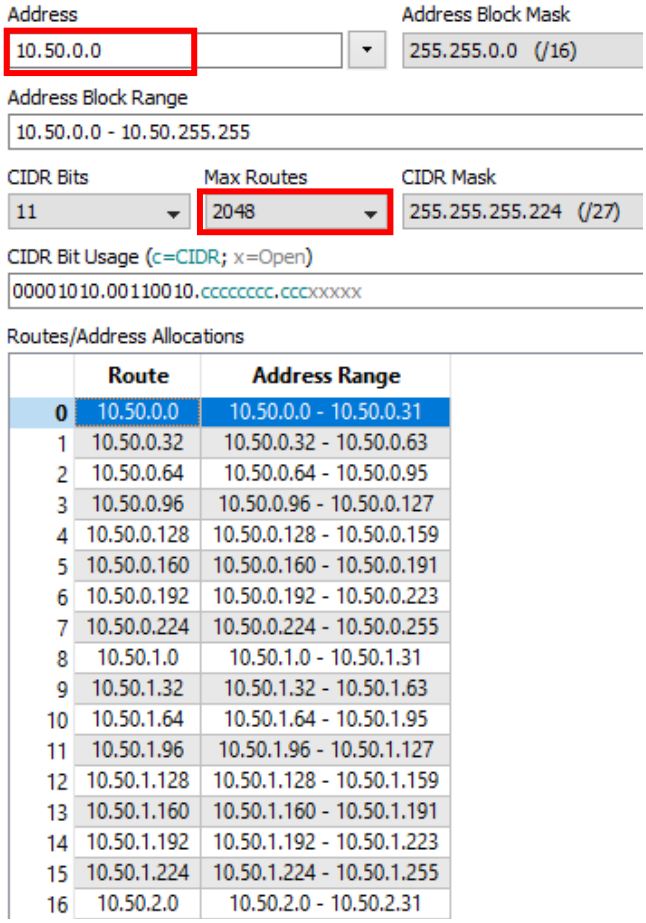
- Vlan 20 = 172.22.20.0
- dont la première machine sera la 172.22.20.1
- dont la dernière IP affectable sera la 172.22.20.254

Précision importante à signaler :
--> La limitation technique : une fois établi, ce plan d'adressage et « quasiment non modifiable ».

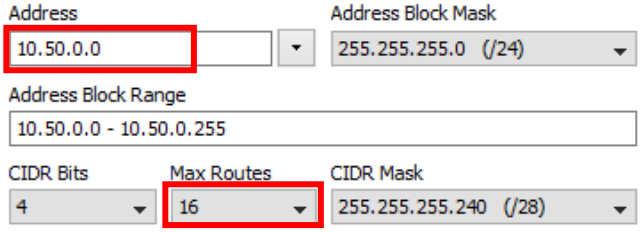
Pour exemple, concernant notre projet :

- 1/ voici deux **exemples** de répartition possible des adresses IP

- Rappel : Ce ne sont que des exemples non exhaustifs -



	Route	Address Range
0	10.50.0.0	10.50.0.0 - 10.50.0.31
1	10.50.0.32	10.50.0.32 - 10.50.0.63
2	10.50.0.64	10.50.0.64 - 10.50.0.95
3	10.50.0.96	10.50.0.96 - 10.50.0.127
4	10.50.0.128	10.50.0.128 - 10.50.0.159
5	10.50.0.160	10.50.0.160 - 10.50.0.191
6	10.50.0.192	10.50.0.192 - 10.50.0.223
7	10.50.0.224	10.50.0.224 - 10.50.0.255
8	10.50.1.0	10.50.1.0 - 10.50.1.31
9	10.50.1.32	10.50.1.32 - 10.50.1.63
10	10.50.1.64	10.50.1.64 - 10.50.1.95
11	10.50.1.96	10.50.1.96 - 10.50.1.127
12	10.50.1.128	10.50.1.128 - 10.50.1.159
13	10.50.1.160	10.50.1.160 - 10.50.1.191
14	10.50.1.192	10.50.1.192 - 10.50.1.223
15	10.50.1.224	10.50.1.224 - 10.50.1.255
16	10.50.2.0	10.50.2.0 - 10.50.2.31



	Route	Address Range
0	10.50.0.0	10.50.0.0 - 10.50.0.15
1	10.50.0.16	10.50.0.16 - 10.50.0.31
2	10.50.0.32	10.50.0.32 - 10.50.0.47
3	10.50.0.48	10.50.0.48 - 10.50.0.63
4	10.50.0.64	10.50.0.64 - 10.50.0.79
5	10.50.0.80	10.50.0.80 - 10.50.0.95
6	10.50.0.96	10.50.0.96 - 10.50.0.111
7	10.50.0.112	10.50.0.112 - 10.50.0.127
8	10.50.0.128	10.50.0.128 - 10.50.0.143
9	10.50.0.144	10.50.0.144 - 10.50.0.159
10	10.50.0.160	10.50.0.160 - 10.50.0.175
11	10.50.0.176	10.50.0.176 - 10.50.0.191
12	10.50.0.192	10.50.0.192 - 10.50.0.207
13	10.50.0.208	10.50.0.208 - 10.50.0.223
14	10.50.0.224	10.50.0.224 - 10.50.0.239
15	10.50.0.240	10.50.0.240 - 10.50.0.255

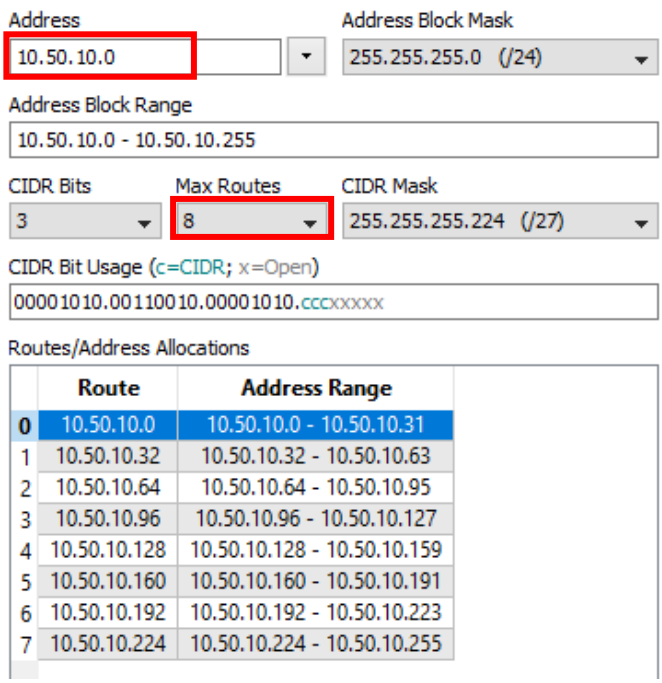
-2/ ou… deux exemples de déterminations possibles des Vlan(s)…

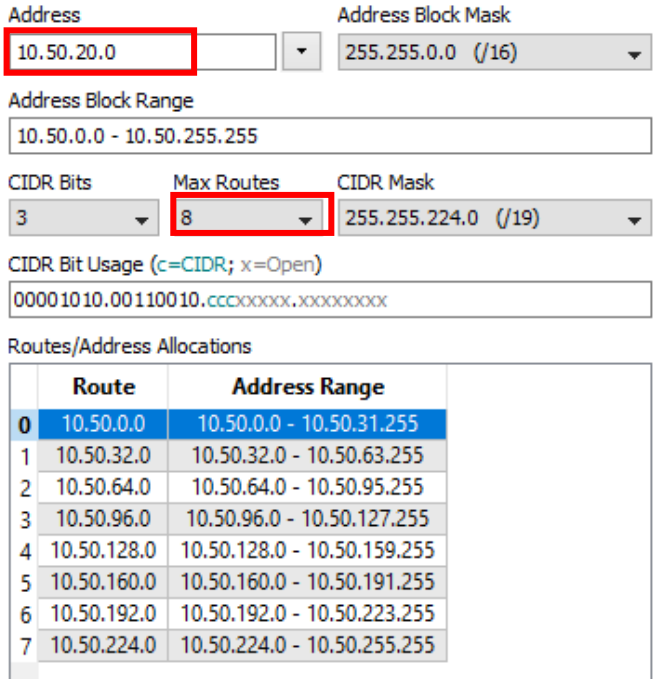
--> Le réseau privé de notre base réseau, est alors divisé (par exemple) en Vlan :

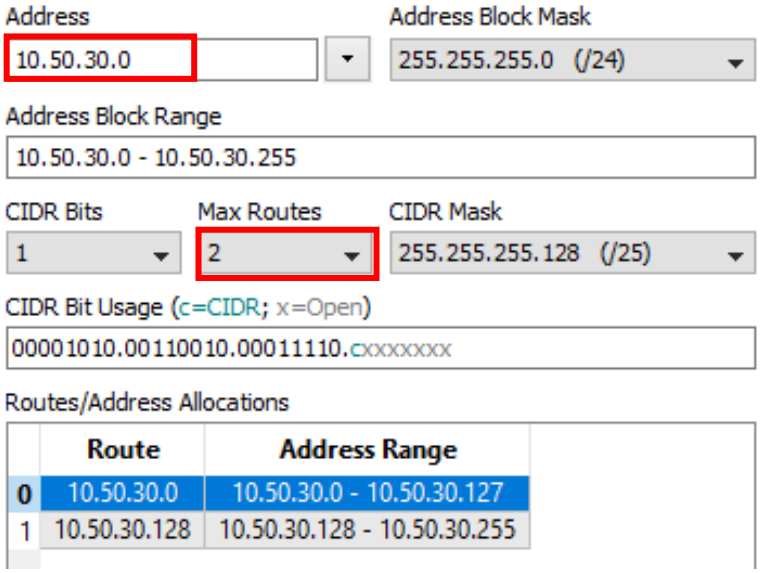
- Le vlan 10, déterminé par un adressage de type 10.50.10.0
- le Vlan 20, déterminé par un adressage de type 10.50.20.0
- le vlan 30, déterminé par un adressage de type 10.50.30.0
- Etc…

- Rappel : Ce ne sont que des exemples non exhaustifs -

Ces Vlan peuvent également faire l'objet d'une répartition encore plus sectorisée, en les répartissant plus avant, en section plus précise et restreinte et donc plus étroite et spécifique pour améliorer la séparation des réseaux et aller plus loin dans la séparation des usages et utilisateurs, voir les exemples ci-dessous :







Bibliographie et Webographie

1) MAES Jérôme, Debois François. La boîte à outils du chef de projet. DUNOD, 2021, 208p.

2) SPETH Christophe. La Matrice SWOT : Élaborer un plan stratégique pour votre entreprise. Books on Demand, Collection 50minutes.fr, 2015, 32p.

3) Textes de loi recherchés sur Légifrance – Le service public de la diffusion du droit [en ligne] : https://www.legifrance.gouv.fr , consulté en 2021-2022.

4) CNIL - Commission nationale de l'informatique et des libertés [en ligne] : https://www.cnil.fr, consultée en 2021-2022.

5) ANSSI - Agence nationale de la sécurité des systèmes d'information [en ligne] : https://www.ssi.gouv.fr, consultée en 2021-2022.

Lexique des acronymes utilisés :

(Organisés par ordre alphabétique)

CDC	Campagne de Caux
ComCom	Communauté de Communes
DEFI	
DGA	Direction .s Générale.s Adjointe.s
DGS	Direction Générale des Services
EPCI	Etablissement Public de Coopération Intercommunale
FAI	Fournisseur d'Accès à Internet
FSRM	File Server Resource Manager
GLPI	Gestion Libre du Parc Informatique
IP	Internet Protocol
ITSM	Information Technology Service Management
LAN	Local Area Network
MAC	Media Access Control
NAS	Network Attached Storage
OSI	Open Systems Interconnection
QUIC	Quick UDP Internet Connection
RDS	Radio Data System
RFC	Request for Comments
SI	Système d'Information
SIG	Système d'Information Géographique
SISR	Système d'Information et Système Réseau
SMB	Server Message Block
SWML	Switch Multi-Layer
VBS	Visual Basic Scripting
VLAN	Virtual Local Area Network
VSS	Volume Snapshot Service