



Nom de naissance : TURCK

Nom d'usage : TURCK

Prénom : Julien

Validation des Acquis de l'Expérience

Livret 2

Diplôme visé

Type : Brevet de Technicien Supérieur

Intitulé : Services informatiques aux organisations

Option A Solution d'Infrastructure Système et Réseau

Réservé à l'administration

Académie :

Numéro de la demande :

Date recevabilité : / / 20...

Date réception : / / 20...

Décision de recevabilité jointe

Cachet de l'administration

Dossier de validation - Livret 2

Mode d'emploi

Vous avez effectué une demande de VAE en déposant votre dossier de recevabilité (Livret 1) auprès du dispositif académique de validation des acquis (DAVA). Votre demande a été déclarée recevable. Cette décision est valable **pendant 3 ans** sous réserve d'évolution réglementaire du diplôme.

Désormais, **vous allez renseigner ce dossier de validation-Livret 2.**

Il s'agit d'un questionnaire guidé pour vous aider à **décrire les activités les plus significatives** que vous réalisez ou avez réalisées et qui correspondent aux activités du référentiel d'activités professionnelles du diplôme visé.

C'est à partir de la description détaillée de vos activités et du contexte dans lequel vous les exercez que le jury détectera les connaissances et compétences que vous mettez en œuvre et vérifiera ensuite si elles sont conformes aux exigences du diplôme.

Suite à l'évaluation que le jury aura faite de votre dossier de validation, il vous recevra en entretien et statuera. Il décidera de valider ou de ne pas valider et dans le premier cas, décidera de vous accorder le diplôme dans son intégralité ou en partie seulement.

Comment choisir les activités les plus significatives que vous allez décrire et qui sont en rapport direct avec le diplôme que vous visez ?

- en consultant attentivement le référentiel d'activités professionnelles du diplôme visé sur le site www.francevae.fr
- en vous faisant accompagner. L'accompagnateur VAE est là pour vous guider dans le choix des activités (de 1 activité minimum à 8 au maximum) et pour vous aider à en parler et les décrire.

Quand vous aurez choisi ces activités, vous présenterez le (les) poste(s) et la (les) structures dans lesquels vous les exercez ou les avez exercées.

Contenu de ce livret

Vérifiez que les éléments suivants figurent dans votre livret et inscrivez-en le nombre. Vous pouvez rajouter les numéros de page dans la colonne de droite.

Documents	Nombre	Numéro de page
Votre CV <i>Vous surlignerez les expériences en rapport direct avec le diplôme visé</i>	1	4
Fiche(s) descriptive(s) de votre (vos) structure(s)	1	7
Fiche(s) descriptive(s) de votre (vos) poste(s) occupé(s)	1	13
Fiche(s) descriptive(s) de votre (vos) activité(s)	3	17 – 72 - 160
Déclaration sur l'honneur	1	202

Table des matières

Contenu de ce livret.....	3
Table des matières	4
Votre CV	5
Introduction.....	7
Fiche descriptive de la structure Réseau de lecture publique BMI de la C.A.E.....	8
Fiche descriptive du poste occupé Bibliothécaire-informaticien.....	14
Fiche descriptive de l'activité 1 <i>La gestion du système d'information au quotidien</i>	17
I. La maintenance préventive	18
a) Les mises à jour	18
b) Les actions du quotidien plus spécifiques	30
II. La gestion des utilisateurs	47
a) La gestion des accès	47
b) La gestion des incidents et de l'accompagnement	59
Fiche descriptive de l'activité 2 <i>L'administration du réseau et des sites distants</i>	72
I. L'infrastructure du réseau	73
a) La bibliothèque d'Epinal : un cœur de réseau à rafraîchir	73
b) Les différentes connexions	95
II. L'exploitation du SI	110
a) Son administration au quotidien	110
b) Mise à disposition d'un service	131
Fiche descriptive de l'activité 3 <i>La sécurité au centre de nos préoccupations</i>	160
I. La sécurisation des installations	161
a) Les menaces internes	161
b) Exemple de menace externe : le cybercriminel	168
II. Insérer le SI dans un monde hostile et changeant	178
a) Sécuriser ses trafics avec l'extérieur	178
b) L'adapter aux situations nouvelles	188
Conclusion.....	199
Déclaration sur l'honneur.....	201

Votre CV

TECHNICIEN INFORMATIQUE

Expériences professionnelles

- Depuis août 2022 : chargé de maintenance numérique éducatif pour l'Agence Départementale d'Ingénierie pour les Collectivités de l'Aisne, Laon :
 - Installer et maintenance du parc informatique et numérique des écoles primaires du département
 - Accompagner de prise en main du matériel
 - Suivre les tickets incidents de l'ENT des hauts de France
 - Suivre le Mobile Device Management "school"
- Octobre 2021 – juillet 2022 : conseiller numérique pour Emmaüs-Connect, Soissons :
 - Conseiller et former autour des usages du numérique
- Mars 2017 – septembre 2021 : agent du secteur Informatique de la Bibliothèque Multimédia Intercommunale et du réseau de lecture publique de la communauté d'agglomération d'Epinal, à Epinal :
 - Gérer le parc informatique
 - Répondre aux demandes d'assistancess
 - Mettre à disposition des services informatiques (RFID)
 - Gérer le SIGB et la visibilité en ligne du réseau de lecture publique
 - Concevoir et déployer des infrastructures réseaux
 - Surveiller et dépanner le réseau
 - Mettre aux normes de la RGPD
 - Sécuriser les données et des équipements
- Octobre 2012 – juillet 2014 : animateur multimédia et référent informatique, médiathèque Intercommunale de la communauté d'agglomération d'Epinal à Thaon-les-Vosges :
 - Gérer le parc informatique
 - Former autour des usages du numérique

Autres expériences

- Juillet 2014 – mars 2017 : adjoint du patrimoine, secteur musique et cinéma, Bibliothèque Multimédia Intercommunale de la communauté d'agglomération d'Epinal, à Epinal
- Avril-octobre 2012 : agent du patrimoine contractuel, médiathèque intercommunale de la porte des Hautes-Vosges
- Eté 2009-2010-2011 : agent du patrimoine saisonnier, maison natale de Jeanne d'Arc à Domrémy-la-Pucelle
- Eté 2007 – 2008 : opérateur machine, fournisseur à Harol
- 09/2006-05/2007 : stagiaire, papeterie de Raon l'étape
- 01/2005-12/2006 : militaire réserviste, 1^{er} régiment de tirailleurs à Epinal

Formation

- **2015 : Diplôme universitaire Médiation Multimédia et Monitorat d'Internet,
Faculté de Sciences et techniques de Poitiers**
- 2012/2013 : formation ABF, IUT Charlemagne à Nancy
- 2007/2011 : deux licences en histoire et histoire de l'art, parcours patrimoine, CLSH NANCY
- 2002/2005 : BAC STI « génie mécanique » option « productique », Pierre Mendès France à Epinal

Introduction

Je soumets ma candidature dans le cadre de l'obtention du BTS SIO option A : SISR, par le biais du dispositif de la V.A.E, afin de faire reconnaître mes compétences acquises sur le terrain, alors que mon parcours scolaire initiale ne me prédisposait pas forcément à une carrière professionnelle dans ce secteur d'activité.

Mon premier choix d'orientation s'est tourné vers un Baccalauréat technologique orienté industrie puis deux essais de BTS dans le même secteur. Ces essais ne m'ont pas convaincu. Etant passionné d'histoire, je me suis très vite réorienté vers une double licence histoire et histoire de l'art dans une faculté, licence par la suite complétée avec un diplôme reconnu des métiers du livre.

A une époque où les bibliothèques s'informatisaient en masse et s'ouvraient aux nouvelles technologies du numérique, j'ai très vite trouvé ma place dans ce milieu, en qualité de médiateur numérique et référent informatique.

Dans une optique de justifier ma position et afin de prétendre à des évolutions de carrières, j'ai complété ma formation par un diplôme d'animateur multimédia dans lequel était inclus des cours dédiés aux réseaux informatiques et développement Web. Tout cela m'a permis, au moment du regroupement de plusieurs communes, d'obtenir un poste dans le secteur informatique de la plus grande bibliothèque du département des Vosges. Dans un premier temps, j'ai commencé sur de la maintenance de 1^{er} niveau du parc, mais les nécessités du service ont fait que j'ai très vite accompagné le seul informaticien de métier dans ses missions. En effet, le service ne pouvait pas supporter une panne sous prétexte que celui-ci soit en congé ou malade. Il m'a donc formé en interne sur les infrastructures au fur et à mesure de ses interventions afin de comprendre les mécanismes et comprendre les problèmes auxquels je pouvais être confronté. Il m'a aussi formé sur ses logiciels de surveillance et de gestion afin que le réseau soit toujours sous surveillance. Enfin, il m'a associé aux chantiers pour pouvoir avoir de l'aide sur certaines tâches voire me les déléguer. Cette expérience m'a fait découvrir un domaine que je ne pensais pas pour moi, et j'ai pu évoluer en interne par le biais de ce poste.

Toutefois, la rencontre de ma compagne et la naissance de mon premier enfant m'ont fait quitter ma région natale pour la Picardie. Cela a coupé mon élan et m'a quelque peu sorti du « système ». J'ai fini par retrouver un poste de chargé de maintenance numérique éducative dans le secteur informatique du conseil départemental de l'Aisne.

Le poste en lui-même ne justifie pas une évolution importante. Toutefois, ce très grand service propose beaucoup de postes à responsabilités. Pour y prétendre, plus que mes compétences, un niveau bac+2 est au minimum requis, c'est pourquoi je compte sur ce BTS pour me permettre de postuler.

J'espère ainsi, que ce dossier réussira à vous convaincre de mes aptitudes dans les domaines visés.

Fiche descriptive de la structure

Réseau de lecture publique BMI de la C.A.E

Entre mars 2017 et septembre 2021, je suis en poste au sein du secteur informatique du réseau de lecture publique des Bibliothèques Multimédia Intercommunales de la Communauté d'Agglomération d'Epinal (C.A.E). J'ai profité de la vacation du poste pour intégrer ce service, alors que je suis employé dans ce réseau depuis octobre 2012.

La Communauté d'Agglomération d'Epinal :



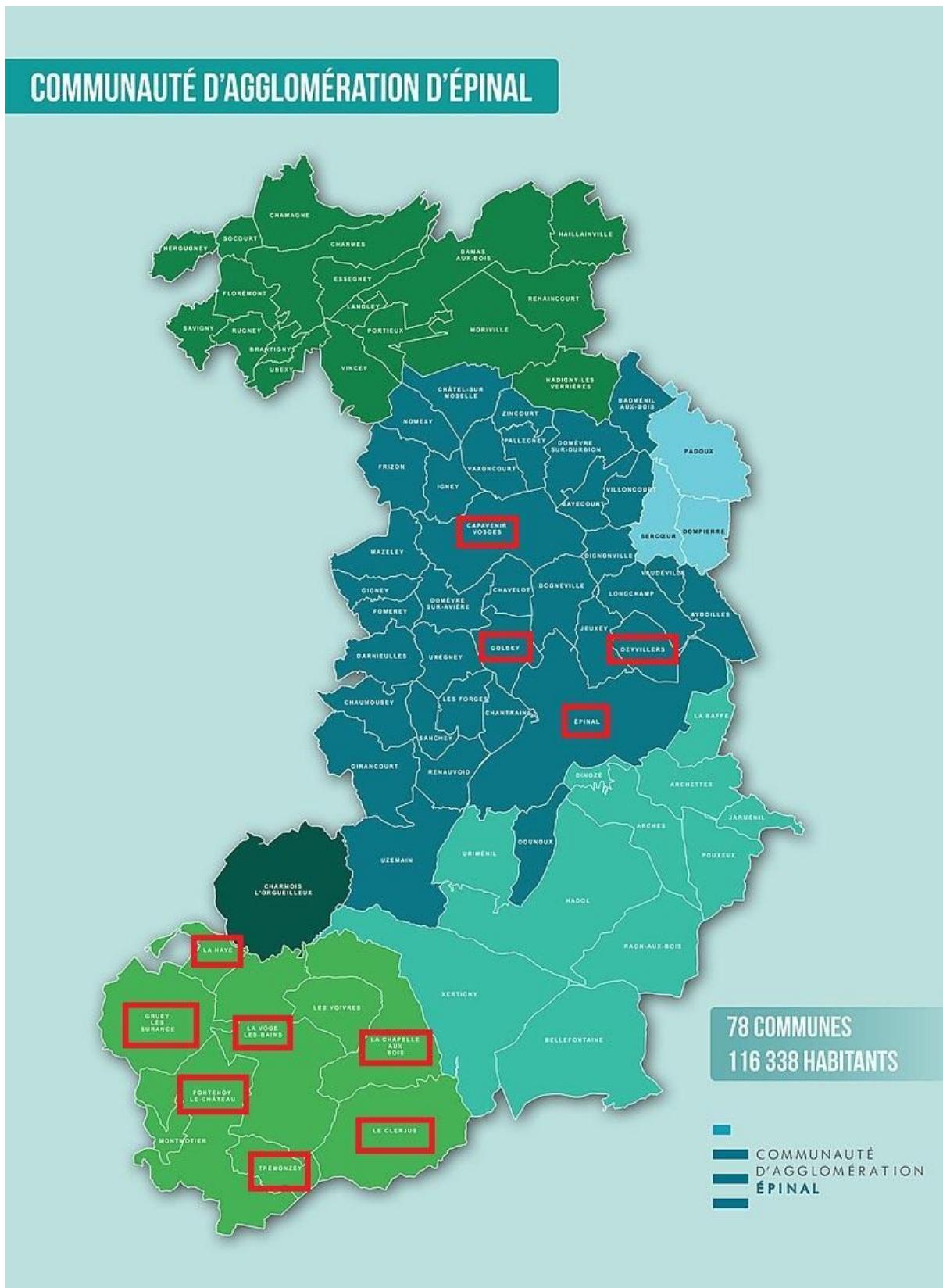
La Communauté d'Agglomération d'Epinal, créée en 1999 sous le nom de communauté de communes d'Epinal-Golbey, a acquis sa forme juridique actuelle en 2017. Elle comprend aujourd'hui 78 communes pour 116338 habitants au recensement de 2018.

L'organe décisionnel se compose d'un 1 président, de 12 vice-présidents et de 15 conseillers délégués.

La Communauté d'Agglomération d'Epinal à la gestion de 10 compétences obligatoires comme la gestion de l'eau ou la collecte des déchets. De 5 compétences optionnelles dont la compétence **Construction, aménagement, entretien et gestion d'équipements culturels et sportifs d'intérêt communautaire** qui me concerne. Et pour finir, 6 compétences facultatives telles que le développement du tourisme.

Carte de la communauté d'agglomération d'Epinal :

Sont encadrées en rouge les communes possédant une des bibliothèques du réseau



Bibliothèques Multimédias Intercommunales :



● **Historique :**

Le réseau de lecture dépend donc de la C.A.E., du fait de la compétence optionnelle sur la gestion des équipements culturels, acquise par celle-ci.

Bien qu'Epinal ait toujours eu une bibliothèque, ce réseau a vu le jour en 2009. À l'époque la communauté d'agglomération n'est encore composée que des deux seules communes d'Epinal et de Golbey. Soucieux d'offrir un service culturel de qualité à sa population, les deux maires s'entendent sur un projet commun. D'une part, ils font déménager la bibliothèque d'Epinal dans un bâtiment spécialement bâti pour l'occasion, plus spacieux et plus moderne. D'autre part, afin que les habitants de Golbey puissent profiter pleinement du service, ils font aménager une annexe dans le bâtiment accolé au centre socio-culturel de Golbey. Sont ensuite intégrées celles qui dépendent des anciennes intercommunalités intégrées à la nouvelle C.A.E. A savoir celle de Capavenir Vosges en 2013, Deyvillers en 2014 qui a la particularité d'être dans le même bâtiment qu'une crèche et l'intégralité du réseau de la Vôge-les-Bains en 2017, composé des médiathèques :

- La Vôge-les-Bains
- La-Chapelle-aux-bois
- Fontenoy-le-Château
- Gruey-lès-Surance
- Trémonzey
- Le Clerjus
- La Haye

D'autres projets d'intégration sont en cours.

Les différentes bibliothèques du réseau de lecture publique :

Epinal



Golbey



Capavenir Vosges



Deyvillers



La Vôge-les-Bains



La Chapelle aux bois



Gruéy-lès-Surance



Le Clerjus



La Haye



Trémonzey



- **Organisation du personnel :**

Ce réseau se compose donc de 11 bibliothèques, dans lesquelles sont répartis 47 salariés, tous fonctionnaires territoriaux, pour faire fonctionner les 5 bibliothèques principales ainsi que d'une quinzaine de bénévoles pour animer les 6 bibliothèques annexes. Tous les salariés sont répartis dans différents services, en fonction de leurs compétences et de leur lieu de rattachement. Chaque service a un chef de service et chaque bibliothèque principale a un responsable. Tous sont sous la juridiction de la directrice qui est secondée par une directrice adjointe.

- **Services :**

Toutes proposent différents services en fonction de leurs tailles et de leurs spécificités. Elles ont toutes en commun l'emprunt et la consultation sur place de documents parmi un très large choix de livres, magazines, bandes dessinées, partitions, dvd, cd, jeux vidéo et jeux de société. Epinal proposent en plus de la consultation de livres anciens. Hormis Deyvillers, bloquée par la présence de la crèche, elles proposent toutes un accès gratuit au WIFI. Toutes les bibliothèques principales mettent aussi à disposition du public des ordinateurs sur place connectés à Internet et à un service de photocopies, hormis Deyvillers, jugée trop petite en taille et peu rentable au de sa fréquentation. Seules l'inscription aux bibliothèques et les photocopies sont payantes.

- **Partenariats :**

Le réseau s'appuie sur des partenaires pour toucher un maximum de public.

Ainsi, les bibliothèques ont développé un grand partenariat avec tout le milieu scolaire du département en offrant les abonnements aux professeurs de tous les niveaux et aux étudiants inscrits dans une école supérieure appartenant au réseau Université de Lorraine, en abritant la didacthèque de l'antenne vosgienne de Canopé, en achetant et en équipant les livres pour toutes les BCD de la ville d'Epinal et en accueillant toutes classes qui en font la demande. Elles travaillent aussi avec les autres équipements culturels de la C.A.E (cinéma, salle de concert, conservatoire ou encore le planétarium) dans le cadre de projets en commun, accueillent tous les centres socio-culturels et associations de la C.A.E qui en font la demande.

- **Prestataires :**

Enfin, le réseau s'appuie sur des prestataires pour certains services pour lesquels il n'y a pas de personnel qualifié ou pour du matériel très spécifique.

Parmi les besoins de prestations, elles font appel lorsqu'il y a des soucis au niveau des chaufferies, des climatisations et des systèmes d'alertes intrusions et incendie. Le reste est géré par les services techniques des communes.

Malgré notre présence, il y a aussi des prestataires pour des services informatiques spécifiques : le fournisseur d'accès Internet, le prestataire du SIGB (Système Intégré

de Gestion de Bibliothèque), celui de la technologie RFID (Radio Frequency Identification Data), le prestataire du proxy et un prestataire qui gère nos pare-feux.

Fiche descriptive du poste occupé

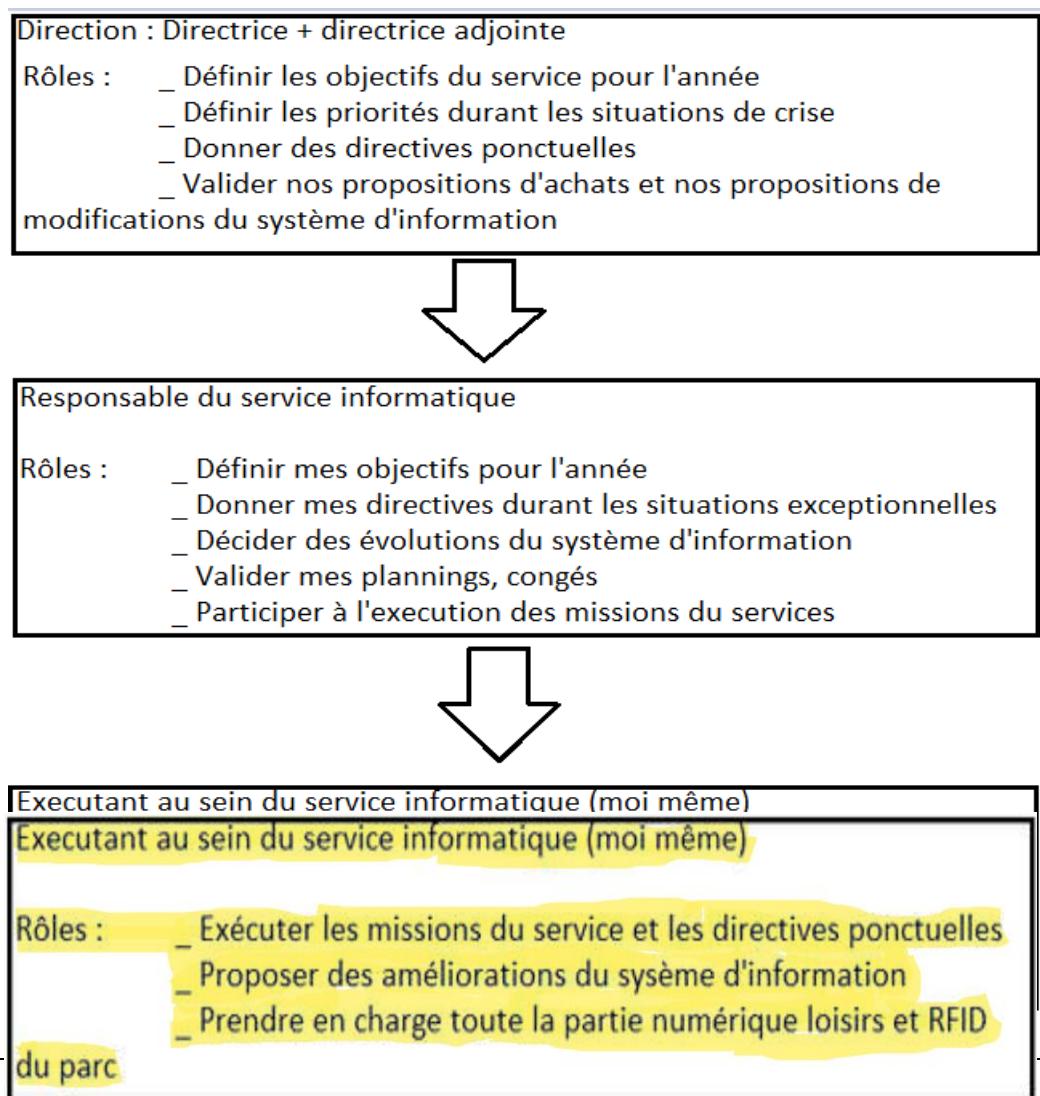
Bibliothécaire-informaticien

Entre mars 2017 et septembre 2021, je suis bibliothécaire-informaticien pour le service informatique du réseau de lecture publique de la communauté d'agglomération d'Epinal.

Je suis salarié, à 37H par semaine. J'ai le statut de fonctionnaire, titulaire sur le grade d'adjoint du patrimoine principal de première classe.

Le service informatique se compose de 2 salariés : le responsable du service, qui est aussi mon supérieur hiérarchique et moi-même. Nous sommes, comme tous les autres employés, sous la tutelle de la directrice et de la directrice adjointe. Nous pouvons être sollicité par n'importe lequel des 45 salariés et 15 bénévoles du réseau, pour toute demande d'assistance, de dépannage, de formation et d'animation concernant les outils informatiques et numériques. Nous gérons ces sollicitations en fonction de leur urgence et de leur impact sur le service.

● Organigramme du service :



● **Les missions du service :**

- Maintenir le parc informatique opérationnel
- Maintenir le réseau informatique opérationnel
- Veiller à la sécurité du réseau et des données
- Accompagner les référents sur le SIGB (système intégré de gestion de bibliothèque) et le site Internet
- Maintenir et développer l'automatisation des tâches récurrentes de la bibliothèque grâce à la technologie RFID (Radio Frequency Identification Data)
- Diagnostiquer, améliorer en conséquence et maintenir le parc informatique des nouvelles extensions du réseau de lecture publique
- Raccorder au réseau informatique existant les nouvelles extensions du réseau de lecture publique
- Mettre à disposition, former et accompagner les bibliothécaires ainsi que le public sur les outils informatiques et numériques des bibliothèques
- En lien avec le DPO (délégué à la protection des données), participer aux mises aux normes de la RGPD
- Mettre en place et faire appliquer le PCA (plan de continuité d'activité) et le PRA (plan de reprise d'activité)
- Proposer des améliorations au SI (système d'information)

● **Financement du service :**

Pour réaliser ces missions, le service se voit attribuer à l'année, par la directrice, un budget de fonctionnement voté par le conseil de la C.A.E. Ce budget concerne les achats de petit matériel et de consommables. Le gros matériel, les renouvellements importants et les travaux sont traités sur les lignes du budget d'investissement, soumis à l'acceptation du président de la C.A.E et font l'objet de procédures de marché public à procédure adaptée.

Le réseau de lecture est labellisé Bibliothèque Numérique de Référence par le ministère de l'éducation. A ce titre, certains de nos projets sont financés en grande partie par la Direction Régionale des Affaires Culturelles de Lorraine et l'Europe.

● **Mes missions au sein du service :**

Mes missions tournent autour de cinq axes de travail :

1. J'effectue en autonomie la maintenance de premier niveau du parc informatique (Mises à jour, dépannage des ordinateurs, remplacement du matériel défectueux, mise en route des nouvelles machines, inventaire du matériel). Je réalise des formations auprès des collègues sur ces outils et les logiciels.
2. En lien avec le chef de service, je participe à la surveillance et au développement du réseau informatique de toutes les bibliothèques du réseau de lecture publique. Je veille à la sécurité du SI. J'effectue en autonomie la gestion de comptes utilisateurs (création, gestion des permissions, récupération des mots de passe, suppression), le rattachement d'équipement au réseau (postes de travail, imprimantes, platines RFID), la gestion d'accès au VPN (création de

compte, suppression de comptes). J'accompagne également le chef du service pour les gros travaux de maintenance, de modifications et d'extensions du réseau informatique. Enfin, je le supplée dans le traitement des urgences lors de ses absences.

Par exemple, il y a eu une fois, une panne qui a déconnecté du réseau tout une partie du parc de la bibliothèque d'Epinal. Le fait que cela ne touche pas l'ensemble des postes m'a fait penser que le problème pouvait venir d'un des trois switches sur lesquels sont répartis les postes. En testant leur réactivité, en débranchant pour chacun un câble réseau d'un de leur port, il s'est avéré qu'un sur les trois ne réagissait pas au changement de situation (la LED du port continuait d'indiquer qu'un câble était soi-disant branché dessus). Après redémarrage de ce switch, les postes de travail concernés se sont tout de suite reconnectés.

3. En autonomie, j'assure la prise en charge de la partie RFID des bibliothèques, en étant l'interlocuteur privilégié de la société qui nous fournit le matériel et qui m'a formé dessus afin d'installer et effectuer de la petite maintenance. Je propose régulièrement des achats, soit pour remplacer du matériel qui commence à devenir défectueux, soit pour améliorer les processus d'automatisation de certaines tâches comme l'enregistrement des nouveaux documents, les prêts et les retours des usagers.
4. Je suis responsable de la partie numérique de la bibliothèque. Je suis le référent pour toute proposition d'achat et d'animation autour d'outils numériques tels que les jeux vidéo, imprimantes 3D, robots programmables, tablettes ou bien encore liseuses. Je centralise les demandes d'achats et effectue celles qui me paraissent les plus pertinentes, en fonction du budget qui m'est alloué. J'encadre les groupes de travail, basés sur le volontariat, autour des nouveaux services au numérique et les animations en lien. Enfin, j'anime des ateliers de formations auprès des collègues et du public.
5. En lien avec les responsables, j'aide à l'administration du SIGB et des services en ligne tels que le portail du site Internet du réseau et du portail des ressources numériques en ligne (création de comptes, gestion des permissions, création de contenus, formations sur leurs utilisations).

Fiche descriptive de l'activité 1

La gestion du système d'information au quotidien

ACTIVITÉ 1 : La gestion du système d'information au quotidien

Une des principales missions qui m'est confiée au moment de la prise du poste est la maintenance de premier niveau du parc informatique. Ça consiste à entretenir le parc afin d'en assurer un bon fonctionnement au quotidien. Soit en anticipant (mises à jour, nettoyage), soit en réglant les problèmes basiques (réinitialisation, remplacement de matériel), ne demandant pas d'être remontés à un niveau supérieur de compétences.

C'est une mission qui s'inscrit dans un cadre plus global de tâches confiées à un technicien informatique. Ce bloc plus complet, que l'on peut résumer par support et mise à disposition de services informatiques, regroupe également la gestion du parc dans son ensemble, la prise en charge de son évolution, le suivi des tickets utilisateurs, la gestion des permissions, la sauvegarde d'une partie des fichiers et la participation à l'image du service sur Internet ainsi qu'au développement de solutions logiciels.

C'est tout le propos de cette activité dans laquelle je vais développer ma participation à toutes ces actions dans un plan en deux parties.

Dans un premier temps je parlerais de ma gestion du patrimoine, qui consiste à entretenir le parc quotidiennement, pour lequel je suis toutefois amené à effectuer des actions ponctuelles plus spécifiques. Dans un second temps, j'expliquerai ma façon de traiter les utilisateurs, que ça soit la gestion de leurs accès ou le traitement de leurs besoins au quotidien.

I. La maintenance préventive

a) Les mises à jour

Beaucoup de personnes se demandent ce que peuvent bien faire le personnel des bibliothèques lorsque celles-ci sont fermées.

Je ne me pencherais pas sur le travail réalisé par les bibliothécaires, bien que ça a été mon quotidien entre avril 2012 et mars 2017. Je vais en revanche m'attarder sur les tâches du quotidien que j'effectue depuis ma prise de poste en mars 2017 au sein du service informatique.

L'objectif de ces opérations est d'assurer le bon fonctionnement des machines des bibliothèques, mises à la disposition des visiteurs lors des périodes d'ouverture ainsi que celles qui permettent aux professionnels d'assurer un service public de qualité. Je les réalise les matinées fermées au public (soit les mardis, jeudis et vendredis) et cela consiste à vérifier le bon démarrage des appareils, leur bon fonctionnement ainsi qu'une vérification de leurs mises à jour, et pour les ordinateurs, contrôler l'antivirus.

Le parc que je surveille est assez conséquent et hétéroclite puisque composé d'une centaine d'ordinateurs, tous sous OS (Operating System ou Système d'exploitation) Windows 10, une vingtaine de tablettes Android et IPad, une dizaine de liseuses et une dizaine de consoles de jeux vidéo, trois de salon et le reste portables. Il me faut donc faire des choix pour être le plus efficace possible. Ma priorité est de m'occuper des appareils fixes, les portables pouvant être réalisés dans mon bureau même lors des horaires d'ouverture. Mon deuxième critère de choix est de m'occuper des appareils à disposition du public en priorité, soucieux de l'image renvoyée par les médiathèques et parce que je peux faire ceux des collègues lorsque ceux-ci ont une tâche à réaliser qui ne nécessite pas l'utilisation de leur poste.

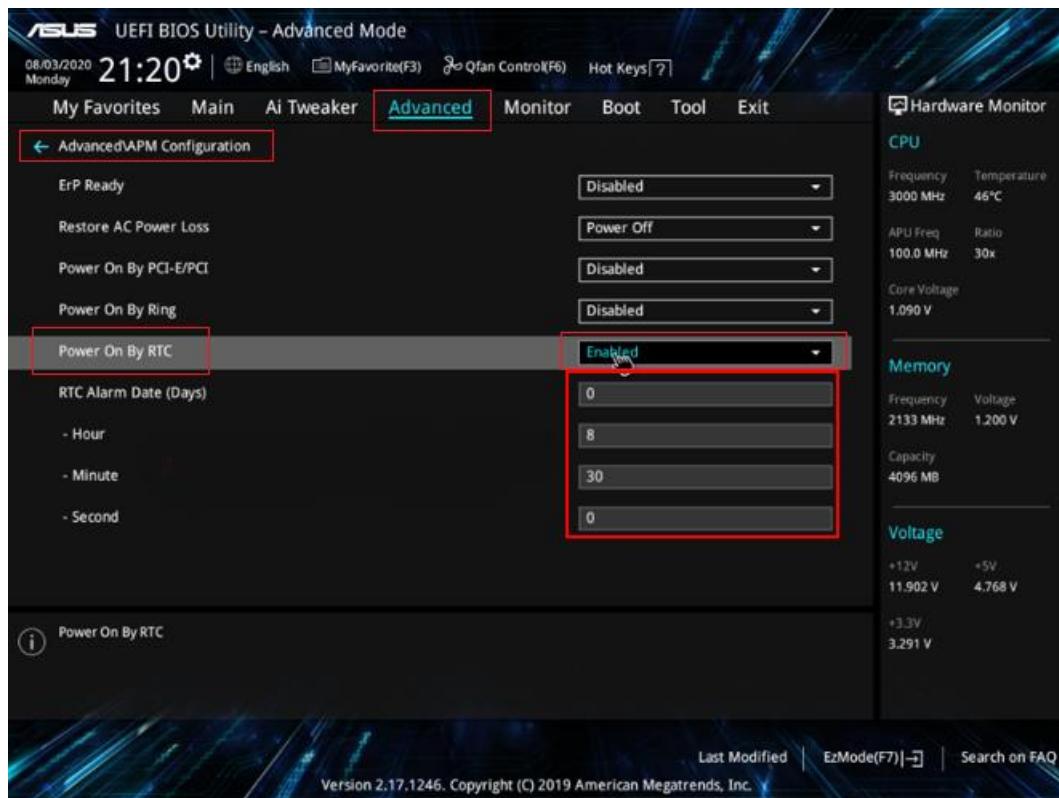
L'automatisation des postes publics

Pour me faciliter les choses, j'ai tout d'abord automatisé le démarrage des ordinateurs publics, en paramétrant dans leur UEFI un allumage automatique les jours ouvrés.

UEFI (Unified Extensible Firmware Interface)

Successeur du BIOS (Basic Input Output System), c'est un micrologiciel contenu dans la carte mère et qui se lance au démarrage de la machine. C'est par exemple lui qui charge l'OS qui prend le relais pour permettre l'interaction entre la machine et son utilisateur.

Pour l'ouvrir, il suffit d'appuyer sur une des touches, soit echap, soit fonction (de F1 à F12), en fonction du constructeur du PC. Pour activer le démarrage automatique, je vais ensuite dans le menu « alimentation » puis « APM Configuration ». J'active l'option « Power On By RTC Alarm » (Enabled) puis je renseigne les jours (0 pour indiquer tous les jours) et l'horaire.



Cette solution pose néanmoins un souci de consommation énergétique inutile puisque cette manipulation ne permet pas de choisir les jours souhaités. Enfin, ils sont allumés même si je ne les manipule pas tout de suite. J'ai compensé cela par un paramétrage de la mise en veille avec des faibles de temps d'attente d'inutilisation.

Pour se faire, j'ouvre le menu système des paramètres. Je clique ensuite sur le sous-menu « alimentation et mise en veille ». Je modifie ensuite les temps d'inactivité par le biais des menus déroulants associés aux cas de figure.

Alimentation et mise en veille

Écran

En cas de fonctionnement sur batterie, éteindre après
2 minutes

En cas de branchement sur le secteur, éteindre après
2 minutes

Veille

En cas de fonctionnement sur batterie, mettre le PC en veille après
5 minutes

En cas de branchement sur secteur, mettre le PC en veille après
5 minutes

Je ne programme pas les temps les plus faible afin que l'ordinateur ne se mette pas en veille à chaque pause de l'utilisateur.

J'ai également simplifié l'ouverture de la session publique en paramétrant dans l'éditeur de registre une connexion automatique à la session publique.

Le registre

Base de données qui sert à stocker les informations nécessaires au bon fonctionnement de l'OS.

Pour automatiser la connexion à une session au démarrage :

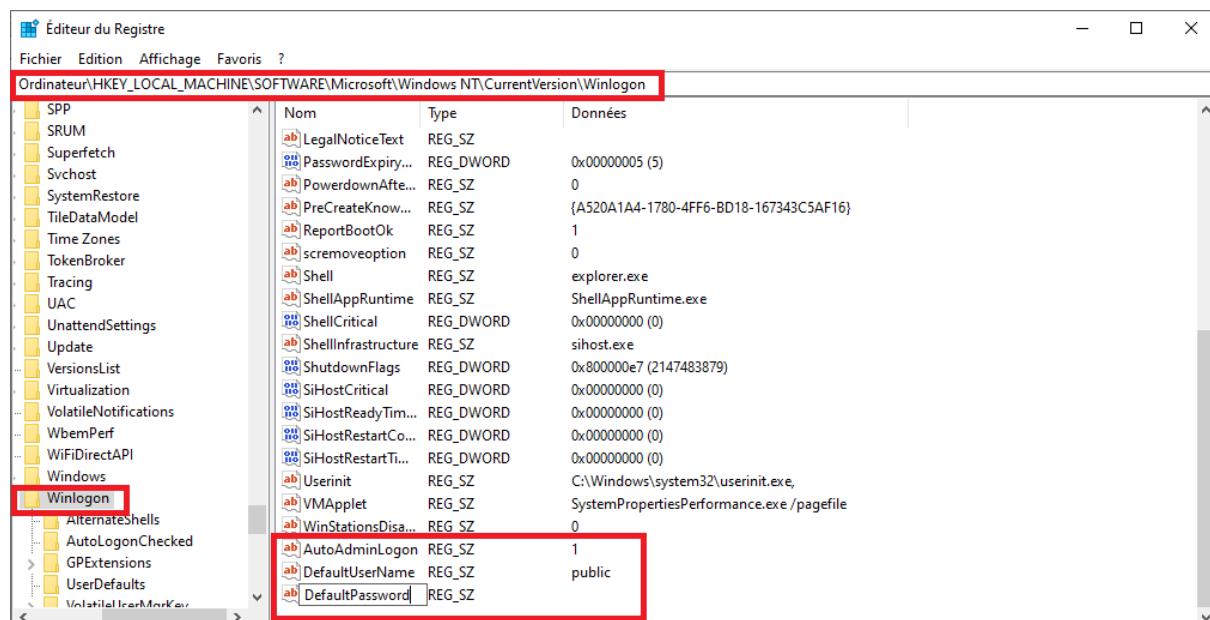
L'éditeur est accessible en tapant par exemple regedit dans la barre de recherche de la barre des tâches.

Il faut ensuite afficher le contenu de la sous-clé winlogon, accessible en suivant le chemin suivant : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

Enfin, on modifie le contenu des 3 entrées suivantes en double-cliquant sur chacune d'elle (voir illustrations ci-dessous) :

- DefaultUserName : ici, on indique le nom de la session
- DefaultPassword : ici, on indique le mot de passe de la session
- AutoAdminLogon : ici, on tape 1 pour activer l'option d'ouverture automatique de la session

Si toutefois une des entrées n'est pas présente par défaut, il faut la créer en cliquant sur « édition » puis « nouveau » et pointer « valeur de chaîne ». On modifie ensuite son nom à gauche, à la place de « nouvelle valeur ».



J'ai bien conscience que cette connexion automatique pose des problèmes de sécurité. En effet, si une personne vient à voler un des ordinateurs, elle pourra s'en servir chez elle. Toutefois, la session paramétrée n'est pas administratrice. Aussi, le voleur ne pourra donc pas installer de nouveaux programmes, à moins découvrir le mot de passe de la session administrateur.

De plus, j'installe Reboot Restore RX. Un logiciel qui « gèle » la configuration des ordinateurs publics. Cela m'assure que les ordinateurs redémarrent avec la configuration souhaitée. Cela efface également tous les documents que les utilisateurs de la veille auraient pu laisser et qui poseraient des problèmes de confidentialité. Ça a tout de même quelques inconvénients, puisque ça m'oblige à quelques manipulations en plus à chaque modification de configuration (dont la mise à jour des logiciels) et ça ne permet plus une mise à jour automatique du système d'exploitation qui est effacée à chaque redémarrage du PC.

Enfin, j'ai programmé l'extinction automatique des ordinateurs en fin de journée pour les jours ouvrés et en début de journée pour les jours non ouvrés, avec un petit fichier txt dans lequel j'ai écrit un script batch :

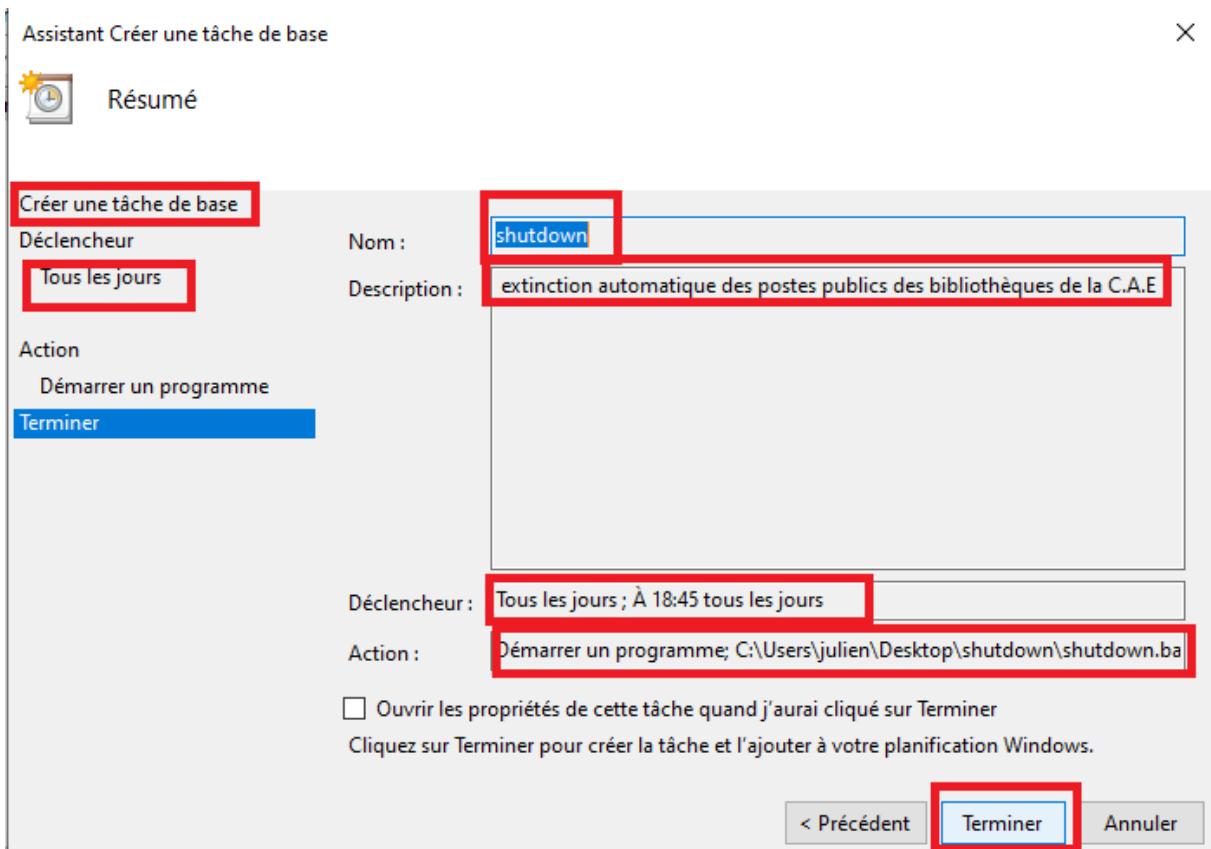
```
shutdown - Bloc-notes
Fichier Edition Format Affichage Aide
shutdown /s /c "Ce PC va bientôt s'éteindre. Vérifiez que vous avez bien enregistré votre travail" /t 300
```

Je modifie ensuite l'extension de ce fichier en .bat et je l'intègre dans une tâche planifiée du planificateur de tâches.

Planificateur de tâches :

Service intégré à l'OS qui permet de programmer des tâches automatisées.

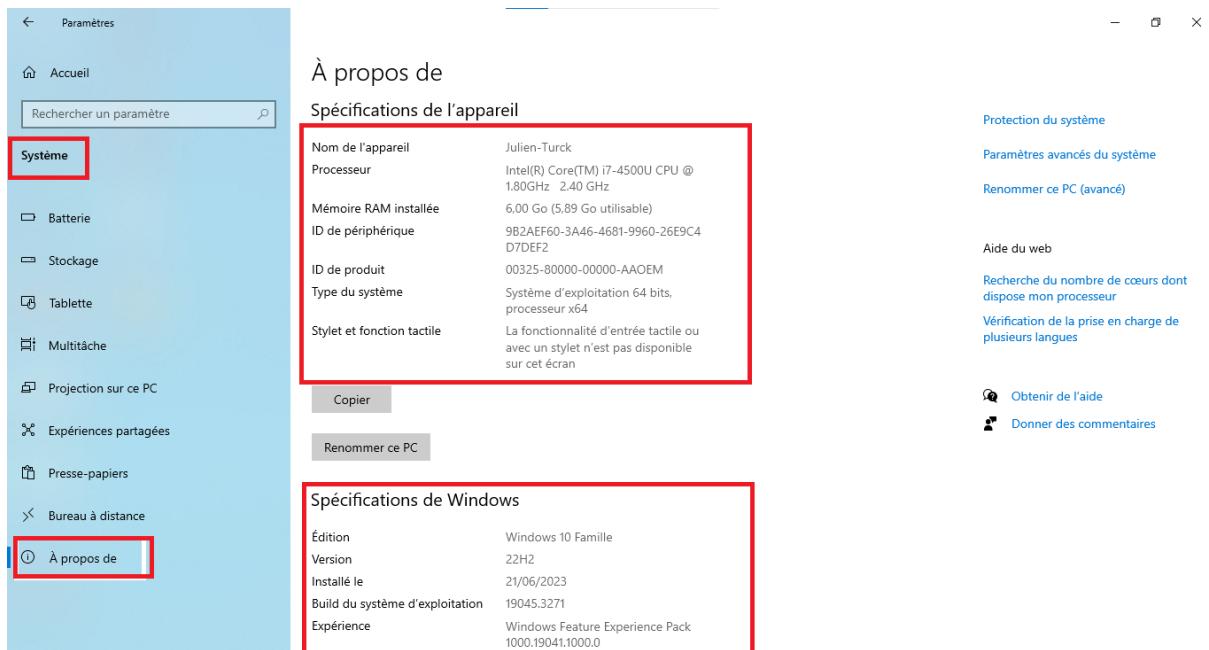
Il est accessible depuis la barre de recherche, en tapant son nom. Pour programmer mon extinction, je clique ensuite sur « créer une tâche de base ». Je vais lui donner un nom compréhensible pour la retrouver dans la liste des tâches que je complète avec un descriptif. Je vais lui renseigner un déclencheur pour lequel je préciser sa fréquence (tous les jours), ainsi que l'heure à laquelle je veux que ça soit effectué. Enfin, je vais lui demander comme action d'exécuter mon script, pour lequel j'indique le chemin à suivre pour le trouver.



Toutes ces automatisations me libèrent beaucoup de temps et me permettent de me concentrer sur ce que j'ai décidé de faire manuellement sur les ordinateurs publics, à savoir la gestion complète des logiciels ainsi que la gestion des mises à jour du système d'exploitation.

Entretien des postes publics

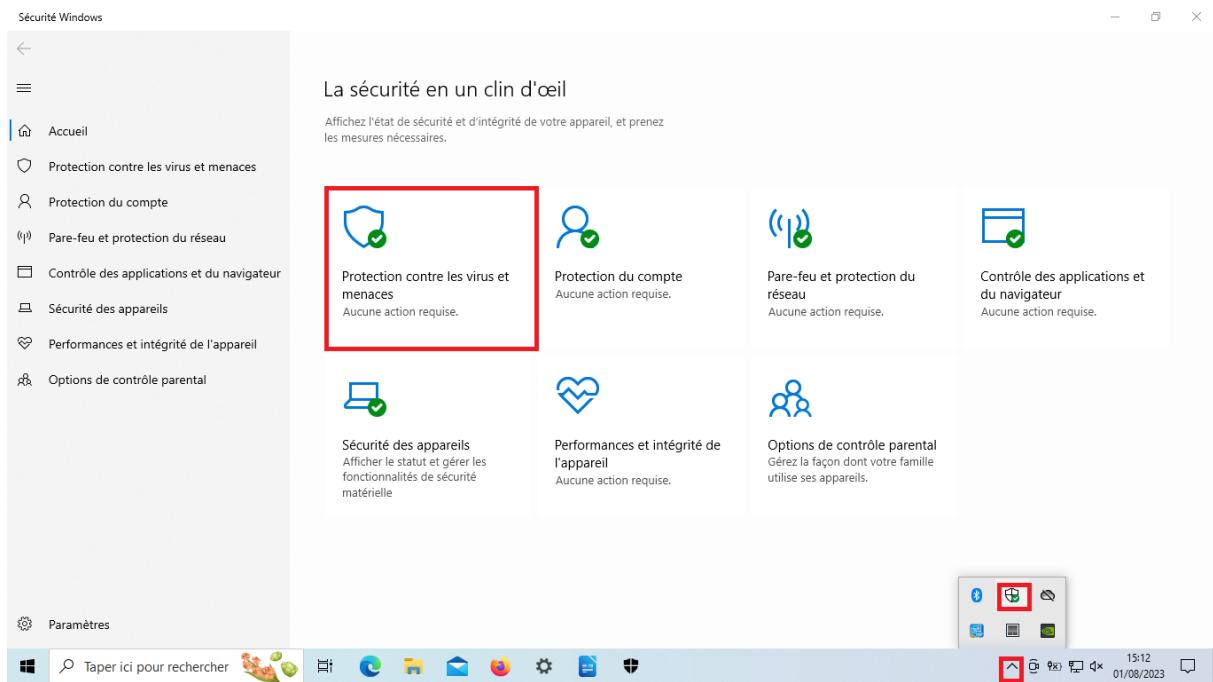
J'ai fait le choix de réduire le nombre de logiciels au strict minimum pour travailler. En effet, l'idée est qu'ils doivent surtout être utilisé pour travailler ou consulter Internet. De plus, ça permet de ne pas surcharger le disque dur inutilement et donc de risquer des ralentissements. Il n'y a donc aucun jeu d'installé par exemple. De toute manière, leur configuration ne permette pas de faire tourner des programmes trop gourmands en termes de ressources.



Tous les logiciels installés sont gratuits, pour réduire les coûts de licences :

- J'essaye de privilégier les utilitaires Windows lorsque je les juge performants comme le lecteur de photos, de vidéos et de musiques et Edge qui fait office de navigateur et de lecteur PDF.
En effet, étant développés par Microsoft, ils sont censés ne pas créer de faille de sécurité dans le système.
- Si ceux-ci ne me semblent pas performants ou inexistant, je privilégie ceux issus du monde libre lorsqu'ils sont gratuits (LibreOffice pour la bureautique, Mozilla Firefox pour la navigation Internet, Gimp pour la retouche d'images qui remplace Paint trop limité).
- Seul le navigateur Google Chrome fait office d'exception pour pallier certains problèmes de compatibilité que peuvent rencontrer les autres navigateurs Internet.
- **Ce sont des logiciels très faciles à mettre à jour, les utilitaires Windows se font à partir du store officiel et pour tous les autres, il suffit d'aller dans leurs menus « à propos » ou « aide » pour les lancer.**
-

De même, l'antivirus est celui fourni avec Windows 10.



Il est, par exemple, accessible en accès rapide depuis la barre d'outils de la barre des tâches.

Je le juge suffisamment fiable et performant pour de la simple consultation d'Internet et du travail de bureautique. Également, parce qu'il se met très facilement à jour par le biais de l'utilitaire de mises à jour de Windows, en même temps que celles des drivers.

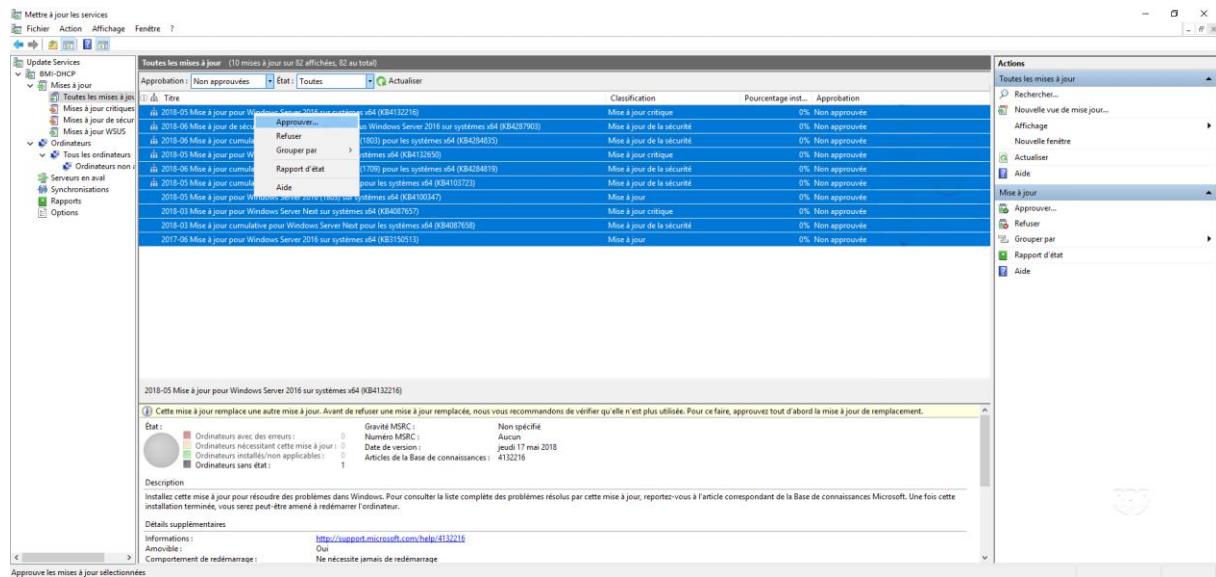
En revanche, je ne mets pas le système d'exploitation à jour durant cette phase, car il y a trop d'ordinateurs à gérer en même temps et ça saturerait le réseau.

Pour y pallier, une solution serait de pousser les mises à jour par le biais d'un serveur qui gérerait le téléchargement et permettrait un gain de temps et de bande passante. Cependant, le choix a été fait de ne pas connecter les ordinateurs publics entre à un serveur, afin d'éviter qu'un utilisateur mal attentionné ou trop imprudent compromette tout le réseau public.

Dans le temps imparti qu'il me reste avant l'ouverture au public, j'en profite pour mettre à jour les systèmes des consoles de jeux, tablettes et liseuses ainsi que les logiciels qui les accompagnent. Elles sont très simples à faire, les systèmes ayant un menu dédié et les applications se mettent à jour directement par le biais des stores d'applications. Elles sont aussi très légères permettant de toutes les faire à la volée sans saturer le réseau.

Gestion du parc professionnel

Lorsque j'ai terminé la partie publique ou lorsque l'on ouvre les portes aux visiteurs, je me retire dans les bureaux et m'attaquent aux équipements professionnels. Les ordinateurs professionnels sont plus faciles à gérer du fait qu'ils sont tous configurés pour appartenir au domaine du réseau de bibliothèques, auquel sont associés des serveurs Windows et plusieurs services. Par exemple, j'ai accès au service WSUS (Windows Server Update Service), activé sur le serveur DHCP, afin de gérer les mises à jour des systèmes d'exploitation de tous les ordinateurs qui sont tous des Windows 10 professionnels.



Ce service me permet de choisir les moments les plus appropriés pour déployer les mises à jour. Par exemple, je vais privilégier les ordinateurs professionnels des espaces publics lors des horaires de fermeture et je vais déployer ceux des bureaux lorsque les agents n'y sont plus, le tout par petits groupes. De plus ce service me permet de ne télécharger chaque mise à jour qu'une fois pour tout le parc.

Une autre possibilité aurait été de paramétrier sur chaque poste une mise à jour automatique de l'OS (operating system) avec un redémarrage automatique en fin de journée par exemple, pour apporter un gain de temps. Cependant je n'aurais plus la main sur les téléchargements, qui si sont trop importants, auraient saturé la bande passante Internet, ni la main sur leur déploiement qui aurait pu ralentir certaines machines durant des moments de fortes utilisations.

Comme pour les ordinateurs publics, il y a très peu de logiciels. A la différence que je mets à disposition du personnel la suite bureautique Microsoft Office. Pour les mêmes raisons que les ordinateurs publics, je privilégie les outils Windows tant que possible. D'autant que ces postes n'ont pas vocations à être utilisés pour autre chose que les tâches administratives et de documentations. Seuls les navigateurs Internet Mozilla Firefox et Google Chrome font office d'exceptions, nécessaires pour pallier un manque de compatibilité d'Edge avec notre SIGB qui est une solution SaaS (Software as a

Service). Ces navigateurs ont aussi l'avantage de se mettre à jour automatiquement régulièrement. Toutefois, certains postes spécifiques nécessitent des logiciels supplémentaires. Je les installe sur la demande de leur supérieur hiérarchique (par exemple, notre chargée de communication utilise la suite Adobe afin de créer certains documents de communication).

L'antivirus est géré à part puisqu'il a été choisi la solution professionnelle Endpoint pour toute la communauté d'agglomération. Les licences sont gérées par le service informatique de la ville d'Epinal qui m'octroie une licence par poste professionnel déclaré. Le choix a été fait de faire un achat groupé afin de profiter d'une grosse remise grâce à l'importance du nombre de licences. Toutefois je gère en autonomie leur attribution aux machines et je les actualise grâce à une console d'administration installée sur le serveur du domaine. Elle me permet :

- De voir sur un seul écran l'ensemble des problèmes détectés par les antivirus

STATUS	DETECTION TYPE	CAUSE	ACTION	OCCURRENCE	RESOLVED	COMPUTER NAME	OBJECT
⚠️	Antivirus	worm	retained	1	0/1	10.1.115.184	file:///C/Users/Bertrand/Desktop/
⚠️	Antivirus	worm	retained	1	0/1	10.1.115.184	file:///C/Users/Bertrand/Desktop/
⚠️	Antivirus	trojan	retained	1	0/1	10.1.115.20	file:///C/Recycle.Bin
⚠️	Antivirus	trojan	retained	2	0/2	10.1.115.20	file:///C/Documents
⚠️	Antivirus	worm	retained	2	0/2	10.1.115.20	file:///C/Documents
⚠️	Antivirus	trojan	retained	2	0/2	10.1.115.20	file:///C/Documents
⚠️	Antivirus	worm	retained	4	0/4	10.1.115.20	file:///C/Documents
⚠️	Antivirus	worm	retained	2	0/2	10.1.115.20	file:///C/Documents
⚠️	Antivirus	trojan	retained	2	0/2	10.1.115.20	file:///C/Documents
⚠️	Antivirus	virus	retained	2	0/2	10.1.115.20	file:///C/Documents
⚠️	Antivirus	potentially unwanted application	retained	1	0/1	10.1.115.184	file:///C/Users/BERTI/Desktop/
⚠️	Antivirus	potentially unwanted application	retained	3	0/3	10.1.115.184	file:///C/Users/BERTI/Desktop/
⚠️	Antivirus	trojan	retained	1	0/1	10.1.115.20	file:///C/Users/Kurt/Desktop/
🟡	Antivirus	trojan	cleared by deleting	1	0/1	10.1.115.20	file:///C/Users/Kurt/Desktop/
🟡	Web protection	An attempt to connect to URL... Blocked by Anti-Phishing block...	blocked	1	0/1	10.1.115.62	https://www.antiko.de
🟡	Antivirus	trojan	cleared by deleting	1	0/1	10.1.115.184	file:///C/Users/Bertrand/Desktop/
🟡	Web protection	An attempt to connect to URL... Blocked by Anti-Phishing block...	blocked	1	0/1	10.1.115.184	https://www.antiko.de
🟡	Antivirus	Dynamic Threat Defense	deleted	1	0/1	10.1.115.184	file:///E/epcdemo/I
🟡	Antivirus	Dynamic Threat Defense	deleted	1	0/1	10.1.115.184	file:///C/Users/Bertrand/Desktop/
🟡	Antivirus	Win32/TrojanDownloader.Agent... cleaned by deleting	1	0/1	10.1.202.21	file:///C/Users/Alain/Desktop/	

- D'avoir la liste de tous les appareils protégés par Eset et de connaître ceux présentant un problème.

- Lorsque je clique sur un des ordinateurs de la liste, je peux, connaître leurs principales caractéristiques ainsi qu'avoir le détail de leurs problèmes.

- Toujours sur la fiche de l'ordinateur, des menus qui me permettent d'agir sur chacun d'entre eux en leur programmant des tâches spécifiques par exemple ou connaître la version de leurs principaux logiciels.

NAME	VENDOR	VERSION	SIZE [MB]	AGENT SUPPORTS UNIN.	LATEST APPLICATION VI.	VERSION CHECK STATU:
Update for Windows 10 for x64-based Systems (KB4400730)	Microsoft Corporation	2.55.0.0	0	yes		
Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.616...	Microsoft Corporation	9.0.30729.6161	13	yes		
ESET Management Agent	ESET, spol. s r.o.	7.2.1267.0	170	yes	7.2.1267.0	Up-to-date version
ESET Endpoint Security	ESET, spol. s r.o.	8.0.2038.0	222	yes	7.3.2044.0	Up-to-date version
Microsoft Edge Update		1.3.139.59		no		
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.414...	Microsoft Corporation	9.0.30729.4148	10	yes		
Microsoft Visual C++ 2015-2019 Redistributable (x64) - 14.24...	Microsoft Corporation	14.24.28127.4	23	no		
Microsoft Visual C++ 2015-2019 Redistributable (x86) - 14.24...	Microsoft Corporation	14.24.28127.4	20	no		
VMware Tools	VMware, Inc.	11.1.5.16724464	94	yes		
Microsoft Edge	Microsoft Corporation	87.0.664.55		no		

Sur la figure ci-dessus, on remarque la présence de deux logiciels Eset installés sur l'ordinateur. L'un est l'antivirus, l'autre et un agent que j'ai déployé sur chacun des postes, en plus de l'antivirus. C'est lui qui fait le lien avec la console d'administration.

Cette console permet également de programmer la mise à jour du système d'exploitation de l'ensemble des ordinateurs. Toutefois, je continu d'utiliser le service WSUS bien que le supprimer soulagerais quelque peu le serveur. En effet, la programmation est plus subtile grâce à la création de groupes d'ordinateurs que ne permet pas la console. Ainsi, ça me permet de maîtriser leur déploiement, de ne pas saturer le réseau ni ralentir des ordinateurs qui seraient en cours d'utilisation. Toutefois, je l'utilise pour vérifier que le service WSUS à bien fait le job et pour corriger individuellement ceux qui auraient rencontré un problème à l'installation.

Les mises à jour des autres équipements et bibliothèques du réseaux

- Les mises jour des serveurs sont réalisés le seul jour de fermeture complet au public et pour lequel aucun professionnel ne travaille, à savoir les lundis. Elles sont faites manuellement bout en bout afin de vérifier que chaque étape se passe bien, notamment leur redémarrage. Ce choix de fréquence a été fait pour ne pas perturber le travail des bibliothécaires ni la réception du public.
- Celles des équipements plus spécifiques comme les pares-feux ou le proxy sont réalisées par les prestataires qui nous les fournissent. C'est souvent compris dans les services proposés par les entreprises. Ça nous permet d'être plus serein également car ce sont des appareils très spécifiques. Ainsi, on sait que c'est réalisé par des personnes qui le font très régulièrement et qui ont la

possibilité de sauvegarder la configuration ainsi que la remonter s'il venait à y avoir un problème.

- De plus, il y a, à Epinal, un petit groupe d'ordinateurs qui ne sont utilisés que durant des animations, des ateliers d'initiations ou des réunions. Ceux-ci, je ne les mets à jour que quelques jours avant un évènement. Leur faible nombre (12) me permet de tous les faire manuellement en une seule journée maximum, en fonction de l'importance de la mise à jour de l'OS et/ou des logiciels qui seront utilisés.
- Enfin, en ce qui concerne les autres bibliothèques du réseau, il y a deux cas de figure :
 - Si elles ont un bibliothécaire référent numérique, c'est lui qui réalise, les mises à jour de sa structure. Je reste toutefois à sa disposition s'il venait à avoir un problème. De plus, je réalise régulièrement des tutoriels que je leur mets à disposition, notamment pour les manipulations spécifiques comme la désactivation et réactivation de reboot restore.
 - Si elles sont trop petites pour justifier un poste de ce type, je me déplace donc certaines demi-journées durant lesquelles elles sont fermées, et j'effectue toutes les mises à jour décrites précédemment manuellement pour les quelques ordinateurs qui s'y trouvent (pas plus de 6 pour la plus grande). Ainsi que du matériel numérique mis à la disposition du public et de leurs logiciels.

Toutes ces mises à jour qui semblent me prendre beaucoup de temps, ont un intérêt pour moi car elles me permettent par la même occasion, de vérifier que tout fonctionne bien. En effet, j'ai besoin que les machines démarrent correctement, sur les bonnes sessions, avec le chargement de ce que j'ai programmé au démarrage (par exemple le lancement du navigateur avec l'affichage de la page d'accueil de notre catalogue pour les ordinateurs dédiés à notre OPAC (Online Public Access Catalog) ou l'affichage de la page de connexion du portail captif de notre Proxy pour les ordinateurs mis à la disposition du public). Enfin, de vérifier que les logiciels se lancent sans problème.

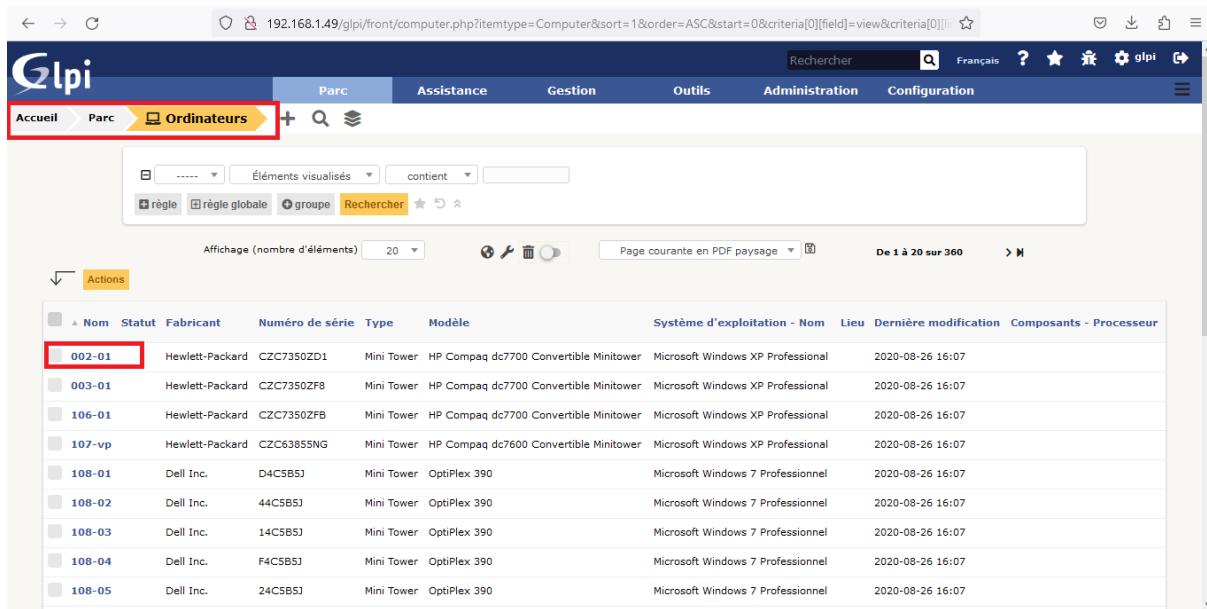
Tout ce travail s'inscrit dans le cadre de la maintenance préventive du parc. C'est sûrement la tâche la plus simple que j'ai à réaliser, celle-ci étant normalement destinée à être accessible à tout utilisateur. La complexité provient du fait que le parc est plutôt conséquent et qu'il me faut des outils pour m'y retrouver, d'autant que je suis très souvent amené à être interrompu entre deux manipulations.

b) Les actions du quotidien plus spécifiques.

Inventaire des appareils et gestion des stocks

Tout d'abord, je dois toujours avoir connaissance des réels états de chaque ordinateur. Pour cela, je m'appuie sur le logiciel de gestion des actifs GLPI (gestionnaire libre de parc informatique). Installé sur une machine virtuelle d'un de nos hyperviseurs, il me permet de :

- Avoir une liste complète des appareils gérés dans mon parc



The screenshot shows the GLPI web interface for managing computer assets. The top navigation bar includes links for Accueil, Parc, Assistance, Gestion, Outils, Administration, and Configuration. The 'Parc' tab is selected. Below the navigation is a search bar with options for 'règle', 'règle globale', 'groupe', and 'Rechercher'. The main content area displays a table of computer inventory. The columns include Nom, Statut, Fabricant, Numéro de série, Type, Modèle, Système d'exploitation - Nom, Lieu, Dernière modification, and Composants - Processeur. One row in the table is highlighted with a red border around the 'Nom' column, which contains the value '002-01'. The table lists ten entries, all of which have 'Microsoft Windows XP Professional' listed under 'Système d'exploitation - Nom'.

Nom	Statut	Fabricant	Numéro de série	Type	Modèle	Système d'exploitation - Nom	Lieu	Dernière modification	Composants - Processeur
002-01		Hewlett-Packard	CZC7350ZD1	Mini Tower	HP Compaq dc7700 Convertible Minitower	Microsoft Windows XP Professional		2020-08-26 16:07	
003-01		Hewlett-Packard	CZC7350ZF8	Mini Tower	HP Compaq dc7700 Convertible Minitower	Microsoft Windows XP Professional		2020-08-26 16:07	
106-01		Hewlett-Packard	CZC7350ZFB	Mini Tower	HP Compaq dc7700 Convertible Minitower	Microsoft Windows XP Professional		2020-08-26 16:07	
107-vp		Hewlett-Packard	CZC63855NG	Mini Tower	HP Compaq dc7600 Convertible Minitower	Microsoft Windows XP Professional		2020-08-26 16:07	
108-01		Dell Inc.	D4C5B5J	Mini Tower	OptiPlex 390	Microsoft Windows 7 Professionnel		2020-08-26 16:07	
108-02		Dell Inc.	44C5B5J	Mini Tower	OptiPlex 390	Microsoft Windows 7 Professionnel		2020-08-26 16:07	
108-03		Dell Inc.	14C5B5J	Mini Tower	OptiPlex 390	Microsoft Windows 7 Professionnel		2020-08-26 16:07	
108-04		Dell Inc.	F4C5B5J	Mini Tower	OptiPlex 390	Microsoft Windows 7 Professionnel		2020-08-26 16:07	
108-05		Dell Inc.	24C5B5J	Mini Tower	OptiPlex 390	Microsoft Windows 7 Professionnel		2020-08-26 16:07	

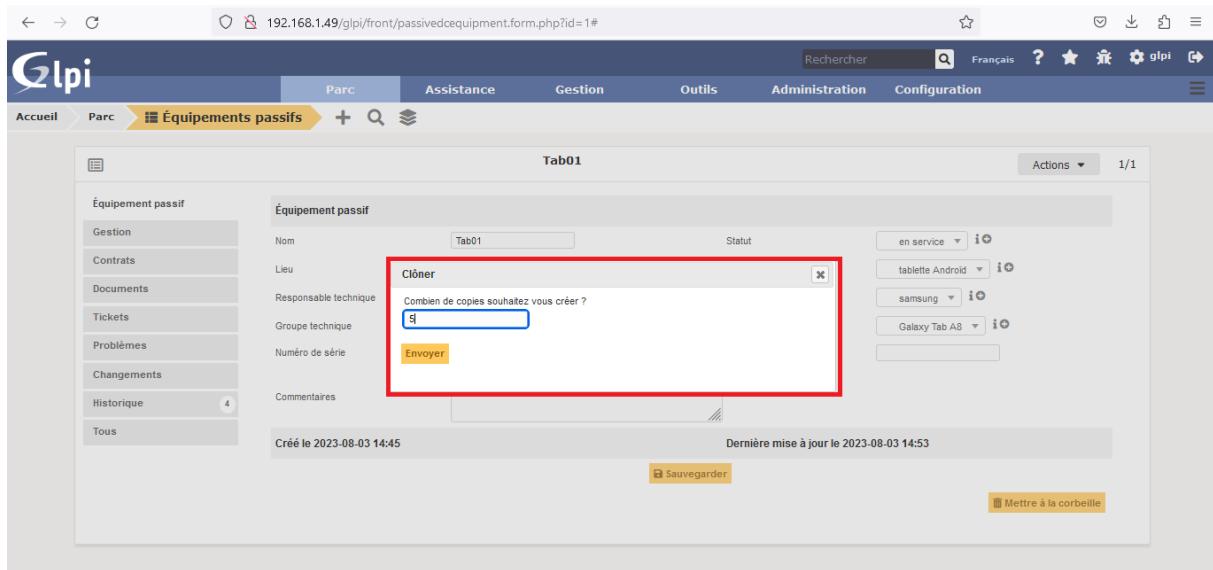
- Remonter les informations des ordinateurs (nom de l'ordinateur, ses composants, son système d'exploitation ou bien encore les logiciels installés), grâce un agent, appelé FusionInventory, sur chacun d'entre eux, appelé FusionInventory. Lorsqu'est affiché la liste des ordinateurs, je clique sur le nom de l'ordinateur visé pour afficher sa fiche. Il ne me reste plus qu'à renseigner la localisation voire la personne à laquelle il est affecté. Grâce à l'interconnexion des sites, les informations des ordinateurs des autres bibliothèques sont également remontés, ce qui me permet de connaître également l'état des autres parcs. Je peux également lui ajouter des composants manuellement si besoin.

The screenshot shows the GLPI software interface for managing computer components. On the left, a sidebar lists various categories like 'Ordinateur', 'Analyse d'impact', and 'Systèmes d'exploitation'. The 'Composants' category is selected and highlighted with a red box. In the main area, a table displays existing components such as 'Alimentation', 'Batterie', 'Boîtier', etc. A modal dialog box titled 'Ajouter un nouveau composant' is overlaid on the table, also highlighted with a red box. The dialog contains fields for 'Nom' (Name), 'Type de composant' (Component type), 'Caractéristiques' (Characteristics), 'Inventaire automatique' (Automatic inventory), and 'Actions' (Actions). The 'Nom' field contains the placeholder '----'.

- Inventorier tous nos appareils informatiques et numériques non compatibles avec l'agent. Je dois simplement compléter les informations manuellement.

The screenshot shows the GLPI software interface for managing passive equipment. The top navigation bar includes 'Accueil', 'Parc', 'Équipements passifs' (highlighted with a red box), 'Assistance', 'Gestion', 'Outils', 'Administration', and 'Configuration'. The main area is titled 'Tab01' and contains a form for creating a new passive equipment item. The form fields include 'Nom' (Name) set to 'Tab01', 'Statut' (Status) set to 'en service', 'Type' (Type) set to 'tablette Android', 'Fabricant' (Manufacturer) set to 'samsung', 'Modèle' (Model) set to 'Galaxy Tab A8', 'Lieu' (Location) set to 'espace jeunesse', 'Responsable technique' (Technical responsible) set to '----', 'Groupe technique' (Technical group) set to '----', 'Numéro de série' (Serial number) set to '0123456789', and 'Commentaires' (Comments). Buttons for 'Cloner' (Clone) and 'Amender le commentaire' (Edit comment) are visible at the top right. A note at the bottom indicates the item was created on 'Créé le 2023-08-03 14:45' and last updated on 'Dernière mise à jour le 2023-08-03 14:53'. Action buttons 'Sauvegarder' (Save) and 'Mettre à la corbeille' (Put in trash) are at the bottom right.

Pour gagner du temps, lorsque je reçois un type d'appareil ou un modèle en plusieurs exemplaires, je crée une première fiche que je clone autant de fois que j'ai de modèle. Je dois simplement ne pas oublier de modifier son nom voire sa localisation.



En revanche, je n'ai aucune vue sur l'état de leurs mises à jour ainsi que de leurs applications.

Une autre solution pour mes appareils mobiles aurait été d'investir dans un MDM (Mobile Device Management). Ce dispositif me permettrait de gérer à distance les appareils, de connaître l'état de l'OS et des logiciels ou encore installer de nouvelles applications. Mais c'est un dispositif que j'ai jugé trop coûteux alors que je n'ai qu'un petit parc d'appareils mobiles. De plus, ils ne sont pas tous sous le même système d'exploitation (Android, iOS), le MDM n'aurait pas pu être compatible avec tous. Enfin, il faut forcément les connecter au réseau WIFI pour que la synchronisation se fasse, ce qui fait que je ne pouvais pas gérer les appareils présents sur les autres sites.

- Connaître l'état des garanties des appareils ainsi que les échéances des contrats de maintenance. Il me suffit de les saisir manuellement en ajoutant une date d'échéance et en programmant un rappel par mail pour me rappeler de la fin imminente d'un contrat, afin de relancer les prestataires ou demander de nouveaux devis.

The screenshot shows the GLPI computer form interface. On the left, there is a sidebar with various categories: Analyse d'impact, Systèmes d'exploitation (with 1 item), Composants (with 21 items), Volumes (with 1 item), Logiciels, Connexions, Ports réseau (with 1 item), Gestion (highlighted with a red box), Contrats, Documents, Virtualisation, Antivirus, Base de connaissances, Tickets, Problèmes, Changements, Liens externes, Certificats, and Verrous.

The main content area is titled "Cycle de vie du matériel". It contains fields for Date de commande (2023-07-15), Date d'achat (2023-08-01), Date de livraison (2023-08-03), Date de mise en service (2023-08-04), Date de dernier inventaire physique (2023-08-03), and Date de réforme. Below this is the "Informations financières et administratives" section, which includes fields for Fournisseur, Budget, Numéro de commande, Numéro d'immobilisation, Numéro de facture, Bon de livraison, Valeur (0.00), Valeur extension garantie (0.00), Valeur nette comptable, Type d'amortissement, Durée d'amortissement (0 an), Coefficient d'amortissement (0), TCO (valeur + montant des interventions) (0.00), TCO mensuel (0.00), Criticité business, Commentaires, and Informations sur la garantie.

At the bottom right of the main form are two buttons: "Sauvegarder" and "Supprimer définitivement".

- Surveiller les stocks des consommables tels que les cartouches d'encre des imprimantes ou les puces RFID. J'entre le stock au moment des achats, et je renseigne à chaque fois que j'utilise un nouvel élément. J'ai aussi programmé des rappels pour m'avertir lorsque le stock atteint un seuil critique que j'ai défini afin de relancer un nouvel achat par anticipation, avant qu'il n'atteigne 0.

The screenshot shows the GLPI Consummables model creation page. The top navigation bar includes Accueil, Parc, Consommables (highlighted with a yellow arrow), Rechercher, Français, and other links. The main form is titled "Modèle de consommable" and "Nouvel élément - Modèle de consommable". It contains fields for Nom (Puces livres), Type (puce rfid), Référence, Fabricant (nedap), Responsable technique (turck julien), Groupe technique, Lieu de stockage (salle serveur), Commentaires, Seuil d'alerte (set to 10), and Numéro d'inventaire. At the bottom right is a "+ Ajouter" button.

C'est d'autant plus pertinent que les achats informatiques sont centralisés. En effet, c'est mon chef de service ou moi-même qui :

- Commande les appareils et consommables, après validation de l'achat par la direction
- Vérifie les colis
- Distribue dans les services en fonction des besoins

Sauvegardes des fichiers

Tout autre chose, mais au combien important, j'effectue régulièrement des vérifications du bon fonctionnement de nos sauvegardes automatisées et je réalise des sauvegardes des postes lorsque je reçois un nouveau modèle d'appareil ou lorsqu'il y a une modification importante faite sur un système.

Les fichiers nécessaires au bon fonctionnement des bibliothèques sont sauvegardés de manière automatisée, c'est à dire qu'elles sont paramétrées grâce à logiciel. Ça me permet de ne pas oublier un soir où je suis préoccupé par autre chose ou absent du site par exemple. Et ainsi ne pas me retrouver avec une sauvegarde incomplète à un moment critique. Les sauvegardes sont réalisées par deux gestionnaires :

- Veeam Backup pour les sauvegardes des serveurs virtuels
- Microsoft Backup pour les dossiers des agents

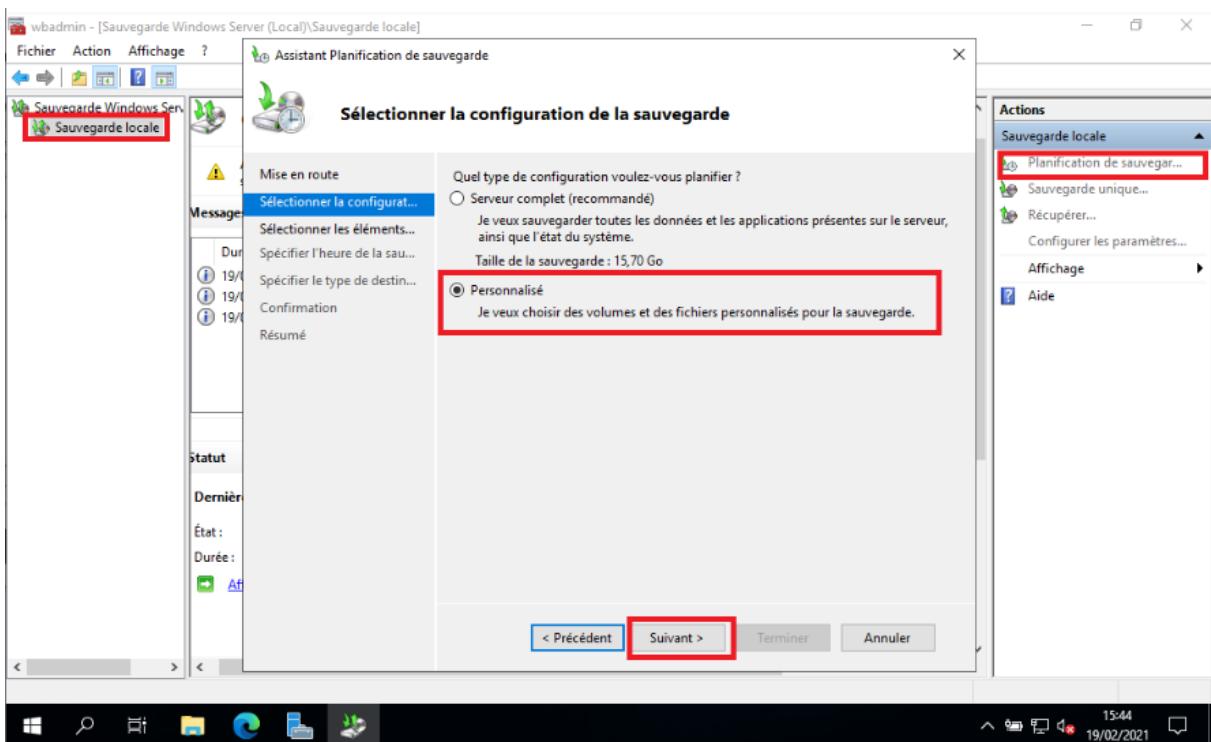
Windows Backup permet également de faire un backup des serveurs. Cependant, je trouve pertinent de privilégier le gestionnaire Veeam pour les serveurs virtuels, bien qu'il soit payant.

En effet, il propose plus de fonctionnalités telles que la prise d'instantanées en l'état ce qui est pratique lorsque je réalise des essais pour lesquels je ne suis pas certain du résultat. De plus, Windows Backup n'est disponible que pour les serveurs Windows. Or, je sauvegarde également des machines virtuelles sous Linux telle que celle dédiée à GLPI qui fonctionne avec l'OS Debian.

Microsoft Backup

C'est une fonctionnalité disponible au moment de l'attribution des rôles et fonctionnalités des serveurs (Voir activité 2). Ce service est accessible depuis la console d'administration dans les outils d'administration.

Pour planifier les sauvegardes journalières des dossiers uniquement, je clique sur « Planification de sauvegardes » et je choisi l'option « Personnalisé ». J'indique ensuite les dossiers à sauvegarder, la fréquence et le type de sauvegarde ainsi que le support de destinations.



Quel que soit le gestionnaire, deux types de sauvegardes ont été programmés :

- Une sauvegarde incrémentale journalière, les soir des jours ouvrés

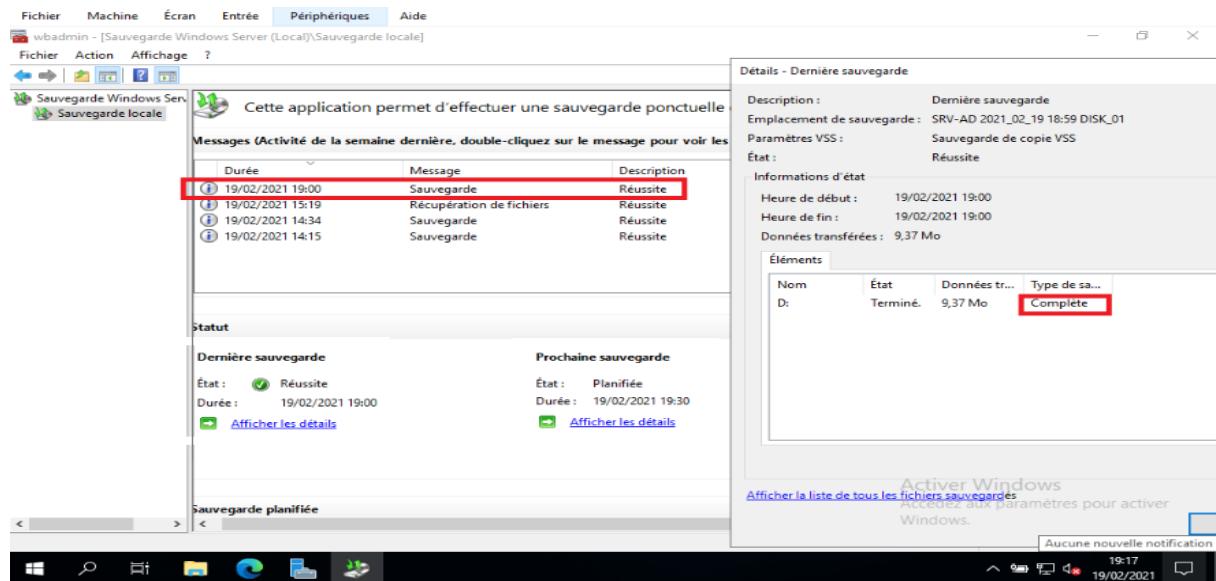
La sauvegarde incrémentale ne sauvegarde que les modifications apportées au volume par rapport à la sauvegarde précédente (quel soit complète ou incrémentale). Ainsi, c'est celle qui prend le moins de temps à se faire. En revanche, c'est celle qui prend le plus de temps à être remontée du fait que le gestionnaire va devoir remonter la dernière sauvegarde complète connue et intégrer chacune des modifications de chaque incrémentale réalisée.

- Une sauvegarde complète hebdomadaire la nuit du dimanche au lundi. Le lundi étant le seul jour de fermeture au public et le seul jour de repos de tous les bibliothécaires, cela permet à une sauvegarde très importante de déborder sur la journée suivante sans gêner.

La sauvegarde complète, va réaliser une sauvegarde de tout le volume. C'est celle qui prend le plus de place et qui prend le plus de temps à se réaliser. Elle reste toutefois indispensable, du fait que les autres types (incrémentale et différentielle), s'appuient en partie sur la dernière sauvegarde complète connue pour calculer les modifications à sauvegarder.

Je trouve ce choix pertinent du fait du volume à sauvegarder et le temps imparti pour le faire. En effet, le volume total est de plusieurs Terra-octet. Les sauvegardes

complètes prennent donc énormément de temps et ne seraient pas terminées avant que mes collègues ne commencent leur journée. Le réseau serait alors fortement sollicité. De plus, ça augmente les chances qu'elles soient interrompues par un incident survenu la nuit (panne de courant, panne d'un matériel...). Enfin, ça prendrait beaucoup trop de place sur les disques de cumuler une sauvegarde complète par jour.



Enfin, ces sauvegardes sont réalisées sur différents supports afin de respecter la règle du 3-2-1, préconisée par tous les professionnels. Ça se présente ainsi :

	Signification	Matérialisation	Intérêt
3	3 jeux de données dont celle en production	<ul style="list-style-type: none"> Le premier jeu est sur le serveur en lui-même. C'est celui qui est accessible et modifié par les salariés afin qu'ils puissent réaliser leurs tâches quotidiennes. Un deuxième jeu est créé durant la sauvegarde. Un dernier jeu est créé lors d'une copie envoyée sur un NAS. 	Si un des jeux venait à être corrompu ou inaccessible, il en reste toujours un de secours le temps qu'un nouveau soit créé. Ça évite ainsi de se retrouver sans filet de sécurité
2	2 supports minimum différents utilisés	<ul style="list-style-type: none"> Le premier jeu est contenu sur le disque dur du serveur Le deuxième est contenu sur un disque dur rattaché au serveur au 	Ça permet de ne pas être dépendant d'une panne d'une machine.

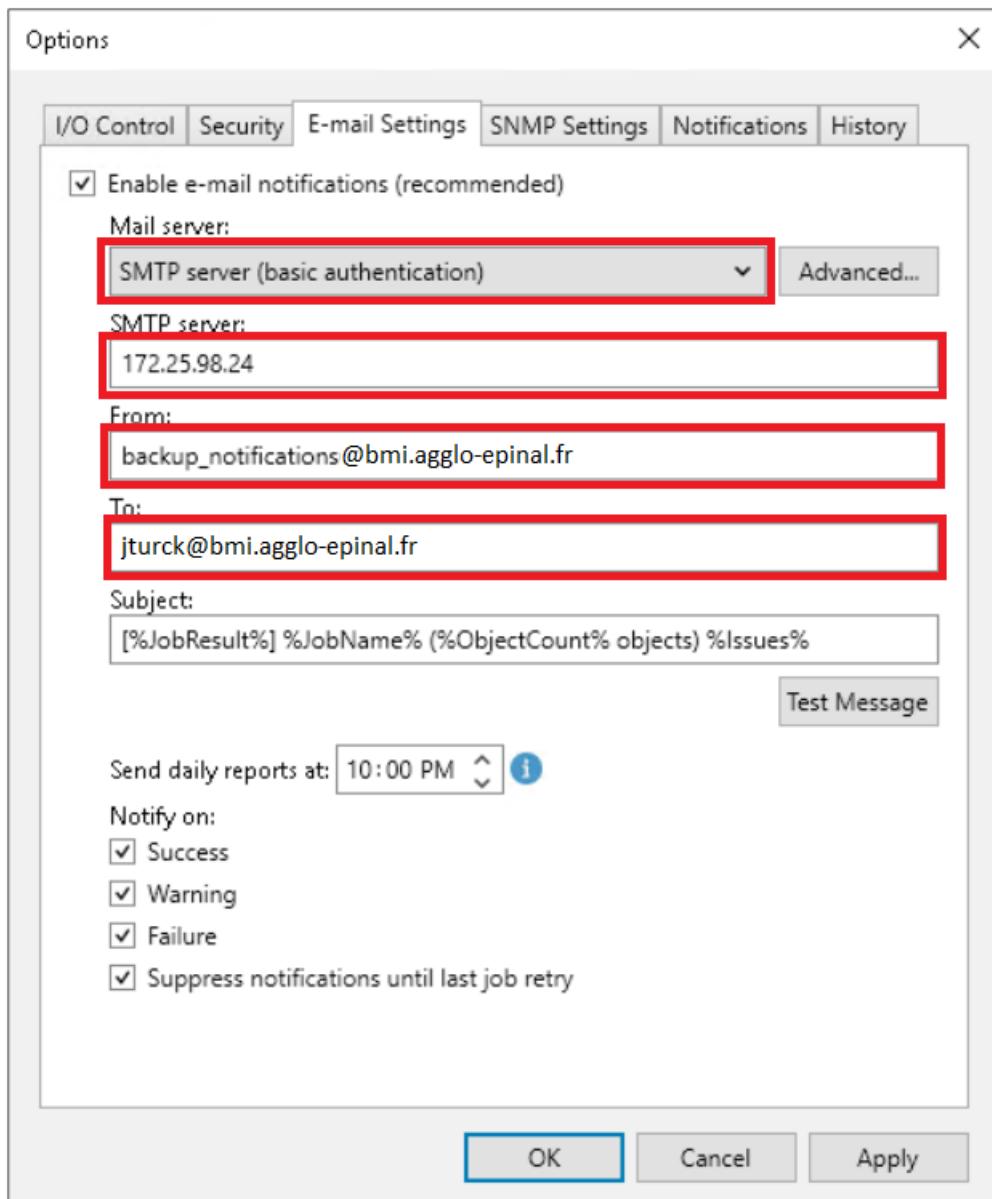
		<p>moment de la sauvegarde</p> <ul style="list-style-type: none"> Le dernier est contenu sur un NAS (Network Attached Storage) 	
1	1 site distant possède un des jeux	<ul style="list-style-type: none"> Le serveur et les disques durs externes sont à la bibliothèque d'Epinal Le NAS se situe à la mairie d'Epinal 	<p>En cas de gros incident dans un des bâtiment (incendie, virus) un jeu se trouve en sécurité loin de la catastrophe et pourra être utilisé pour relancer le service</p>

Mon rôle est donc de contrôler que les sauvegardes se soient bien déroulées.

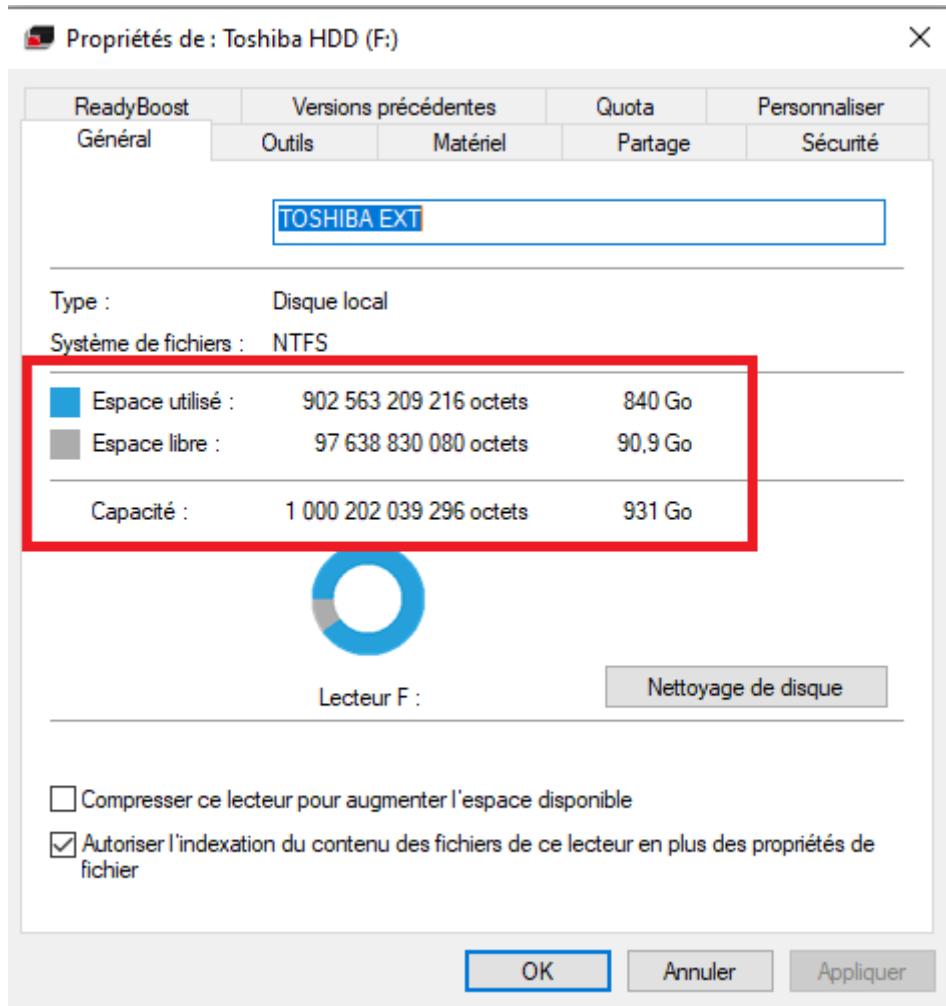
- Mes contrôles :

- Les gestionnaires fournissent des journaux des événements dont le statut des tâches exécutées
- Le gestionnaire Veeam Backup permet également de recevoir un compte rendu des tâches par mail

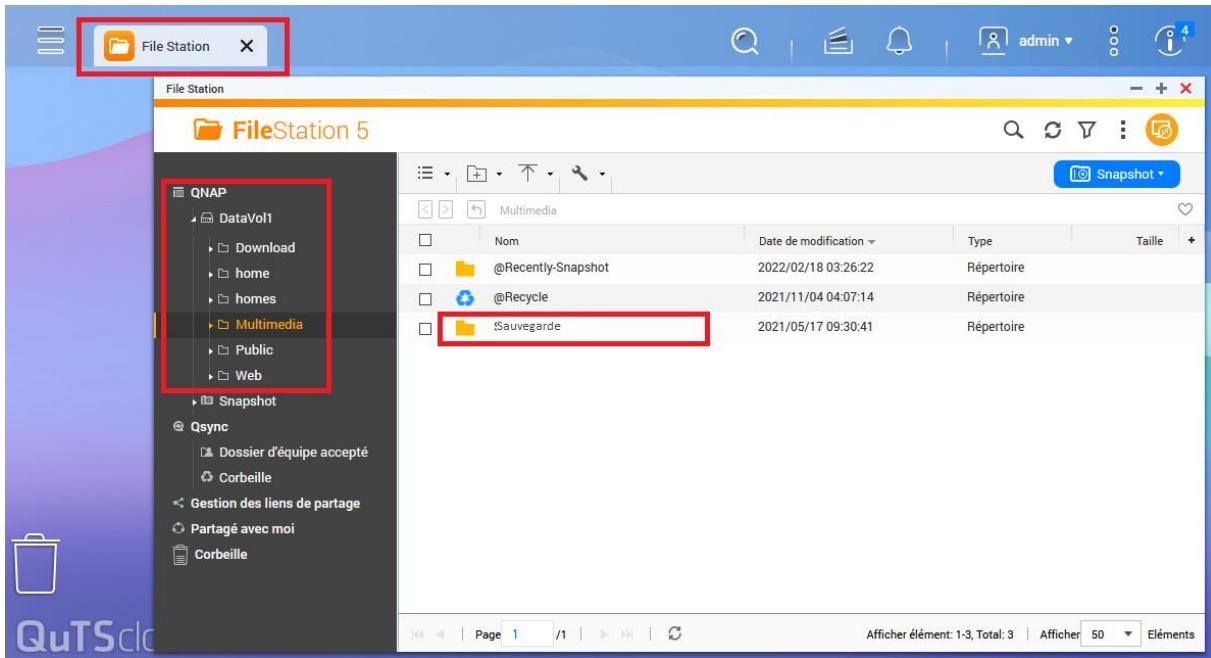
Pour se faire, dans la console d'administration, je me rends dans les options générales et je clique sur l'onglet « E-mail Settings ». Je sélectionne SMTP server. J'indique l'adresse IP du serveur de messagerie de la mairie d'Epinal. J'indique l'adresse que j'ai créé pour veeambbackup dans la base du serveur. Enfin, j'indique mon adresse de messagerie.



- Je vérifie au niveau du disque dur externe, que son volume correspond bien au volume à sauvegarder et que la date de dernière modification de son dossier de sauvegarde est bien la veille
J'y accède en allant dans le menu démarrer puis en cliquant sur « Ce PC ». J'effectue ensuite un clic droit sur l'icône du disque dur pour ouvrir ses propriétés et connaître son espace utilisé. Puis je double clique sur la même icône pour afficher son contenu.



- Je vérifie qu'il y a bien sur le NAS un dossier créé avec les documents modifier de la veille et qu'ils s'ouvrent correctement en testant deux ou trois au hasard
Pour se faire, j'ouvre l'icône « file station » présent sur le bureau du NAS QNAP. J'accède ensuite aux dossiers voulus en double-cliquant dessus.



- Mes champs d'interventions :

- Un des journaux indique qu'une des tâches a échoué :

- _ Je lis le journal d'événements du serveur pour vérifier qu'il n'y a pas eu une extinction de la machine (dû à une coupure de courant par exemple)
- _ Je vérifie que les espaces disques ne soient pas saturés
- _ Je vérifie que la sauvegarde ne prenne pas plus de place que prévu
- _ Je relance une sauvegarde manuellement

- Le NAS n'est plus joignable :

- _ Je vérifie avec le service informatique de la mairie que la liaison n'est pas coupée entre la bibliothèque et la mairie
- _ Je vérifie avec le service informatique de la mairie que le NAS est toujours joignable sur leur réseau
- _ Je vais dans leurs locaux vérifier l'état des disques. Si un disque dur sur les 8 ne répond plus, des disques durs de secours sont prévus. Je remplace le défaillant à chaud (c'est-à-dire sans éteindre le NAS). Le NAS reconstitue ensuite la sauvegarde à partir des données qu'il a sur les autres disques.

Cette manipulation est possible du fait que le RAID utilisé est le RAID 50.

RAID

Le RAID (Redundant Array of Independent Disks ou regroupement redondant de disques indépendants) est un ensemble de techniques de répartition des données sur plusieurs disques.

Le RAID 50 est l'alliance des techniques du RAID 0 et du RAID 5 :

_ Le RAID 0 (ou volume agrégé par bandes) répartie les données sur l'intégralité des disques.

- Avantages :
 - C'est celui qui offre les meilleures performances en lecture et écriture.
 - L'intégralité des disques sont utilisés pour sauver les données. Il n'y a aucune perte de capacité de stockage
- Inconvénients :
 - Il ne tolère aucune panne de disques

_ Le RAID 5 (ou volume agrégé par bandes à parité répartie) répartie les données sur n-1 disques (3 sur 4 par exemple) de chaque bande. Le dernier disque est réservé à un bloc de parité contenant des informations sur les données des autres disques.

- Avantages :
 - Il tolère la panne d'un disque dur par bande
 - Il offre de bonnes performances en lecture
- Inconvénients :
 - Les capacités de stockages de données sont réduites d'un disque par bandes (Par exemple si ma bande est composée de 4 disques d'1 To chacun, je ne pourrais stocker que 3 To de données).
 - Du fait des calculs des blocs de parités, les performances en écriture sont réduites

_ RAID 50 (ou 5 + 0) est le fait de combiner la répartition du 0 sur plusieurs nœuds, chacun basé sur un sous-système du 5, donc chacun protégé par un bloc de parité.

The screenshot displays a storage management interface with two main sections:

Storage Pool List - Total 2 Pool(s)

Name/Alias	Controller	Capacity	Allocated	Free Size	Dedup Saving	Status
pool2	SCA	6.78 TB	1.24 MB	6.78 TB	0 KB (0%)	Ready

RAID Group of Storage Pool pool2

Name/Alias	Capacity	RAID Type	Status
RAID Group pool2-0	3.39 TB	RAID5	Ready
REXP#1: Disk 1	932.00 GB	Ready	
REXP#1: Disk 2	932.00 GB	Ready	
REXP#1: Disk 3	932.00 GB	Ready	
REXP#1: Disk 4	932.00 GB	Ready	
REXP#1: Disk 5	932.00 GB	Ready	
RAID Group pool2-1	3.39 TB	RAID5	Ready
REXP#1: Disk 6	932.00 GB	Ready	
REXP#1: Disk 7	932.00 GB	Ready	
REXP#1: Disk 8	932.00 GB	Ready	
REXP#1: Disk 9	932.00 GB	Ready	
REXP#1: Disk 10	932.00 GB	Ready	

Pour son utilisation, c'est pour moi un bon compromis financier. En effet, il n'est utilisé que pour stocker des copies de fichiers et n'est sollicité qu'en cas de pertes de ceux-ci sur ses deux autres supports. Nous n'avons donc pas besoin d'investir dans un RAID 1 qui offre de meilleures performances en lecture et une tolérance aux pannes accrue mais qui est beaucoup plus couteux, si l'on veut la même capacité de stockage.

Sauvegarde des postes

Enfin, je sauvegarde aussi mes postes de travail. En revanche, elles sont réalisées manuellement. Pour ce faire :

- Logiciel utilisé : Clonezilla
 - Avantages :
 - _ Bootable à partir d'une clé USB
 - _ la sauvegarde du disque se fait sur un simple disque dur externe.
 - _ Logiciel libre et gratuit
 - Défauts :
 - _ Sauvegarde le disque dans son ensemble. La sauvegarde peut donc contenir des fichiers personnels ainsi que les informations spécifiques à chaque PC
 - _ Nécessite que le disque dur à qui on injecte la copie, ai, au minimum, la même capacité de stockage que celui cloné.
 - _ Les procédures prennent plusieurs minutes à se lancer, à cause d'un nombre important d'étapes à réaliser
 - _ Toutes les étapes se font par le biais d'une console, ce qui est perturbant, voire rebutant, lorsque l'on n'a pas l'habitude.

```

*****.
PS. La prochaine fois vous pourrez exécuter cette commande directement :
/usr/sbin/ocs-sr -q2 -c -j2 -zip -i 4096 -fsck -senc -p choose savedisk 2018-04-18-13-img-ancien-disque-dur sda
Cette commande a été enregistrée sous le nom suivant pour usage ultérieur si nécessaire: /tmp/ocs-2018-04-18-13-img-ancien-disque-dur-2018-04-18-13-31
*****.
Appuyez sur "Entrée" pour continuer...
Activating the partition info in /proc... done!
Selected device [sda] found!
The selected devices: sda
Searching for data/swap/extended partition(s)...
Excluding busy partition or disk...
Unmounted partitions (including extended or swap): sda1 sda2 sda3 sda4
Collecting info.... done!
The data partition to be saved: sda1 sda2 sda3 sda4
Activating the partition info in /proc... done!
Selected device [sda1] found!
Selected device [sda2] found!
Selected device [sda3] found!
Selected device [sda4] found!
The selected devices: sda1 sda2 sda3 sda4
Getting /dev/sda1 info...
Getting /dev/sda2 info...
Getting /dev/sda3 info...
Getting /dev/sda4 info...
*****.
La prochaine étape consiste à sauvegarder le disque ou la partition de cette machine sous forme d'une image:
*****.
Machine: VirtualBox
sda (137GB_VBOX_HARDDISK__VBOX_HARDDISK_VB585944d7-726be39b)
sda1 (499M_ntfs_Récupérati(In_VBOX_HARDDISK_)_VBOX_HARDDISK_VB585944d7-726be39b)
sda2 (99M_vfat_NO_NAME(In_VBOX_HARDDISK_)_VBOX_HARDDISK_VB585944d7-726be39b)
sda3 (16M_MS_Reserved_Partition(In_VBOX_HARDDISK_)_VBOX_HARDDISK_VB585944d7-726be39b)
sda4 (127.4G_ntfs(In_VBOX_HARDDISK_)_VBOX_HARDDISK_VB585944d7-726be39b)
*****.
-> "/home/partimag/2018-04-18-13-img-ancien-disque-dur".
Etes-vous sûr de vouloir continuer? (y/n) y

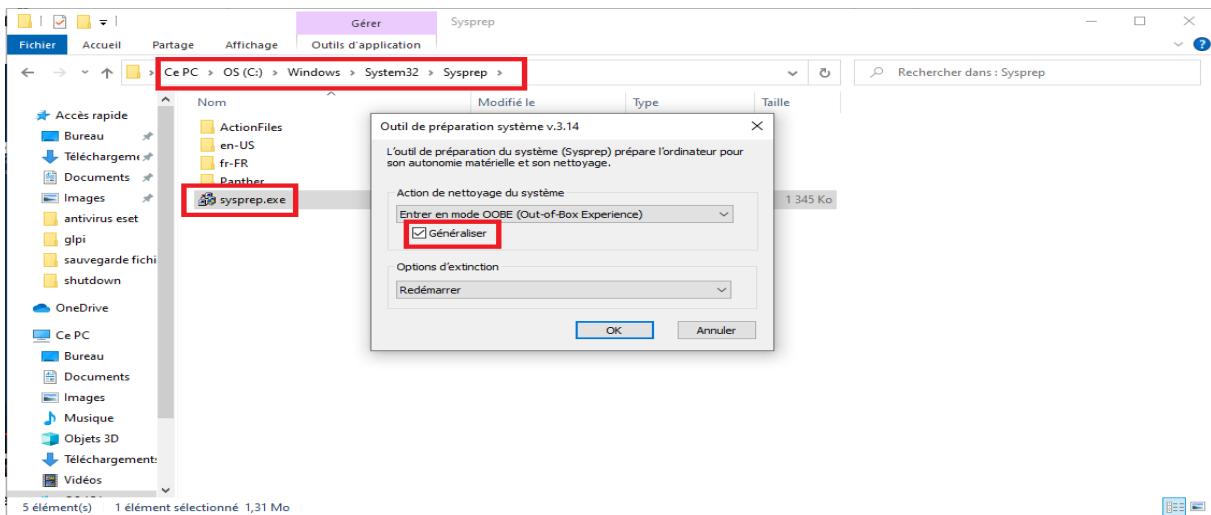
```

- Précautions au préalable :
 - Je sauvegarde des ordinateurs types (un pour chaque modèle existant dans le réseau) que je ne mets pas à disposition. Ils ne possèdent donc aucun fichier personnel
 - Je les mets régulièrement à jour et ils sont paramétrés comme pour être opérationnels.
 - Je réalise un **Sysprep**, afin de supprimer les informations spécifiques du PC tel que le SID (Security Identifier) de l'OS qui doit être unique pour chaque PC Windows présent dans un même réseau. Celui-ci est disponible dans le dossier HKEY_USERS de l'éditeur de registre

Sysprep :

Outil intégré à l'OS qui permet d'effacer certaines informations spécifiques à chaque ordinateur et qui peuvent gêner dans le déploiement d'une image.

Il est disponible en suivant le chemin suivant : <C:/Windows/System32/Sysprep>
Il suffit ensuite de cocher la case « généraliser »



- Le déploiement des images

Je déploie les images dans 3 cas de figures :

- Au moment du paramétrage de plusieurs nouveaux ordinateurs identiques.
En effet, au moment de la réception d'une commande de plusieurs ordinateurs similaires, j'en paramètre un complètement. Puis je crée une ISO de son disque que je déploie sur tous les autres PC. Ça m'assure que tous les PC seront identiques. Je dois simplement bien vérifier la configuration du PC source, afin de ne pas déployer une série qui comporterait des erreurs.
- À la suite d'une panne critique du système d'un PC
- Lors des mises à jour les plus importantes de l'OS des PC publics.
En effet, je n'effectue pas les mises à jour de l'OS manuellement sur tous les PC. Il y en a beaucoup et Windows 10 est très gourmand en mises à jour (1 à 2 fois par mois). Aussi, je ne mets à jour régulièrement que celui que je garde dans mes bureaux et je déploie son image au moment des changements de versions ou par petits paquets lorsqu'il y a un cumul de plusieurs mois sans Maj.
Simplement, l'opération s'étale sur plusieurs jours du fait de la lenteur du processus. Parce qu'également, je ne peux pas lancer ce logiciel durant les heures d'ouvertures au public. Ça m'obligerait à soit rester à côté de l'ordinateur tout le long de la restauration afin d'éviter que quelqu'un ne stoppe le processus ou bien me vole mes disques amovibles.

Une autre manière de procéder aurait été d'utiliser la version serveur de la solution. Elle apporte plusieurs avantages comme le déploiement massif par le biais du réseau ou des sauvegardes centralisées. Toutefois, ayant des images de PC pour les professionnels et pour le public, il aurait fallu que ce serveur communiquait avec les 2

VLANs simultanément, ce qui peut ouvrir une brèche de sécurité. De plus, le service restant à échelle raisonnable, le déploiement massif ne se justifie pas et risquerait de saturer le réseau.

Aussi, pour gagner du temps, j'ai acheté deux stations d'accueil de disques dur qui me proposent également de dupliquer des disques.



Là encore, ça ne me permet pas une duplication de masse, car ces docks ne copient qu'un disque à la fois. Mais ils me font gagner du temps par rapport à Clonezilla du fait que ces appareils lancent la copie en appuyant simplement sur un bouton, sans passer par une multitude de menus. La seule contrainte est que je dois démonter les deux disques durs qui s'insèrent dans les ports, le premier étant pour celui à cloner, le second pour celui qui va recevoir la copie.

Toutefois, ces deux procédés ne sont pas des doublons mais sont complémentaires. En effet, je privilégie

- Le logiciel pour :
 - Les ordinateurs portables dont les disques durs sont moins accessibles et plus difficilement démontables selon les modèles
 - Les dépannages urgents des ordinateurs des sites distants.

J'ai toujours mes disques amovibles à porter de main alors que démonter le disque dur du PC source me fait perdre du temps.

- Les docks pour :
 - Le déploiement d'une image d'un ordinateur public durant les heures d'ouvertures au public.
Je démonte simplement son disque dur pour l'emmener dans mon bureau. C'est moins lourd que porter la tour et ça me permet de réaliser la copie sans avoir à surveiller l'appareil.
 - Le déploiement d'une image professionnelle
La copie étant plus rapide, ça mobilise moins l'appareil d'un agent.
- Les deux simultanément :
 - Lorsque je déploie une ou plusieurs images en très grand nombre en même temps.
Ainsi, je peux traiter jusqu'à 3 PC en même temps. Le premier mobilisant mes deux disques amovibles, les deux autres en passant par les docks.
 - Lorsque je veux utiliser le logiciel mais que l'ISO n'est pas viable.
En effet, les deux systèmes sont compatibles pour fonctionner ensemble. Je branche sur le PC à copier le dock en USB, dans lequel je place au préalable le disque dur qui recevra la copie. Puis je lance Clonezilla au démarrage du PC. Ce dernier est capable de repérer le matériel et propose dans ses menus de copier directement le disque dur de la machine sur celui du dock. Ce procédé m'évite d'effectuer une nouvelle sauvegarde ainsi que de démonter le disque dur de la machine et donc de faire une mauvaise manipulation sur un de ses composants.
Toutefois, je dois effectuer toutes les étapes de validations des menus. De plus, je dois être certain que le disque de la machine est viable.

On le voit à travers ces quelques exemples, que ça soit la gestion des mises à jour, des sauvegardes ou l'inventaire du parc, la maintenance préventive du parc est une de mes fonctions premières. Elle prend du temps, surtout au moment de sa mise en place. Mais elle est indispensable pour gagner du temps dans la gestion du parc sur du long terme et est le point de départ de la maintenance curative.

En effet, malgré ces efforts, les problèmes ne sont jamais bien loin. D'autant que je n'ai pas encore traité la plus grande source d'erreurs d'un système, à savoir ces utilisateurs. Or, une de mes autres missions, en tant que référent informatique, est bien évidemment de venir en aide aux bibliothécaires afin que le service puisse toujours fonctionner de manière efficace.

II. La gestion des utilisateurs

a) La gestion des accès

Mon chef de service me dit souvent avec humour que 99% des bogues en informatique se situent entre la chaise et le clavier. Bien que le chiffre soit quelque peu exagéré, il est vrai que beaucoup des erreurs surviennent à la suite d'une mauvaise manipulation (service informatique y compris) d'un utilisateur. Ils sont donc à prendre en compte ainsi que leur aisance sur l'outil informatique.

Dans un premier temps, il est important de gérer leurs accès afin de limiter les risques d'erreurs et leurs impacts sur le service. Sans pour autant que ces limitations n'entravent à l'exécution de leurs tâches. La création de nouveaux profils ainsi que le paramétrage de leurs droits se font à chaque arrivé d'un nouvel employé ou d'un stagiaire. Aussi je me pose ces questions pour m'aider à trouver le meilleur compromis :

- Quelle est leur place dans la hiérarchie ?
 - Le personnel de directions doit avoir une vision globale de ce qui se fait dans les structures sans pour autant modifier le travail réalisé
 - Les chefs de services n'ont besoin que de connaître ce réalise les agents qui leurs sont affectés. Ils doivent aussi pouvoir intervenir dans les dossiers de leur service
 - Chaque agent doit pouvoir contribuer aux dossiers de leurs service sans pouvoir modifier le travail de son collègue, ainsi qu'avoir un accès total à son dossier personnel
- Quels sont leurs droits sur le réseau ?
 - Seul le service informatique est habilité à intervenir sur le SI
 - Tous les agents doivent pouvoir s'y connecter en permanence et ce, malgré le poste utilisé. Ainsi qu'avoir accès aux ressources logiciels nécessaire pour l'exécution de leurs missions
- Quels sont leurs droits sur les machines ?
 - Seuls les agents du service informatique sont habilités à effectuer des modifications sur les PC
 - Chaque agent doit pouvoir se connecter sur n'importe quel appareil et utiliser toutes les ressources mise à disposition
 - Les référents numériques doivent avoir des droits supplémentaires sur les postes.

En effet, n'étant que deux dans le service pour plusieurs bibliothèques, il ne faudrait pas qu'une d'entre elle se retrouve bloquée juste parce que mon chef se trouve en congé et moi en déplacement, ou à cause d'un arrêt de travail. De plus, les plus grosses structures annexes ont un référent numérique sur lesquels je peux m'appuyer pour me soulager de certaines tâches redondantes ou des manipulations les plus simples lors des pannes (mises à jour des postes, installation d'un logiciel spécifique, intervention sur l'antivirus par exemple). Le but étant aussi de

m'économiser de nombreux déplacements, couteux pour la collectivité et polluants car effectués avec des voitures à essence.

Une fois toutes ces questions résolues, je leur crée un compte utilisateur

Active Directory

Pour se faire, j'utilise l'outil Active Directory (AD) de Windows server.

L'AD est un service d'annuaire pour les serveurs de Microsoft. Il répertorie et hiérarchise tous les objets composant le réseau. Les objets sont les utilisateurs, les ressources matériels (PC, serveurs, imprimantes) et logiciels (applications, bases de données, stratégies de groupes) ainsi que les unités d'organisations (décris plus loin dans le texte).

En ce qui concerne la hiérarchisation des éléments, l'AD fonctionne comme un entonnoir, en partant du global pour finir sur les éléments particuliers. Aussi, ça doit être le plus représentatif de l'organisation de la structure. Voici comment ça se concrétise pour les réseaux de bibliothèques, éléments par éléments de l'AD :

- La forêt : Non utilisé dans mon cas, elle facilite la communication entre plusieurs entreprises qui partageraient un catalogue global par exemple.
- L'arbre : Pas encore utilisé dans mon cas. Un arbre permet de regrouper, par exemple, plusieurs filiales d'une même entreprise à sa maison mère.
La forêt et l'arbre implique tous les deux la présence de plusieurs annuaires, ce qui n'est pas mon cas.
- Le domaine : C'est le niveau le plus important de l'organisation de l'AD que je gère. Un domaine équivaut à un annuaire, ce qui est mon cas. Aussi cet annuaire regroupe tous les agents et toutes les ressources de tout le réseau de bibliothèques.

Une autre organisation possible aurait été de mettre en place un annuaire par bibliothèque (que chaque bibliothèque soit un domaine donc). Ensuite toutes les bibliothèques auraient été regroupées dans un arbre.

Toutefois, cette organisation impliquerait l'installation d'un serveur dans chaque bibliothèque. Ce qui augmente les coûts du matériel ainsi que les coûts de consommations électriques.

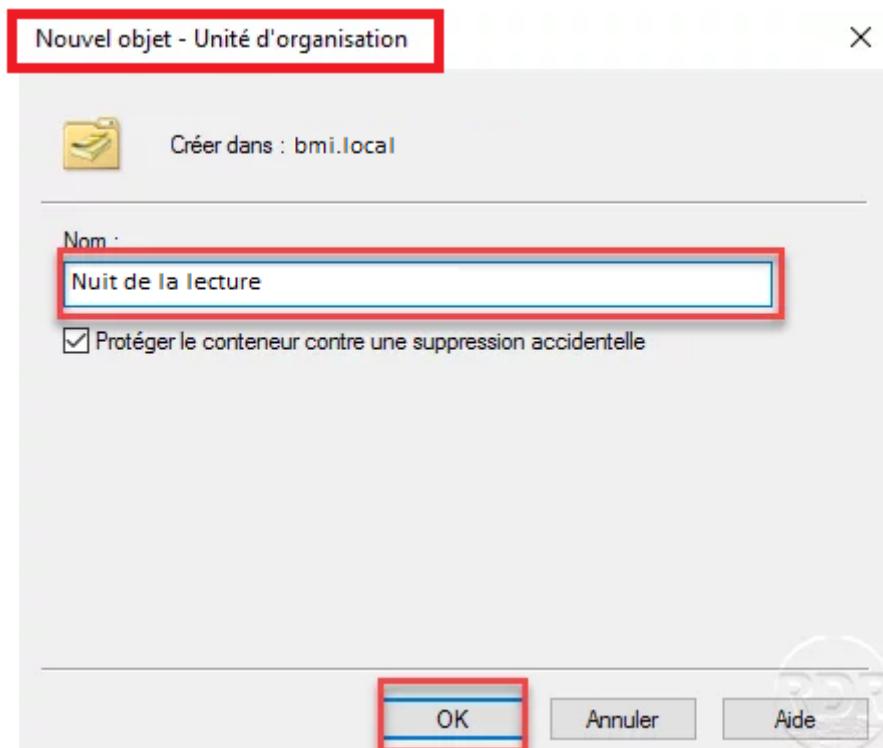
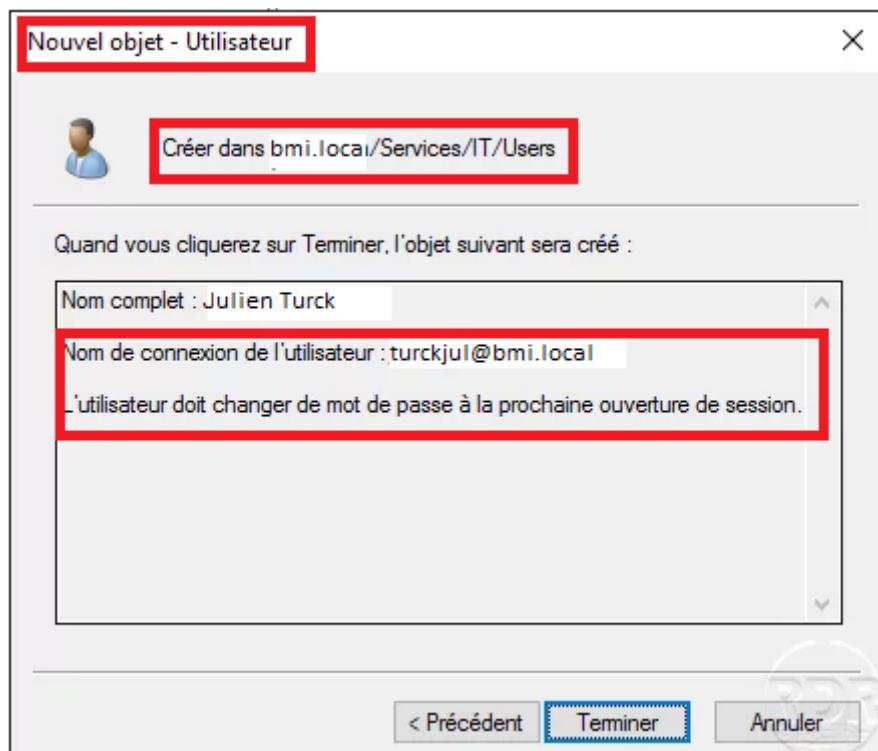
Or, le choix de mise en réseau des services (décrit dans l'activité 2) ne justifie pas une telle organisation. En effet, la plupart des ressources (SIGB et boîte mail) sont disponibles avec simplement une connexion Internet. L'accès aux fichiers centralisés à Epinal, est quant à lui disponible à partir d'une connexion de bureau à distance, par le biais d'un VPN. Ainsi, les agents des autres bibliothèques n'ont besoin que d'un compte dans l'AD d'Epinal pour effectuer toutes leurs missions.

- L'unité d'organisation : Il y a une UO par service qui représentent :

- Les différents services des bibliothèques qui, bien que travaillant sous le même toit, ont des missions bien distinctes. Par exemple, le service adulte va gérer les espaces, documents et animations destinés aux usages de plus de 14 ans. Le service jeunesse fera la même chose mais pour les moins de 14 ans. Le service patrimoine va gérer les ouvrages les plus anciens ainsi que la salle boiserie, classée aux monuments historiques etc...
- Les autres bibliothèques du réseau de lecture publique. Les agents doivent avoir un accès aux fichiers mises en commun. De plus, bien qu'il y ait un responsable par bibliothèque, elles sont toutes chapeautées par la directrice adjointe qui doit avoir une vision sur tout ce qui est fait en dehors d'Epinal
- Les groupes de travail. Ces groupes de travail peuvent être permanents (groupe de direction par exemple) ou temporaires (groupe de travail autour d'un événement exceptionnel tel que la nuit des bibliothèques qui mobilisent plusieurs agents dans des actions bien distinctes)
- Les sous-groupes au sein de chaque service. Par exemple, le chef du service a plus de droits sur les dossiers de celui-ci que ses agents.
- Les groupes de machines. L'AD gère que le VLAN professionnel (les VLAN sont abordés dans l'activité 2). Aussi, il n'y a qu'une UO qui regroupe tous les PC professionnels.
- Les objets : C'est la plus petite unité de l'AD. Elle comprend notamment les comptes d'utilisateur ainsi que chaque machine.

A chaque mouvement de personnel (départ, arrivé, long congés) je suis amené à modifier la liste des utilisateurs en les supprimant ou en créant un nouveau compte. Je crée également de nouvelles UO lorsque se crée des groupes de travail.

Dans les deux cas, je réalise un clic droit à l'endroit où je veux les insérer. Puis je sélectionne l'option correspondant à l'objet souhaité dans du menu « nouveau ».

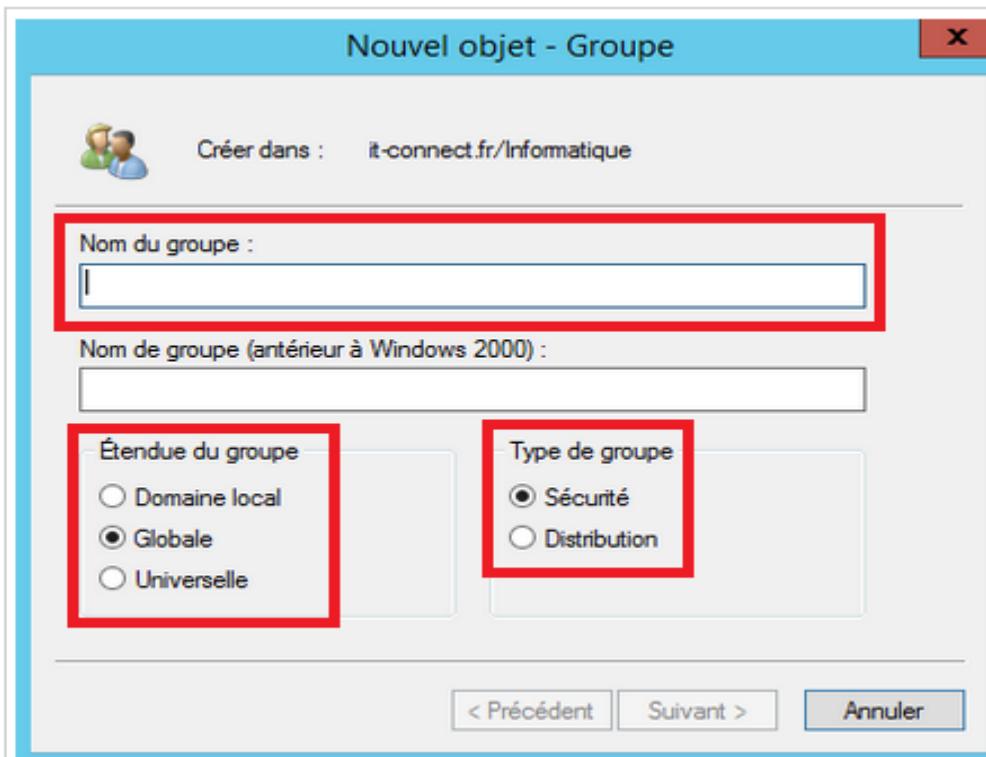


Méthode AGDLP

Réaliser une organisation claire de l'AD permet de gagner du temps par la suite, lors de l'attribution des droits sur les partages de fichiers. En effet, je les attribue en m'appuyant sur la méthode **AGDLP** (**A**ccount, **G**lobal, **D**omain **L**ocal, **P**ermission) préconisée par Microsoft. L'acronyme précise l'ordre dans lequel sont faites les étapes :

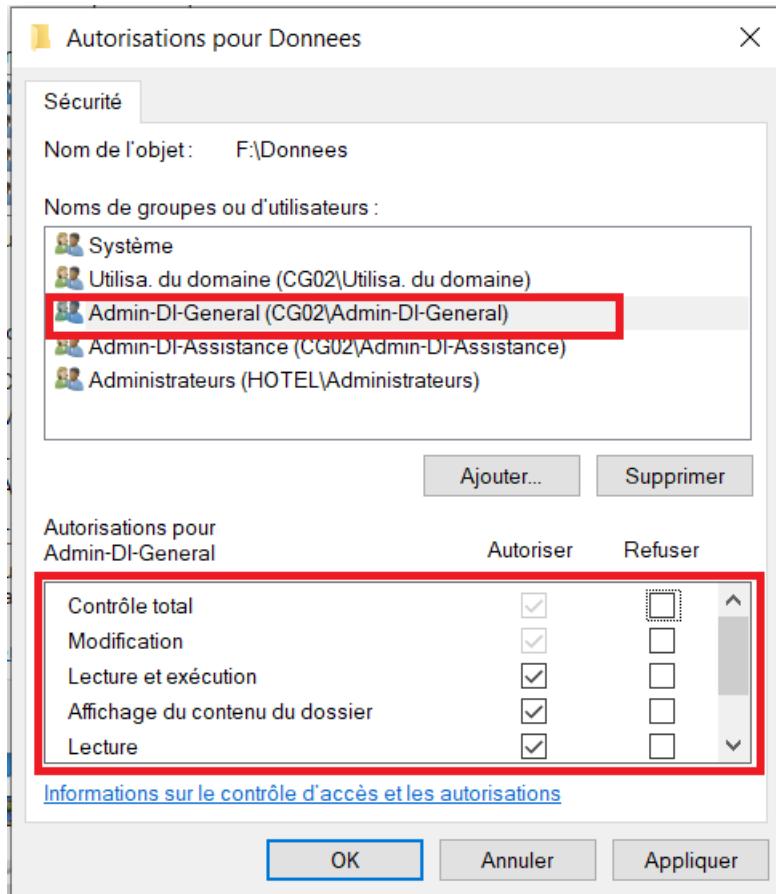
- Account :
 - Représente les comptes utilisateurs qui seront concernés par les permissions
 - Intégrés aux groupes que je crée
- Global :
 - Représente les groupes d'étendue globale dans lesquels les individus sont rattachés.
 - Les groupes d'étendue globale sont des groupes qui peuvent s'étendre au-delà du domaine.
 - Dans mon cas, ils sont représentatifs d'une des UO du domaine.
 - Intégrés à d'autres créés spécifiquement pour l'attribution des droits.
- Domain Local :
 - Ce sont les groupes d'étendue Domaine Local.
 - Ces groupes ne peuvent pas s'étendre au-delà du domaine.
 - Pour mes besoins, ils ne représentent pas un service concret mais correspondent aux types d'utilisateurs. Par exemple, il y aura un groupe d'étendue Domaine Local pour ceux qui n'ont qu'un droit de lecture sur le dossier et un groupe de même étendue pour ceux qui auront également le droit de lecture et d'écriture, voire de contrôle total sur le dossier.
 - Ce sont sur ces groupes que l'on va agir sur l'attribution des droits.

Pour créer un groupe, je clique sur l'icône « créer un nouveau groupe » situé dans le bandeau juste en dessous des menus. Dans l'assistant, je donne un nom au groupe, je choisi son étendu et je laisse comme type de groupe « sécurité » puisque ce sont des groupes créés pour attribuer des droits.



- Permission :
 - C'est la dernière étape, l'attribution des droits aux groupes d'étendue Domaine Local.
 - Ne se réalise pas dans l'AD mais dans les propriétés des dossiers

Je réalise l'affectation des droits en ouvrant les propriétés des dossiers grâce à un clic droit dessus puis sur l'onglet sécurité. Ensuite, je clique sur les boutons « modifier » puis « ajouter » pour ajouter des groupes. Je les ajoute en tapant leur nom dans la case « entrez les noms des objets à sélectionner » de la fenêtre « sélectionner des utilisateurs ou des groupes ». Enfin, je leur attribue leurs droits en cochant les cases correspondantes.

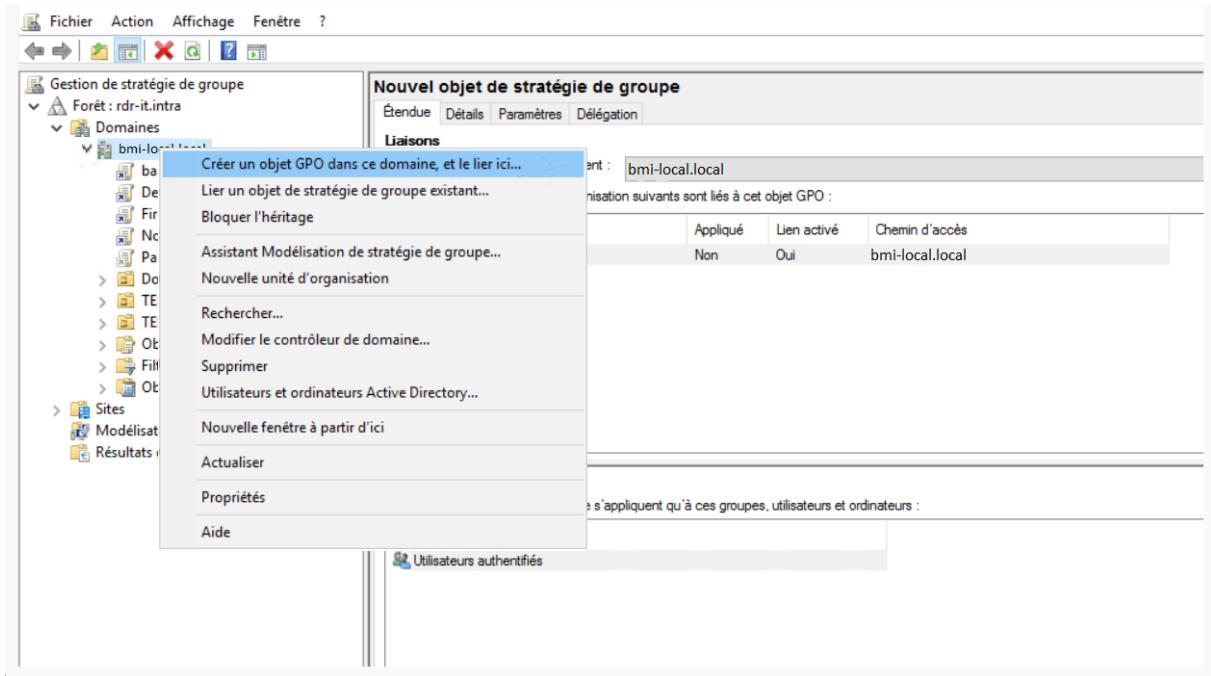


Cette méthode est très pratique car elle me permet de déplacer des individus d'un groupe à un autre sans le risque qu'il ne se retrouve avec des droits sur des fichiers auxquels il ne devrait plus avoir accès (lors d'un changement de service par exemple) ou supprimer un objet sans qu'il n'y ai d'impact sur le reste du groupe (départ d'un individu par exemple). Enfin, cette façon de faire m'évite de créer des dossiers de partages directement sur les postes, ce qui serait trop contraignant. En effet, il faudrait que j'agisse sur chacun des postes professionnels (soit plus d'une cinquantaine de postes). De plus ça augmente le risque de perdre des fichiers importants si le poste vient à ne plus fonctionner par exemple.

Les GPO

Enfin, l'AD me permet également une gestion centralisée lorsque je veux faire appliquer une règle à un ensemble d'objets (individus ou machines) grâce aux [GPO \(Group Policy Object ou stratégies de groupe\)](#).

Ceux-ci peuvent être affectés soit à un objet, soit une UO soit au domaine. Pour se faire, il me suffit de faire un clic droit sur le groupe concerné. Ensuite, je clique soit sur « créer un objet GPO » si celle-ci n'existe pas encore, soit sur « Lier un objet de stratégie de groupe existant » si celle-ci existe déjà et que je veux l'appliquer à un nouveau groupe.



Cette méthode m'évite des configurations manuelles sur chacun des postes et des profils utilisateurs. De plus, pour faire appliquer une consigne à un nouvel objet ou au contraire, créer une exception, il me suffit de l'ajouter ou de le retirer du groupe concerné.

Avec les GPO, j'applique par exemple, le mappage du lecteur réseau des fichiers communs à tous les utilisateurs du domaine. Ainsi, une fois que j'ai créé la GPO (vidé pour le moment) je la modifie et lui applique l'option « mappage des lecteurs » du sous menu Configuration utilisateur / Préférences / Paramètres Windows. Je lui indique ensuite dans un formulaire, le lien du lecteur, sa dénomination (commun), ainsi que sa lettre de mappage.

Profils utilisateurs

J'ai également associé GLPI à l'AD pour la création des accès du personnel à celui-ci.

Une fois les comptes intégrés, j'accorde des droits à chacun d'entre eux. Pour cela, je m'appuie sur des profils d'utilisateurs pour attribuer leurs droits. GLPI propose des profils par défaut qui suffisent pour attribuer des droits suffisants à chacun. Les profils que j'utilise sont :

- Super-Admin qui n'est accordé qu'à un compte créé par défaut au moment de l'installation du logiciel. Il me permet de paramétriser GLPI dans son ensemble ainsi que d'effectuer des modifications dans les bases de données.
- Supervisor qui est attribué à mon profil ainsi que celui de mon chef de service. Il me permet de traiter les tickets ouverts par nos collègues ou d'en créer et de me l'attribuer lorsque je suis sollicité par un autre biais. Ça me permet de garder une trace de la demande si elle n'est pas traitée tout de suite. Ça me permet également de noter le suivi pour connaître son avancement si elle n'est pas réglée immédiatement.

- Observer qui donne un droit de consultation des bases de données et des tickets. Il est attribué aux comptes :
 - Des personnels de direction pour qu'ils aient une vue sur tout ce qu'il se fait ainsi que de pouvoir connaître en permanence l'état du patrimoine.
 - Du personnel administratif qui doit pouvoir consulter les documents liés aux contrats de garanties ou de maintenance par exemple, ainsi qu'aux stocks de matériels.
- Self-Service qui offre des droits très restreints tels que la création d'un ticket de demande d'aide ou réserver du matériel. Il est attribué par défaut à tous les comptes, au moment de leur création et conservés pour tous ceux non concernés par les profils ci-dessus.

The screenshot shows the Glpi administration interface. The top navigation bar includes links for Parc, Assistance, Gestion, Outils, Administration (which is highlighted in blue), and Configuration. Below the navigation is a search bar and language selection (Français). The main content area is titled 'Utilisateurs' and shows a list of users. One user, 'turck julien', is selected and highlighted with a red box. A modal window titled 'Ajouter une habilitation à un utilisateur' (Add privilege to a user) is displayed. It contains a dropdown menu labeled 'Profil' with several options: Admin, Hotliner, Observer, Read-Only, Self-Service, Super-Admin, Supervisor, and Technician. The 'Technician' option is highlighted with a red box. To the right of the dropdown, there is a checkbox for 'Récursif' (Recursive) and a 'Ajouter' (Add) button.

C'est la même philosophie que j'applique lors de la création des comptes des agents sur le SIGB. A part qu'on ne parle pas de profil mais de rôle.

SYRACUSE - EXTRANET

Ajout d'un utilisateur

Entité de rattachement *

Type d'utilisateur *

COMPTES UTILISATEUR

Identifiant *

Mot de passe *

L'utilisateur doit changer de mot de passe à la prochaine connexion

Date d'expiration

AUTORISATIONS

Rôle dans l'entité

INFORMATIONS PERSONNELLES

Nom *

Prénom *

Date de naissance

Sexe

Adresse électronique

Téléphone

Adresse

Annuaire des utilisateurs

Mes prêts

En cours

Attendus par d'autres

En retard

Mes réservations

Documents

Outils d'animation

Mises à disposition

Enfin, les bibliothécaires utilisent tous les jours un logiciel qui gère les plannings des agents (Planno).

Lorsque je crée un nouvel agent, je lui attribue là encore des droits (lecture du planning, gestion de ses absences ou encore attribution d'un poste à agent par exemple).

La différence avec ce logiciel est que je n'attribue pas un profil à un utilisateur mais je lui accorde ses droits en cochant ceux que la direction lui accorde, en fonction de sa place dans la hiérarchie.

Ajout d'un agent

Infos générales	Activités	Heures de présence	Droits d'accès	Annuler	Valider
-----------------	-----------	--------------------	----------------	---------	---------

Absences

- Modifier ses propres absences
- Enregistrement d'absences pour plusieurs agents
- Gestion des absences, validation niveau 1
- Gestion des absences, pièces justificatives

Agendas

- Voir les agendas de tous

Agents

- Voir les fiches des agents
- Gestion des agents

Heures de présence

- Gestion des heures de présence, validation niveau 1
- Gestion des heures de présence, validation niveau 2

Planning

- Création / modification des plannings, utilisation et gestion des modèles
- Modification des plannings
- Griser les cellules des plannings
- Modification des commentaires des plannings
- Configuration des tableaux

Postes

- Gestion des postes

Statistiques

Toutes ces restrictions permettent ainsi de limiter les accidents ou les actions mal-attentionnées. Bien que ça porte, à court et moyen terme, ces fruits, je ne suis jamais à l'abri d'une mauvaise manipulation, d'une méconnaissance ou d'une panne.

Aussi, la dernière partie de mes missions en tant que référent informatique, est donc de venir en aide à mes collègues ainsi qu'auprès du public, ainsi que de les accompagner sur la prise en main de certains outils spécifiques.

b) La gestion des incidents et de l'accompagnement

A moins d'animer un atelier à destination du public, je peux être interpellé à tout moment par un collègue pour lui venir en aide ou pour dépanner un usager.

Le service étant à petite échelle, tous les moyens sont autorisés pour me contacter en fonction de l'importance de la demande. On peut venir frapper à la porte de mon bureau, me téléphoner, m'envoyer un mail ou bien créer un ticket d'incident par le biais de GLPI. Cette dernière est la méthode la moins utilisée car la plus contraignante pour les bibliothécaires. Les deux premières sont les plus prisées alors que le mail n'est déjà utilisé qu'en dernier recours lorsque je ne suis pas présent ou lorsque la demande peut attendre plusieurs jours voire semaines. Toutefois, afin de

La gestion des incidents

D'un point de vue général, je tente d'organiser et de gérer le [SI \(Systèmes d'Informations\)](#) en me reportant au maximum au référentiel ITIL.

Référentiel ITIL (Information Technology Infrastructure Library) est un référentiel de bonnes pratiques qui peuvent être adoptés pour la gestion des SI.

La gestion des incidents en fait bien évidemment partie et la solution GLPI permet par exemple de mettre en œuvre une partie de ses recommandations dans ce domaine ainsi que dans la gestion du parc.

[D'un point de vue ITIL, il y a incident lorsqu'il y a dégradation ou perte d'un service.](#)

Dans ma démarche pour gérer un incident, je respecte le cycle de vie d'un ticket incident, même si celui-ci n'a pas été formellement ouvert. C'est-à-dire :

- Signalement et enregistrement : un problème survient et j'en suis informé de plusieurs manières :
 - Un collègue ou un usager me le signal. Pour se faire, il a plusieurs méthodes :
 - _ Il vient me trouver personnellement
 - _ Il me téléphone sur mon DECT
 - _ Il m'envoie un mail
 - _ Il ouvre un ticket GLPI

The screenshot shows a 'Ticket' creation form. Key fields include:

- Type:** Demande
- Demandeur:** chassard raphael (cours : 0)
- Attribué à:** turck julien (cours : 0)
- Statut:** Nouveau

➤ Je le détecte en visualisant les appareils

➤ Un logiciel de supervision m'envoie une alerte

Quel que soit la manière, ça abouti à la création d'un ticket que ça soit par moi ou par un collègue, même à posteriori. Il me permettra de garder une trace de l'incident et de sa résolution, il permet également de montrer l'activité à la direction qui peut prendre connaissance des statistiques de nos interventions.

- Classification : Bien que le premier arrivé soit le premier servi, j'évalue la gravité de la situation en fonction de son impact sur le service au public et de son niveau d'urgence (la tâche a-t-elle besoin d'être réalisée immédiatement). Mon but est de définir si l'intervention doit être immédiate ou si elle peut attendre que je termine celle sur laquelle je suis, si je suis déjà occupé. Ainsi que pour établir une hiérarchie, si plusieurs problèmes subviennent en même temps.

Tableau qui résume la méthode de réflexion, qui reprend le principe de la matrice d'Eisenhower :

Urgence / Impact	Fort	Moyen	Faible
Fort	1	2	2
Moyen	3	3	4
Faible	4	5	5

1 correspondant aux interventions les plus urgentes, 5 aux moins prioritaires.

- Traitement : Le problème va être attribué en fonction de la situation :
 - Je suis seul, je vais donc intervenir spontanément
 - Mon chef et moi sont tous les deux présents. On va alors se concerter et se demander :
 - Qui est le plus compétent sur le problème ?
 - Qui est déjà occupé et lequel à l'occupation la moins importante ?
 - Je constate l'incident mais ne pense pas pouvoir le résoudre. J'effectue alors une procédure d'escalade. C'est-à-dire que je vais me référer à quelqu'un de plus compétent que moi :

_ Ça dépasse mes compétences, je fais appel à mon chef de service qui pourra intervenir à ma place, si présent sur le site. Sinon, à distance, me prodiguer des conseils voir me dicter la marche à suivre.

_ Ça concerne du matériel ou un logiciel très spécifique (pare-feu, RFID, SIGB par exemple) j'ouvre alors un ticket auprès de leurs plateformes de maintenance, en conformité avec ce qui a décrété dans le [SLA \(Service Level Agreement ou accord de niveau de service\)](#) conclu au moment de l'achat du matériel.

- Solution : J'apporte une solution qui, soit :

_ Résout totalement problème dans un délai raisonnable. Dans ce cas je l'applique immédiatement et je rétablie le service dans son état de performances initiale.

_ Ne résout qu'en partie le problème ou dans un laps de temps trop long. Dans ce cas je propose une solution de secours qui permettra au service de fonctionner en mode dégradé. Il y a dégradation de service lorsqu'il fonctionne mais plus lentement ou avec des offres de service manquants par exemple. En attendant de mettre en place la solution qui rétablira complètement le service.

Quelques exemples de situations problématiques auxquelles j'ai eu à faire, hors problèmes de réseau, ainsi que leur résolution :

Type d'appareil	Problème	Résolution
Ordinateur	L'écran n'affiche rien alors que son voyant est bien allumé	Après vérification, le câble VGA était HS. Il a suffi de le remplacer.
Ordinateur	L'ordinateur met énormément de temps pour répondre à n'importe quelle tâche demandée	Après un scan de l'antivirus afin de vérifier que ça ne vienne pas d'un malware, j'ai réalisé un profond nettoyage du système. J'ai tout d'abord supprimé les sessions des anciens utilisateurs partis entre temps ainsi que leurs dossiers personnels. J'ai ensuite réalisé un nettoyage du disque avec l'utilitaire Windows du même nom ainsi qu'une défragmentation, toujours avec l'utilitaire Windows dédié.
Ordinateur	Au fur et à mesure, c'est le parc dans son ensemble qui est devenu moins réactif, avec des démarriages d'ordinateurs toujours plus long.	J'ai remplacé tous les disque durs HDD par des SSD de même capacité de stockage.
Ordinateur	Lors du démarrage, un écran bleu s'affiche en informant qu'une erreur a	J'ai remonté une sauvegarde du poste récente

	survenu et qu'il doit redémarrer. Mais au redémarrage, rien ne change.	grâce à l'utilitaire Clone-Zilla.
Ordinateur	Perte d'un fichier important à la suite d'une mauvaise manipulation	Je suis allé chercher la sauvegarde du fichier la plus récente et je le lui ai remonté dans son dossier d'origine
Copieur	Au moment de lancer l'impression, le copieur se met en erreur.	Après observation de son écran, il s'agissait d'un bourrage papier. Le fait de retirer manuellement le papier coincé a suffit à relancer l'impression.
Copieur	Les impressions ne se lançaient plus alors qu'aucune erreur ne s'affiche sur l'écran du copieur	La file d'attente des documents était obstruée par un fichier de la veille qui ne s'était pas lancé. En me connectant en tant qu'administrateur, j'ai pu supprimer les fichiers en attente. J'ai ensuite redémarré le copieur pour le réinitialiser.

Les abonnés de la bibliothèque ainsi les utilisateurs des ordinateurs publics peuvent également me solliciter après avoir fait une demande auprès d'un bibliothécaire présent dans les espaces publics. Bien qu'il y ait rarement urgence, c'est l'impact qui est fort car toute panne dégrade l'image du service.

Quelques exemples typiques que j'ai eu à faire auprès du public :

Type d'appareil	Problème	Résolution
Appareil personnel	La personne n'a pas la page d'accueil du proxy qui s'affiche et ne peut donc pas naviguer sur Internet. Ça ne semble toucher que son appareil	Je vérifie l'activation du WIFI et la connexion au WIFI public de la bibliothèque. Je vérifie que le proxy est bien joignable en tapant son adresse IP dans la barre de navigation.
Copieur	La personne n'arrive pas à récupérer son impression	Je vérifie que la personne tape le même mot de passe qu'il a indiqué au moment de la demande d'impression. Que sa carte d'impression ait assez de crédit vis-à-vis de ce qu'il a demandé

		(ce n'est pas le même prix en fonction de si c'est une copie en noir et blanc ou couleur ou si c'est un format A4 ou A3). Qu'il sélectionne bien son document dans la liste d'impressions en attente et non celle d'un autre qui aurait été envoyé en même temps.
Appareil personnel	N'accède pas à son compte d'abonné	Je vérifie que la personne est bien à jour dans sa cotisation Je réinitialise son mot de passe s'il a perdu ses identifiants.

- Validation et clôture du ticket : A la suite de sa résolution, je ferme l'incident avec l'accord de la personne qui m'a interpellé, avec un mail explicatif de l'incident et de sa conclusion envoyée à qui de droit (le demandeur si c'est un professionnel ainsi que ma hiérarchie directe). Je clos également le ticket GLPI afin que mon chef ne pense pas que ça soit une tâche à faire. Là encore, j'explique ma résolution afin d'avoir une trace si le problème réapparaît.

Heureusement, il n'y a pas des pannes tous les jours. Et les sollicitations peuvent également être de l'aide sur une manipulation qu'ils ne maîtrisent pas. Ainsi je suis amené à expliquer comment se branchent et fonctionnent certains appareils tels que les vidéoprojecteurs, les sonos ou le matériel spécifique à l'animation comme les robots, le casque de réalité virtuelle ou l'imprimante 3D.

Mais surtout je suis amené à accompagner les agents dans l'utilisation des réseaux sociaux ainsi que la chargée de communication pour le site Internet.

Réseaux sociaux

Les contenus sont rédigés par les différents services. Aussi je les accompagne sur deux volets :

- La programmation des posts : J'utilise l'outil en ligne Buffer (<https://buffer.com/>) Il permet de gérer sur une même page la totalité de ses comptes et notamment de programmer ses posts à l'avance. On va pouvoir insérer tout le contenu ainsi que de décider de la date et de l'heure de la publication.

Pour cela, je clique sur le menu « publishing » puis sur create post. Je choisi ensuite le compte du réseau social concerné par la publication. Je renseigne le contenu. Puis je clique sur « add to queue » et je sélectionne l'option « Schedule post ». Je peux alors sélectionner le jour et l'heure de publication

The screenshot shows the Buffer Queue interface. At the top, there are navigation links: Create, Queue (highlighted with a red box), Sent Posts, Approvals (0), Drafts (0), and Settings. Below the navigation is a date selector showing Today (AUGUST 28) and Tomorrow (AUGUST 29). The time zone is set to Europe/Paris. A 'Create Post' button is highlighted with a blue box. The main area displays a post scheduled for August 29th at 7:05 PM (GMT+2). The post content is "test" and includes a note: "Post scheduled for August 29th at 7:05 PM (GMT+2)". Below this, there is a section for Wednesday, AUGUST 30, with a post scheduled for 7:56 AM.

➤ Avantages :

- _ Ça permet de s'adapter aux heures des pics d'audiences des comptes, qui ne sont pas forcément les heures de bureau des bibliothécaires.
- _ Ça permet d'avoir des publications régulières sans à avoir à mobiliser un collègue en tout temps.

➤ Inconvénient :

- _ Perte de spontanéité qui sera compensée par les publications faites en directe durant certains événements ou des informations de dernière minute par exemple

- La modération des commentaires :

Je crée des filtres avec des mots clés afin que certains contenus soient signalés. Pour faire ça, j'ouvre le menu « gérer » puis « alertes de modération ». Je clique ensuite sur « modifier les alertes ». Je peux alors demander à être prévenu en cas d'utilisations de mots clé ou demander à être prévenu lorsqu'un commentaire est posté.

The screenshot shows the 'Alertes de modération' (Moderation Alerts) page. On the left, there is a sidebar with various moderation categories: Demande de badge (0 aujourd'hui), Questionnaire d'adhésion, Approbations en attente (0 aujourd'hui), Spam potentiel (0 aujourd'hui), Publications programmées, Historique d'activité, Règles du groupe, Contenu signalé par un membre (0 aujourd'hui), and Alertes de modération (0 aujourd'hui). The 'Alertes de modération' item is highlighted with a red box. The main content area shows a bell icon and the message: "Aucune alerte de modération" (No moderation alert). It also states: "Aucune publication ni aucun commentaire n'a déclenché les alertes de modération." A 'Modifier les alertes' button is highlighted with a red box.

- Je suis moi-même sur les réseaux sociaux :
 - Je dissocie mes comptes personnels et professionnels
 - Pour mes contacts professionnels j'utilise Linkedin
 - Mon compte est accessible en tapant mon nom sur Google
 - Je verrouille suffisamment pour que ne s'affiche que l'intitulé de mes comptes par les suggestions Google et dans les images.

Environ 764 000 résultats (0,30 secondes)

Images correspondant à julien turck

brand manager mariage dinozé golbey bmi

Tout afficher →

LinkedIn
<https://fr.linkedin.com/julien-turck-96ab991b1>

Julien TURCK - Manager - Groupe C2E
 Dijon, Bourgogne-Franche-Comté, France · Manager · Groupe C2E
 Julien TURCK. Manager chez Groupe C2E. Groupe C2E. Dijon, Bourgogne-Franche-Comté, France. 79 abonnés ...

julien turck - Spécialiste informatique - BMI
 Nancy et périphérie · Spécialiste informatique · BMI
 julien turck · Spécialiste informatique chez BMI · Expérience · Autres pages consultées ·
 Autres personnes nommées julien turck · Voir le profil complet de julien.

Site Internet

Mon rôle est d'accompagner la chargée de communication dans l'utilisation et l'appropriation de l'outil qui permet de gérer le site Internet.

L'outil proposé par notre fournisseur SIGB est un CMS (Content management System), tout comme WordPress ou Drupal. Cette solution apporte :

- Avantages :
 - Je n'ai accès qu'au back-office (c'est-à-dire l'interface qui permet de modifier sa structure et son contenu). Le reste est géré par notre fournisseur SIGB (hébergement, accessibilité en ligne, sauvegardes et mises à jour).
 - Aucune compétence dans les langages HTML, CSS ou encore JavaScript à avoir pour modifier le site. En effet, il s'agit de simplement placer

des blocs prédéfinis sur les pages ou sous-menus concernés. On charge ensuite des images ou on écrit du texte comme on le ferait sur un traitement de texte par exemple.

➤ Propose des outils :

_ Pour enregistrer la version du site avant d'effectuer des modifications. Ainsi, si une mauvaise manipulation est effectuée, je peux revenir en arrière.

Pour cela, je clique sur « informations sur les révisions » en bas de la page modifiée. Je coche ensuite la case « créer une révision » que je renseigne avec un rapide commentaire.

The screenshot shows the Joomla administrator interface with the following details:

- Top Bar:** Gérer (Manage), Raccourcis (Shortcuts), jturck (User).
- Menu Bar:** Contenu (Content), Structure (Structure), Apparence (Appearance), Extension (Extension), Configuration (Configuration), Personnes (People), Rapports (Reports), Help.
- Current View:** Rubrique (Category). Subtitle: Qui sommes nous (12). Hint: Sélectionner la rubrique à laquelle doit être rattaché l'article (Select the category to which the article should be attached).
- Form Fields (Left Column):**
 - Status
 - Paramètres du menu (Menu parameters): Vos interlocuteurs
 - XML Sitemap
 - Informations sur les révisions (Information about revisions):** Nouvelle révision (New revision) is selected.
 - Alias d'URL (URL alias): Alias : /Vos-interlocuteurs
 - Informations de publication (Publication information): Par admindi (1) le 2017-05-29
 - Options de publication (Publication options): Non promu (Not promoted)
- Form Fields (Right Column):**
 - Créez une nouvelle révision (Create a new revision)
 - Message du journal de révision (Revision journal message):** version ok au 28 aout 2023. Hint: Décrivez brièvement les modifications apportées. (Describe briefly the changes made.)
- Bottom Buttons:** Published (Published) checked, Enregistrer (Save), Preview (Preview), Delete.

_ Pour prévisualiser sa modification et ainsi se rendre compte du rendu final avant de la publier.

Pour cela, toujours en bas de la page modifiée, je clique sur le bouton « Preview ».

Rubrique Qui sommes nous (12)

Sélectionner la rubrique à laquelle doit être rattaché l'article

Status	<input checked="" type="checkbox"/> Créer une nouvelle révision
Paramètres du menu	
Vos interlocuteurs	
XML Sitemap	
Informations sur les révisions	
Nouvelle révision	
Alias d'URL	
Alias : /Vos-interlocuteurs	
Informations de publication	
Par admindi (1) le 2017-05-29	
Options de publication	
Non promu	

Published

Enregistrer **Preview** Delete

- Inconvénient :
 - Je suis limité aux options qui sont proposés par le prestataire. Il est d'ailleurs déjà arrivé que pour faire des modifications très spécifiques, je passe directement par le code source, qui lui, demande des notions dans les langages cités auparavant.
- Pour cela, je clique sur le bouton « source » du contenu à modifier

The screenshot shows a web-based content management system. At the top, there's a navigation bar with links like 'Gérer', 'Raccourcis', and 'jturck'. Below the navigation bar, a horizontal menu bar includes 'Contenu' (which is highlighted with a red box), 'Structure', 'Apparence', 'Extension', 'Configuration', 'Personnes', 'Rapports', and 'Help'. The main area is titled 'Onglets' and has tabs for 'Informations-generales *', 'contenu *' (which is highlighted with a red box), 'Informations', 'Média', 'Widget home', and 'Rubrique article'. Under the 'contenu' tab, there's a section titled 'Contenu *' with a rich text editor toolbar. The toolbar includes standard text formatting icons (B, I, S, etc.) and a 'Source' button, which is also highlighted with a red box. Below the toolbar, the content area contains some HTML code and a preview of the text. At the bottom of the content editor, there's a link 'À propos des formats de texte' and a dropdown menu 'Format de texte' set to 'HTML complet'.

Enfin, j'organise, de manière plus légère, des formations à destination du public, autour des outils informatiques et numériques. Par exemple, j'organise des ateliers d'initiation à la prise en main des tablettes et des liseuses que nous mettons à leur disposition et en prêt. J'anime également des sessions de tournois de jeux vidéo afin de présenter l'offre de la bibliothèque, qui a aussi pour but de rassurer les parents sur nos contenus, sur le média de manière générale et qui a pour dernier objectif d'initier ceux qui n'aurait pas la possibilité d'y avoir accès à leur domicile.

■ Les jeux vidéo à l'honneur à la bibliothèque

Il y avait de l'animation samedi matin à la bibliothèque multimédia intercommunale. Sous la houlette de Julien Turck, des jeunes se sont lancés dans des joutes amicales de jeux vidéo.

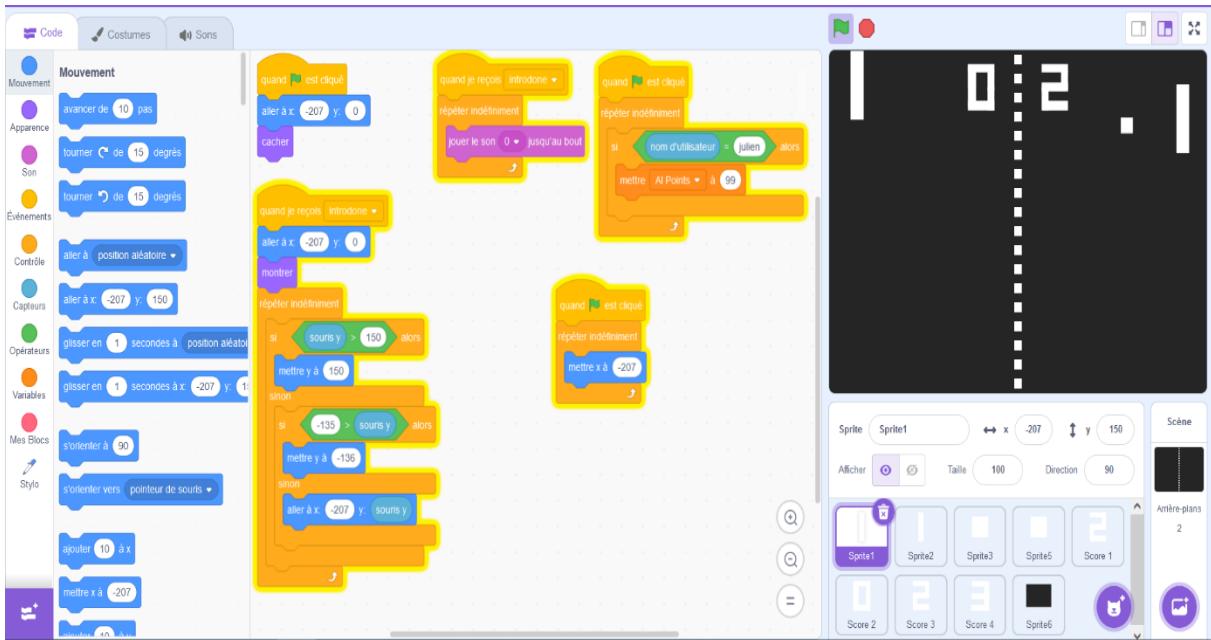
Vosges Matin - 07 nov. 2017 à 05:00 - Temps de lecture : 1 min



Avant de s'opposer dans des joutes amicales, les joueurs ont suivi les conseils de Julien Turck (à d.).

Je réalise aussi régulièrement des initiations à la programmation avec les adolescents. Pour se faire, j'utilise deux outils que je présente en deux temps :

- Dans un premier temps, je présente l'outil Scratch.
 - Outil gratuit en ligne, créé par le MIT (Massachusetts Institute of Technology) qui est un institut de recherche américain et une université, spécialisé dans les domaines de la science et de la technologie.
 - Ne demande pas de connaissances dans un quelconque langage de programmation (Python, C, Java etc...). Son principe est d'assembler des blocs préprogrammer pour chaque action ou évènement voulu. Seules les variables sont à modifier pour avoir le résultat souhaité (temps, distance, texte à afficher etc...). Il permet également d'importer des objets (fonds, personnages, objets etc...) afin de personnaliser ses créations.
 - Permet d'aborder la notion de programmation évènementielle (programmation dont l'exécution varie en fonction d'actions ou d'événements)
 - Les productions suffisent lorsqu'elles ont pour vocations d'être des domaines du loisir créatif ou de la pédagogie. Par exemple, je fais faire aux enfants des reprises de jeux vidéo tels que Pong.



- Dans un second temps, je présente l'[IDE Visual Studio Community \(Integrated Development Environment, ou environnement de développement « intégré »\)](#) :

- Logiciel gratuit de chez Microsoft
- Permet d'aborder la notion de programmation séquentielle (Programmation dont l'exécution se fait ligne par ligne)
- Permet d'essayer différents langages de programmation
- Propose des outils et des options d'aide à la programmation tels que :

_ L'indentation : A chaque validation de ligne, le curseur se positionne à l'endroit exact où doit commencer la ligne suivante

_ L'auto-complétions : l'IDE anticipe les premières frappes des lignes et proposent les possibilités qui en découle pour faciliter l'écriture et éviter des fautes

_ Colorisation du code : Les différents éléments se colorisent différemment en fonction du type d'élément

_ Aide à la frappe : les erreurs sont immédiatement soulignées d'une vaguelette rouge. De plus, les lignes contenant des erreurs sont signalées sur le côté

_ Débogueur : Outil qui permet notamment d'exécuter son programme pas à pas ou à partir d'une ligne bien précise. Facilitant ainsi la lecture des événements et comprendre, par exemple, ce qui cause l'arrêt du programme

- Permet de réaliser de véritables programmes exécutables dans des environnements Windows ou Androïd. Pour ma part, je leur apprends à programmer en séquentiel, le jeu du chiffre mystère :

```
// importation de la fonction permettant au programme de choisir un nombre au hasard
Import random
// déclaration des variables
int nbre_essais_max = 5 ;
int nbre_essais = 1 ;
int borne_sup = 20 ;
int mon_nombre = randint (1,borne_sup) ;
int ton_nombre = 0 ;
```

```

// affichage des consignes
Console.WriteLine("J'ai choisi un nombre entre 1 et ",borne_sup);
Console.WriteLine("Tente de le découvrir en ",nbre_essais_max, "tentatives maximum");
// itération indéterministe tant qu'un des conditions n'est pas remplie
while (ton_nombre != mon_nombre && nbre_essais <= nbre_essais_max)
{
    // proposition de réponse du joueur
    Console.WriteLine("Essai n° ", nbre_essais);
    ton_nombre = int.Parse(Console.ReadLine("Votre proposition :"));
    // alternative en fonction du choix du joueur
    if (ton_nombre < mon_nombre)
    {
        Console.WriteLine("Trop petit")
    }
    elif (ton_nombre > mon_nombre)
    {
        Console.WriteLine("Trop grand")
    }
    else
    {
        Console.WriteLine("Bravo ! vous avez trouvé ",mon_nombre," en ",nbre_essais_max, " essais")
    }
    // augmentation du nombre d'essai si reboucle
    nbre_essais += 1
}
// message si perdu
if (nbre_essais>nbre_essais_max)
{
    Console.WriteLine("Perdu !")
    Console.WriteLine("J'avais choisi le nombre ",mon_nombre)
}

```

En conclusion, cette activité montre mon quotidien qui est essentiellement celui d'un technicien de maintenance. En effet, Je suis amené à :

- _ Gérer le patrimoine informatique
- _ Répondre aux incidents et demandes d'assistance
- _ Développer la présence en ligne du service

De plus, j'ai démontré que j'organise mon développement professionnel à travers ma présence personnelle sur Internet

Toutefois, pour les besoins du service, j'ai dû monter en compétence en interne pour assister mon chef de service dans ses missions d'administration des systèmes et des réseaux. C'est le sujet de l'activité n°2.

Fiche descriptive de l'activité 2

L'administration du réseau et des sites distants

ACTIVITÉ 2 : L'administration du réseau et des sites distants

Bien qu'il n'y eût pas de missions spécifiques à l'administration des réseaux, décrites dans la fiche de poste, des connaissances de bases dans l'équipement réseaux, l'adressage IP ainsi que dans la virtualisation.

Et pour cause, puisqu'à terme, un des objectifs d'évolution du poste est de pouvoir épauler le technicien informatique dans ces missions d'administration des systèmes et des réseaux.

Concrètement, cela consiste à administrer les infrastructures informatiques dont on assure l'installation, le paramétrage, la sécurisation, le maintien en condition opérationnelle et en condition de sécurité. L'administrateur systèmes et réseaux a aussi la charge d'appliquer la politique de sécurité de l'entreprise et contribue à son renforcement par l'étude et la mise en œuvre de solutions techniques. Enfin, il veille au bon usage du système de ses utilisateurs, en menant des actions de sensibilisation et de diffusion de bonnes pratiques.

Bien que je n'aie pas encore de diplôme dans ce domaine, je me suis tout de même senti légitime de postuler grâce à deux éléments de mon CV.

Le premier est mon diplôme DU3MI, qui a pour objectif de former des responsables de tiers-lieux numériques, et qui propose tout un module dédié aux bases des réseaux informatiques. Le second ma casquette de référent informatique dans mes premières années de bibliothèques qui m'a permis d'être en contact avec des techniciens avec qui j'ai pu acquérir des notions autour de la gestion d'un serveur, du raccordement physique d'un nouvel équipement ainsi que de l'adressage IP.

Je me suis donc rapidement approprié ces missions en plus et ce sera tout le propos de cette activité qui se présentera en deux parties.

Dans un premier temps je présenterais l'infrastructure réseau dont le point central est la bibliothèque d'Epinal, à partir de laquelle nous avons rattachées toutes les autres bibliothèques au fur et à mesure de leur entrée dans le réseau de lecture publique. Dans un second temps, j'expliquerais comment je l'administre au quotidien et comment je m'en suis servi pour proposer un service innovant afin de moderniser le fonctionnement des médiathèques.

I. L'infrastructure du réseau

a) La bibliothèque d'Epinal : un cœur de réseau à rafraîchir

L'état de l'équipement informatique à mon arrivé

La nouvelle bibliothèque d'Epinal a été inaugurée en 2009. Elle a été pensée pour dispenser un service public aux seuls habitants des deux communes d'Epinal et de Golbey, les deux seules communes qui comptaient l'EPCI d'Epinal, accompagnée d'un plus petit bâtiment à Golbey.

- Leur raccordement :
 - Une fibre qui avait été tirée entre les deux bâtiments avec seulement un point relais à mi-chemin dans un équipement de la ville d'Epinal.
 - Permet au seul poste professionnel de se connecter au réseau d'Epinal comme s'il s'y trouvait physiquement, lui permettant ainsi d'accéder à tous les services hébergés sur les serveurs d'Epinal.
- Médiathèque de Golbey, équipée pour être le relais d'Epinal
 - Petit local pourvu d'une baie Murale 9U

U : Unité de mesure pour désigner la hauteur d'un appareil destiné à être placé dans une baie de brassage. 1 U = 44,45 mm

- Un panneau de brassage

Un panneau de brassage est un élément non électronique d'une baie de brassage qui ne sert qu'à organiser physiquement les câbles.

C'est sur cet élément que l'on va rapporter les noms des prises, afin de repérer le câble qui lui est associé.

- Une box Internet

Box Internet : équipement réseau qui permet un accès à Internet.

Il est fourni par un FAI (Fournisseur d'Accès Internet) au moment de la souscription à un abonnement Internet et conservé tout le long de la durée de l'abonnement.

- Une borne WIFI

Équipement réseau qui permet l'accès à un réseau ou à Internet par le biais d'ondes électromagnétiques.

- Un switch qui sert de :

_ Point d'arrivée de la fibre qui relie les deux médiathèques

_ Desserte Internet pour la borne ainsi que les deux postes mises à la disposition du public

Un switch est un équipement réseau qui permet l'interconnexion entre les différents appareils d'un réseau. Il permet également une segmentation logique d'un réseau complexe.

- Proxy Ucopia : Insérer entre la box et les deux postes publics

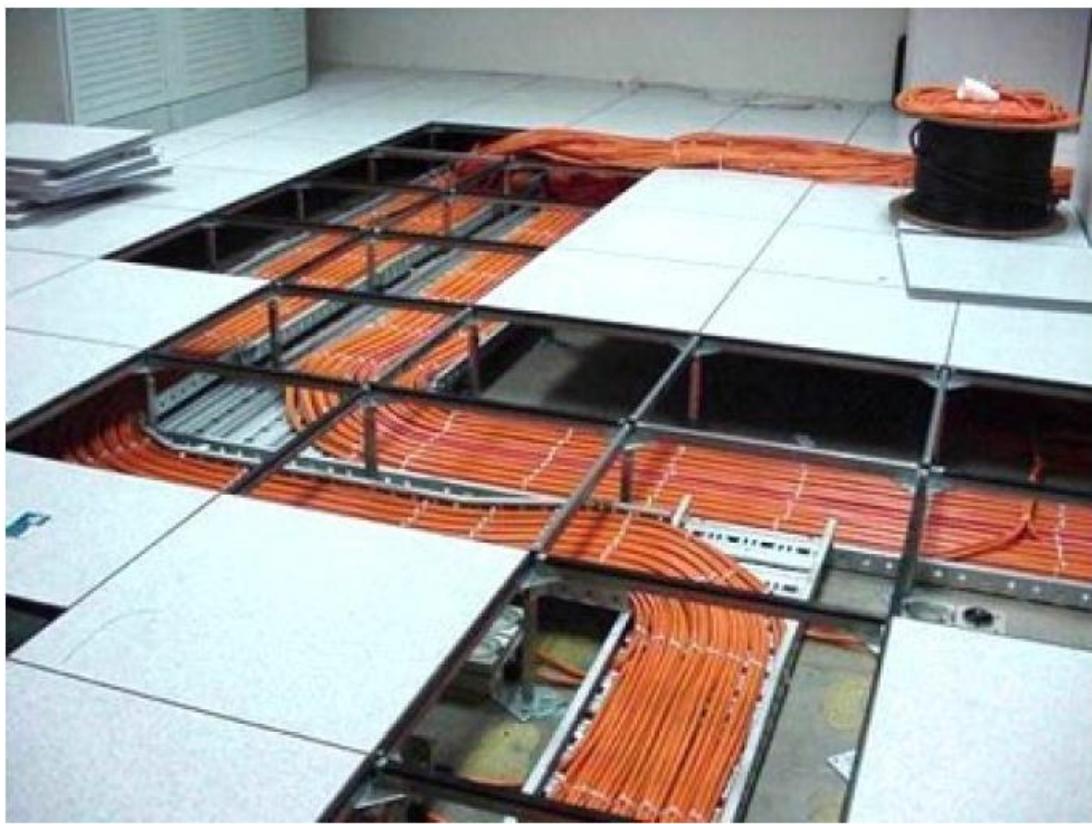
Un proxy est un élément réseau qui sert d'intermédiaire entre des appareils clients et internet.

Il me sert, entre autres, au filtrage des sites visitables par le biais de l'accès Internet des bibliothèques. Il va également enregistrer toutes les activités réalisées sur Internet, quel que soit l'appareil utilisé.

- Médiathèque d'Epinal, dimensionnée pour être le centre névralgique d'un petit réseau et pour fonctionner en autonomie.
 - Pourvue d'une salle serveur dédiée avec une importante baie de brassage composée de 3 armoires.
 - Plusieurs panneaux de brassages qui contient les prises RJ45 reliés aux prises murales.



- Le tout desservi par des centaines de câbles 100Mbps qui filent à travers les cloisons et les faux plafonds, à partir du plancher technique de la salle serveur et dispatchés aux 2 niveaux qui composent le bâtiment.



- Deux switches permettant de répartir les équipements et terminaux dans 3 VLANs. Enfin, un des switches réceptionne le raccordement fibre de Golbey



VLAN (Virtual Local Area Network) est un groupe d'appareils, appartenant à un plus gros réseau local, reliés logiquement entre eux.

Ils disposent de toutes les fonctionnalités d'un réseau local classique. Mais ne peuvent plus communiquer avec le reste du réseau physique.

- Une douzaine de bornes WIFI disséminées dans la bibliothèque.



- 2 serveurs hyperviseurs sur lesquels tournaient plusieurs machines virtuelles.

Un hyperviseur est un super-ordinateur offrant une plateforme de virtualisation permettant de faire fonctionner plusieurs machines virtuelles en même temps, en fonction de ses capacités.

Ces machines correspondent au :

- _ Serveur DHCP, DNS et AD du VLAN pro
 - _ Serveur DHCP, DNS et AD du VLAN public
 - _ Serveur DHCP et DNS du VLAN formation
 - _ Réplication du serveur du VLAN pro
 - _ Serveur Web
 - _ Serveur de messagerie
-
- Un serveur dédié à l'hébergement du logiciel SIGB de l'époque (Aloes de l'entreprise Archimed) fonctionnant avec des bases de données MySQL

MySQL est un système de gestion de bases de données relationnelles.

Les logiciels qui traitent ses bases de données sont des SGBDR (Système de Gestion de Bases de Données Relationnelles).

- Un autocommuateur PABX

PABX (Private Automatic Branch eXchange) est un appareil qui sert à relier un réseau de téléphonie interne au réseau externe. Il permet également plusieurs services en interne, tels que les appels en interne ou le transfert d'appel par exemple.



- Un lecteur de bandes magnétiques

C'est un périphérique de stockage de données au même titre qu'un disque dur par exemple.

Il est utilisé ici pour les sauvegardes des fichiers.

- Deux pares-feux

_ Le pare-feu est un élément du réseau dont le rôle principal est de le sécuriser en définissant les communications autorisées et interdites

_ A la BMI c'est également lui qui prend en charge le routage :

_ Le routage est le processus de choix des routes à empruntés pour acheminés les paquets d'une machine à une autre.

_ Ici le routage est dynamique afin de permettre une répartition des charges.

_ Le protocole utilisé est l'OSPF (Open Shortest Path First)

_ Le pare-feu a le rôle d'OSPF DR (Designated router) ou OSPF référent



- Un proxy dédié au VLAN public.



- Enfin la connexion Internet était assurée par une box fibre doublée d'une connexion SDSL en cas de panne de la fibre.

SDSL (Symmetric Digital Subscriber Line) est une connexion Internet qui garantit une bande passante montante, équivalente à celle descendante. Elle garantit également un débit minimum en temps de fonctionnement opérationnel. Toutefois, son débit est bien en dessous des capacités d'une connexion fibre (quelques dizaines de Mbps, tout au plus).

Ainsi la communauté de communes de 2009 c'était dotée d'un équipement fiable et relativement stable. Toutefois, c'est un réseau qui était bien calibré pour le projet de départ, mais qui a montré toutes ses limites au moment de l'intégration des bibliothèques de Thaon-les-Vosges en 2013 puis de Deyvillers en 2015. Les débits étaient trop limités pour permettre des connexions à distance fluides et fiables.

Événements extérieurs favorables

Toutefois, avant de pouvoir financer et justifier de tels travaux, il aura fallu la convergence de plusieurs événements, afin de permettre une opportunité que la direction va saisir avec l'appui des pouvoirs publics locaux :

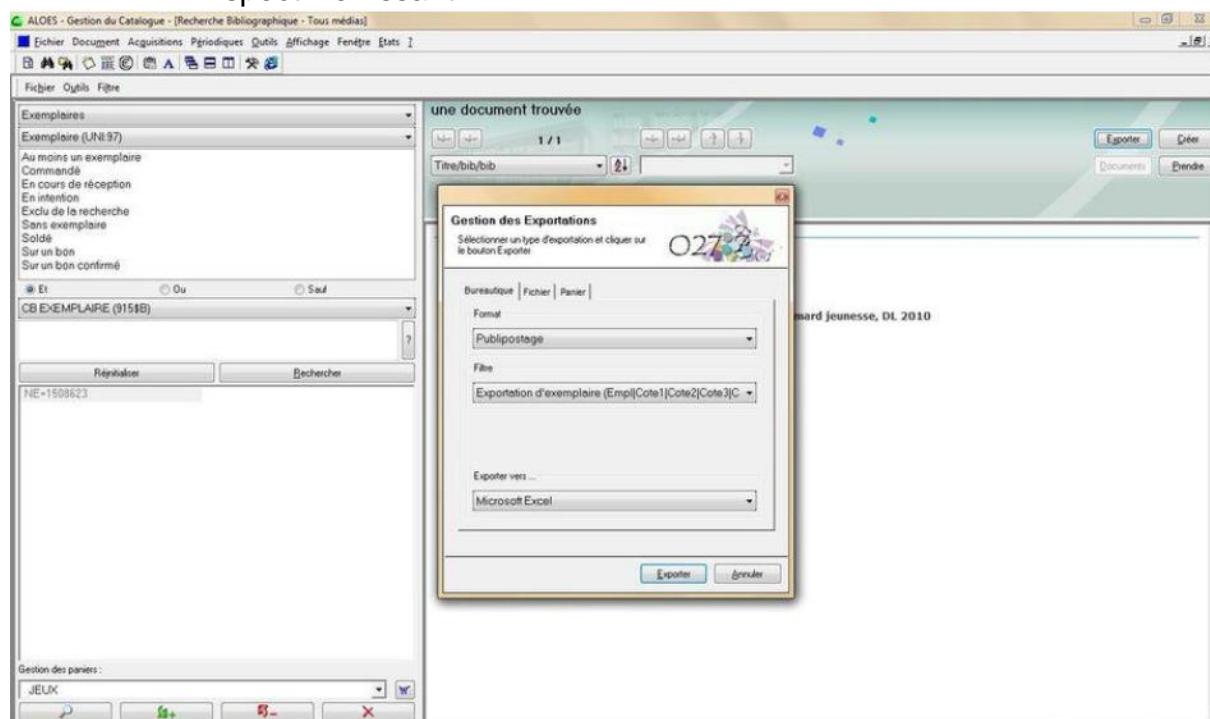
- La promulgation de la loi NOTRe (nouvelle organisation territoriale de la république).

La loi n° 2015-991 du 7 août 2015 ou la loi NOTRe a été promulguée sous la présidence de François Hollande.

Elle a, entre autres, précisé les compétences des collectivités, renforçant celles des régions et des EPCI et à réhaussé le seuil d'habitants minimum des Communautés de Communes faisant passer celui-ci de 5000 à 15000 au 1^{er} janvier 2017.

Ce qui entraîne dans ma collectivité :

- Accélération du processus de rattachement des territoires isolés à Epinal bien que parfois très éloignés (plus d'une demi-heure de route pour les communes les plus lointaines),
- Renforcement des compétences prises par la communauté d'agglomération dont la compétence culturelle.
- Arrivée massive de bibliothèques dans le réseau de lecture publique qui va devoir être repensé si l'on veut un réseau de bibliothèques cohérent.
- Abandon du SIGB actuel par la société Archimed,
- Aspect vieillissant



- Ne s'adaptait pas aux nouveaux usages des bibliothèques et notamment à leurs regroupements
- Lourd en besoin d'installations pour des structures qui ne sont pas toujours bien dotés en termes de matériel informatique.
- Développe à la place une solution en mode SaaS (Software as a Service).

Un service SaaS est un service basé sur le Cloud. Il n'est plus installé directement sur les machines. Mais est accessible par le biais d'une connexion Internet.

Ses avantages :

- _ Accessible de n'importe quel endroit et avec n'importe quel terminal

_ Son hébergement, sa disponibilité, ses sauvegardes et ses mises à jour sont maintenant du ressort du prestataire

Ses inconvénients :

_ Le coût sur le long terme est plus élevé qu'un achat de licence, du fait que l'on paye un abonnement qui peut être très important en fonction des options choisies. Ce coût est toutefois contrebalancé par les économies réalisées sur le matériel et les ressources pour mettre en place, le faire fonctionner en interne et le rendre accessible aux autres médiathèques du réseau.

_ Rend dépendant de la connexion Internet, ce qui nécessite tout de même de mettre en place une solution de secours, en mode dégradé, en interne.

- Mise en place du projet BNR (bibliothèque numérique de référence) par le ministère de la culture. Celui-ci permettait, sur dossier, de prendre en charge jusqu'à 80% des dépenses liés à des projets qui contribue à la modernisation des structures ainsi qu'à atteindre de nouveaux publics grâce à des services numériques innovants.

Tout ceci va aboutir à une réflexion d'une extension du réseau pour chaque nouvelle bibliothèque qui intégrera le réseau de lecture publique d'Epinal. Ce qui va également obliger une réfection de l'infrastructure de sa médiathèque principale, celle-ci devant être le point central vers lequel toutes converges.

Rafraîchissement de la médiathèque d'Epinal

Les éléments remis à neuf sont :

- La connexion Internet :

➤ Suppression de la ligne SDSL :

_ Ne suffit plus à prendre en charge les demandes de connexion en cas de panne de l'Internet principale

_ Prix plus élevé qu'une connexion fibre

➤ Ajout d'une seconde fibre :

_ Compense la perte de connexion en cas de panne de la première

_ Permet la mise en place du Load balancing lorsque les deux fonctionnent

Load balancing : procédé permettant une répartition équilibré des tâches entre plusieurs appareils ayant la même fonction.

Toutefois, l'installation présente, à mon avis, deux défauts.

_ Premier défaut : Lors de l'achat de la seconde fibre, il a été imposé de passer par le fournisseur SFR qui a obtenu le marché de la fibre de la C.A.E. Or, notre première fibre est de chez Numéricâble qui a été racheté entre temps par SFR. Nous n'avons donc aucune solution de secours en cas de défaillance de celui-ci. La SDSL avait l'avantage de provenir d'un autre fournisseur, en l'occurrence Orange.

_ Second défaut : Les deux fibres pénètrent dans le bâtiment au même endroit, à savoir la salle serveur. Or, pour bien faire, il aurait fallu que les deux connexions arrivent par un côté différent l'une de l'autre.

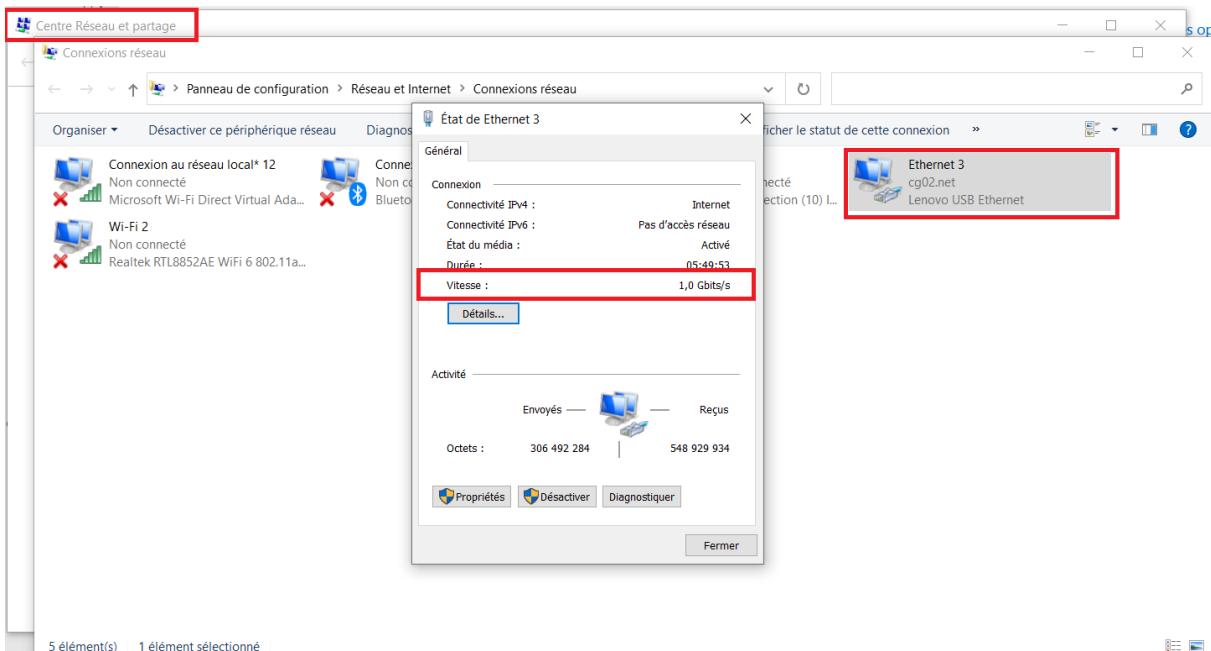
- Le câblage :
 - Régie par les normes ISO/CEI 11801 (normes internationales) et NF EN 50173-2/A1 (normes françaises et européennes) en matière de recommandations de câblage ainsi que par la norme ANSI/TIA-568 qui définit certaines caractéristiques techniques des composants.
 - Installés par une entreprise d'électriciens
 - Câblage cuivre de catégorie 6 pour un débit de 1000 Mbps
 - Blindage :

_ FTP (Foiled Twisted Pair) pour les câbles courant à travers le bâtiment.
 _ UTP (Unshielded Twisted Pair) pour les câbles allant des prises aux terminaux



Je pense pour ma part que les choix de câblages sont judicieux :

_ Les normes sont respectées
_ Le choix des débits est cohérent. En effet, les connexions fibres, permettant de dépasser les 100 mbps, il est important qu'elles ne soient pas bridées par des câbles trop limités. Toutefois, il n'est pas nécessaire d'aller jusqu'au 10 gbps plus couteux. La connexion Internet n'atteint pas ces niveaux de performances et les câbles auraient été bridés par les capacités des cartes réseaux des postes limitées à 1Gbps (que l'on peut connaître en ouvrant le « centre réseau et partage » et en double cliquant sur la carte réseau).



_ Les choix de blindage également. En effet, le FTP qui est écranté avec une feuille d'aluminium, permet d'atténuer les effets de la diaphonie (transfert d'énergie d'un signal sur un autre) qui pourrait être causé par la présence de câbles électriques à proximité par exemple. C'est indispensable pour les câbles qui couvrent plusieurs dizaines de mètres à travers les murs et plafonds. En revanche, ce n'est pas indispensable pour ceux qui relient un terminal à une prise murale. En effet, ça ne couvre que quelques dizaines de centimètres parfois. Le UTP, sans aucune protection, donc moins coûteux, est suffisant.

- Ajout de prises dans les bureaux :
 - Dû à la réorganisation des bureaux :

_ Recrutement de personnel pour aider dans la coordination du réseau
 _ Recrutement de personnel pour permettre des remplacements dans les autres médiathèques
 _ Aménagement de postes à disposition des personnels des autres médiathèques à Epinal

- Pour l'aménagement des bureaux, il existe un cadre de référence non obligatoire, la norme Afnor NF X 35-102
- La direction a opté pour un poste tous les 9 m² environs. Pour chaque poste, la présence de 4 prises électriques et de 2 prises réseaux (exceptés les postes dédiés aux réceptions des commandes qui obligent la présence en permanence d'une platine RFID et donc d'une 3^{ème} prise réseau).

_ le choix des m² est quelque peu en dessous de la norme (9m² au lieu des 11 préconisé). Cela s'explique par la contrainte des tailles des pièces existantes ainsi que

la volonté de la direction que chaque équipe puisse se tenir dans un seul bureau et que chacune soit le plus possible isolée.

_ Le choix du nombre de prises est pertinent. En effet, la présence de deux prises réseau permet le raccordement d'un PC et d'un téléphone IP pour chaque poste ce qui est suffisant, du fait que les impressions se font par le biais d'un copieur, partagé sur le réseau et présent dans un petit local de reprographie. Aussi, si un besoin ponctuel oblige le raccordement d'un troisième appareil en réseau (une platine RFID par exemple), je mets à disposition des petits switches 4 / 6 ports. Il n'était donc pas nécessaire d'ajouter une 3^{ème} prise réseau à chaque poste, compte tenu du surcout que ça aurait entraîné.



La présence de 4 prises électriques permet de raccorder aisément le PC et le téléphone en permanence tout en conservant la possibilité de raccorder des appareils d'appoint tel qu'un switch 4 port + une platine RFID ou d'avoir sous le coude une prise pour recharger son téléphone par exemple.

- Remplacement des switches :
 - Tous les ports ont maintenant une vitesse de 1Gbps
 - Présence de ports fibres
 - Switches 48 ports
 - Ajout d'un 3^{ème} switch
 - Manageables
 - Gèrent le protocole STP (Spanning Tree Protocole)

Le choix des switches me paraît cohérent avec l'évolution souhaité du réseau.

En effet, pour le choix des ports, il est important que la vitesse des ports des switches soit en adéquation avec les capacités des câbles. De plus, il faut garder le raccordement fibre de la médiathèque de Golbey maintenu et pouvoir faire de même avec le service informatique de la ville d'Epinal.

Aussi, les 48 ports des 2 anciens switches étaient occupés. Or, l'ajout de postes professionnels, ainsi que la mise en place du service RFID (expliquée dans la dernière sous partie de cette activité) implique qu'il y en a davantage de disponibles. Une première solution aurait été d'acheter deux switches plus grands (64 ports chacun aurait suffi). Toutefois, le choix de 3 switches 48 ports me paraît plus pertinent :

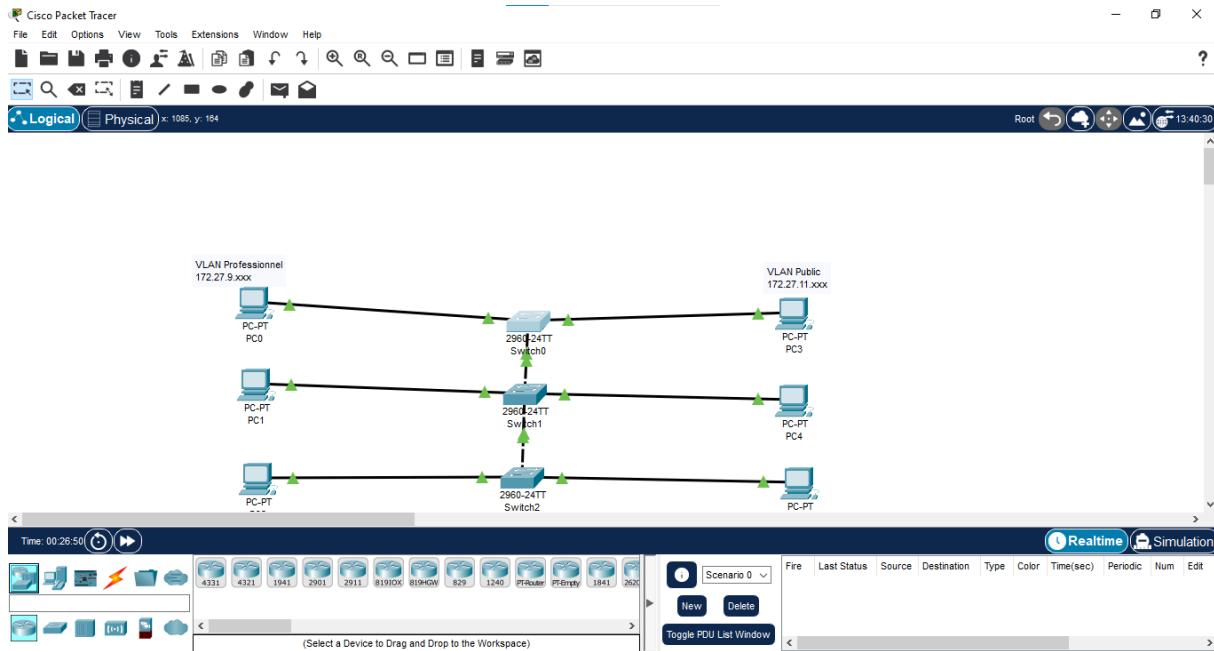
- _ Plus de ports de disponibles ($48 * 3 = 144$ contre $64 * 2 = 128$)*
- _ Répartir les appareils sur 3 switches permet une meilleure tolérance à une panne. En effet, répartie sur 2, c'est la moitié du réseau qui est coupé, contre un tiers seulement, si répartis sur 3.*

Enfin, le maintien des VLAN implique forcément que ceux-ci doivent être manageable et le protocole STP est la réponse apportée à un incident survenu il y a peu et expliqué dans l'activité 3.

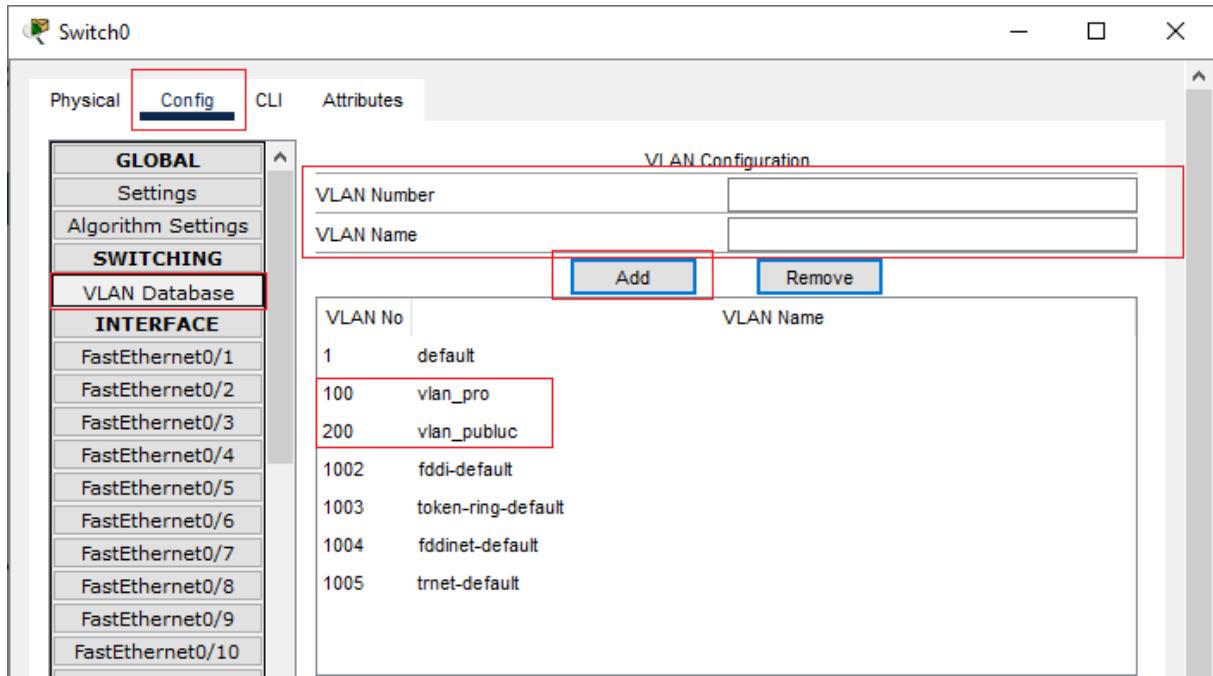
- Avant de configurer les nouveaux switches, j'utilise un logiciel de maquettage. Il me permet de simuler les installations et les configurations. Le but est de vérifier que tout sera bien opérationnel au moment de l'installation.
Le logiciel que j'ai utilisé, s'appelle Cisco Packet Tracer

[Cisco Packet Tracer](#) est un simulateur de matériel réseau créé par Cisco System, un des leaders du marché.

- _ Avantages :*
 - _ Gratuit*
 - _ Très réaliste, il permet de comprendre la philosophie de chaque type d'appareil*
 - _ Outil pédagogique*
 - _ Accompagné de cours d'initiation et de perfectionnement pour le prendre en main*
- _ Inconvénients :*
 - _ Les appareils testés sont uniquement des appareils Cisco*
 - _ Les manipulations peuvent varier lorsque l'on manipule un matériel d'un autre constructeur*

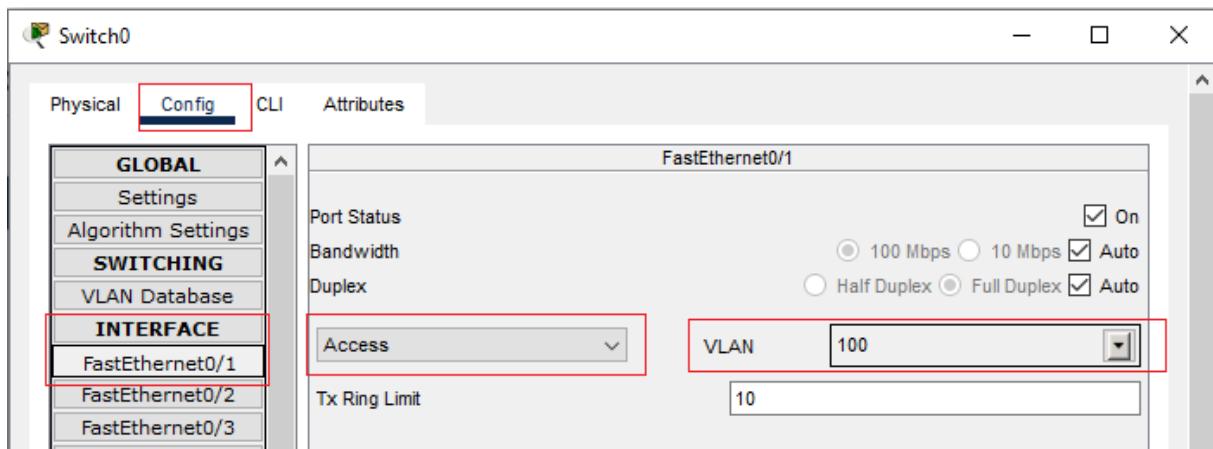


- Afin de valider mon montage, je test les différentes connectivités entre les machines :
 - _ J'utilise la commande ping (expliquée plus tard dans cette activité)
 - _ Les résultats attendus :
 - _ Les pings entre les 3 PC du VLAN professionnels doivent être positifs
 - _ Les pings entre les 3 PC du VLAN public doivent être positifs
 - _ Les pings d'une machine du VLAN professionnel vers une machine du VLAN public doit être négatif
 - _ Les pings d'une machine du VLAN public vers une machine du VLAN professionnel doit être négatif
 - Une fois la maquette validée, je configure les switches avant de les installer dans la baie. En faisant de cette manière, les anciens switches continuent d'effectuer le travail, le temps que je termine. Ça évite de paralyser le réseau trop longtemps.
 - Pour chaque Switch, le paramétrage c'est fait en 3 temps :
 - _ Dans la base de données des VLAN, je crée les 3 VLAN : professionnel, public et salle de formation.
- Pour se faire je vais dans l'onglet de configuration du switch. J'ouvre ensuite le sous-menu « Switching » « VLAN Database ». Ici, j'affecte un numéro et un nom à un VLAN et je clique sur « add » (ajouter). Je fais cette opération 3 fois, pour les 3 VLAN. En faisant attention que chacun ait un nom et numéro différent.



_ Pour chaque port, je lui affecte un numéro de VLAN, en fonction du plan donné par mon chef.

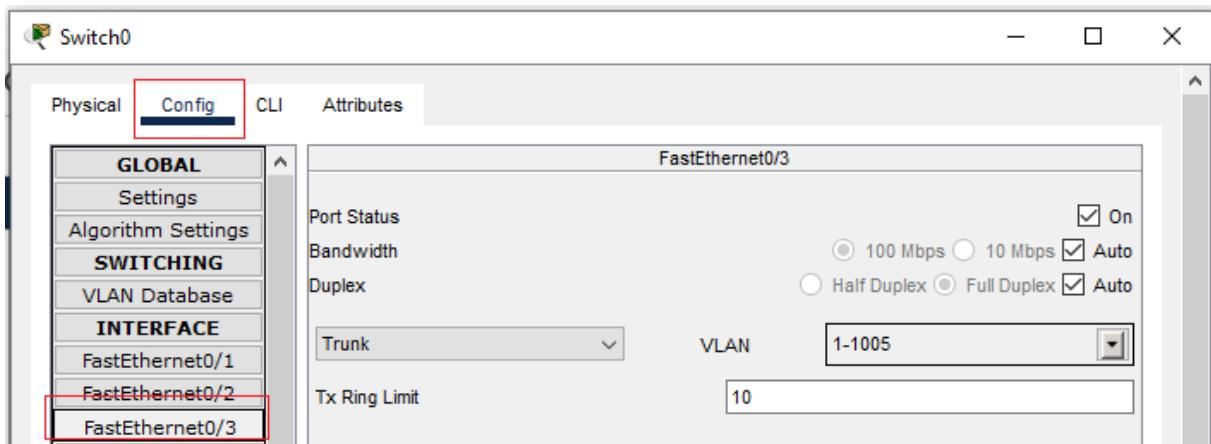
Pour se faire, toujours dans l'onglet « config », je vais dans le menu « Interfaces » et je clique sur le port à configurer. Je le met en mode « access » et je lui affecte le numéro du VLAN souhaité par le biais du menu déroulant.



Avec ses deux étapes, les ports sont maintenant configurés pour ne communiquer qu'avec ceux qui ont le même numéro VLAN d'affecté.

_ J'affecte à chacun un ou deux ports, en fonction de leur position dans la baie, à la communication avec les deux autres switches.

Pour se faire, toujours dans « Intefaces », au lieu de mettre le port en mode « access », je le met en mode Trunk (lien). Ces ports serviront à relier les switches entre eux.



C'est grâce à cette manipulation qu'un appareil du switch 1 pourra communiquer avec les appareils des switches 2 et 3, du moment qu'ils ont le même numéro VLAN.

- Remplacement du lecteur de bandes magnétiques par un NAS (Network Attached Storage), installé dans la salle serveur du service informatique de la mairie d'Epinal. En contrepartie, ils ont installé un des leurs dans la salle serveur de la bibliothèque.

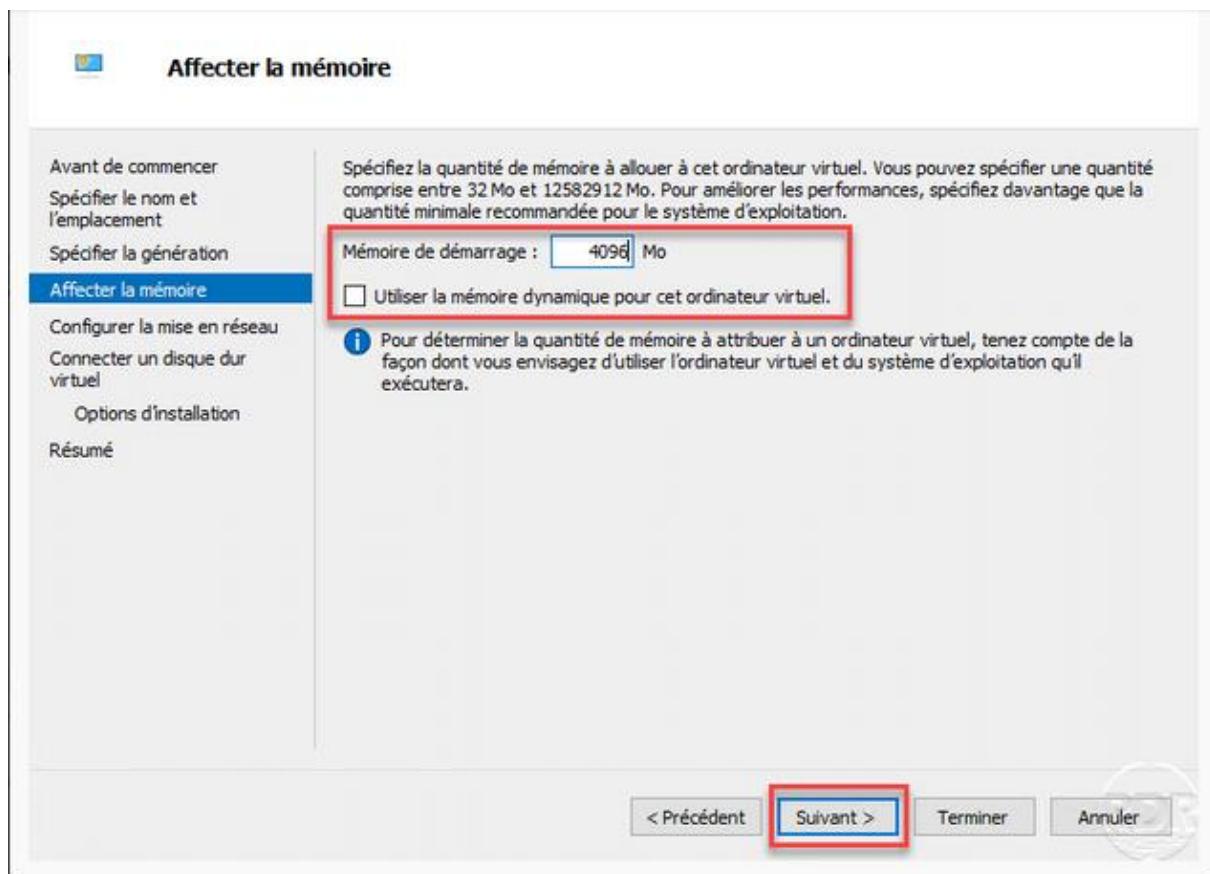
Lecteur de bandes magnétiques reste un système de sauvegarde fiable. Aussi, je pense qu'il aurait pu être conservé bien que l'installation du NAS me semble tout de même nécessaire.

En effet, jusqu'à présent, pour répondre au besoin de la présence d'une sauvegarde hors les murs, j'apportais la cassette de la semaine précédente au service informatique de la ville qui me remettait la leur. Avec ce système, nous risquons qu'un événement corrompe ou détruisse la cassette en cours d'utilisation et de nous retrouver avec quasiment une semaine de données de perdu. Problème que le NAS résout.

Toutefois, je pense qu'il aurait pu continuer à être utile, notamment pour l'archivage des versions numérisés des documents patrimoniaux, qui nécessite de longues durées de conservations et avec des besoins de restitutions de grande qualité.

- Remplacement des hyperviseurs
 - Processeur plus performant, plus de RAM et de capacité de stockages
 - Plusieurs alimentations et plusieurs cartes réseaux
 - Réinstallation des machines virtuelles sur des OS Windows server 2016

Les anciens hyperviseurs fonctionnaient encore très bien au moment de leur remplacement, qui n'était donc pas une obligation. Toutefois, un financement comme le BNR ne se présentant pas tous les jours, c'était, je pense, une opportunité que la direction à bien fait de saisir. Leur remplacement à fait gagner presque 10 ans de durée de vie au parc. De plus, leurs composants plus performants permettent d'allouer plus de ressources aux VM (Virtual Machines).



Toutefois, pour des raisons économiques et écologiques, les anciens hyperviseurs ont été donnés au service informatique de la ville d'Epinal, qui en a très certainement fait bon usage. Tout comme nous leur donnons tout le matériel remplacé qui n'est pas cassé ou obsolète, afin que ça puisse être réinstallé dans d'autres services avec moins de moyen de la C.A.E (écoles, crèches, petite mairie etc.)

Installation serveur Windows 2016

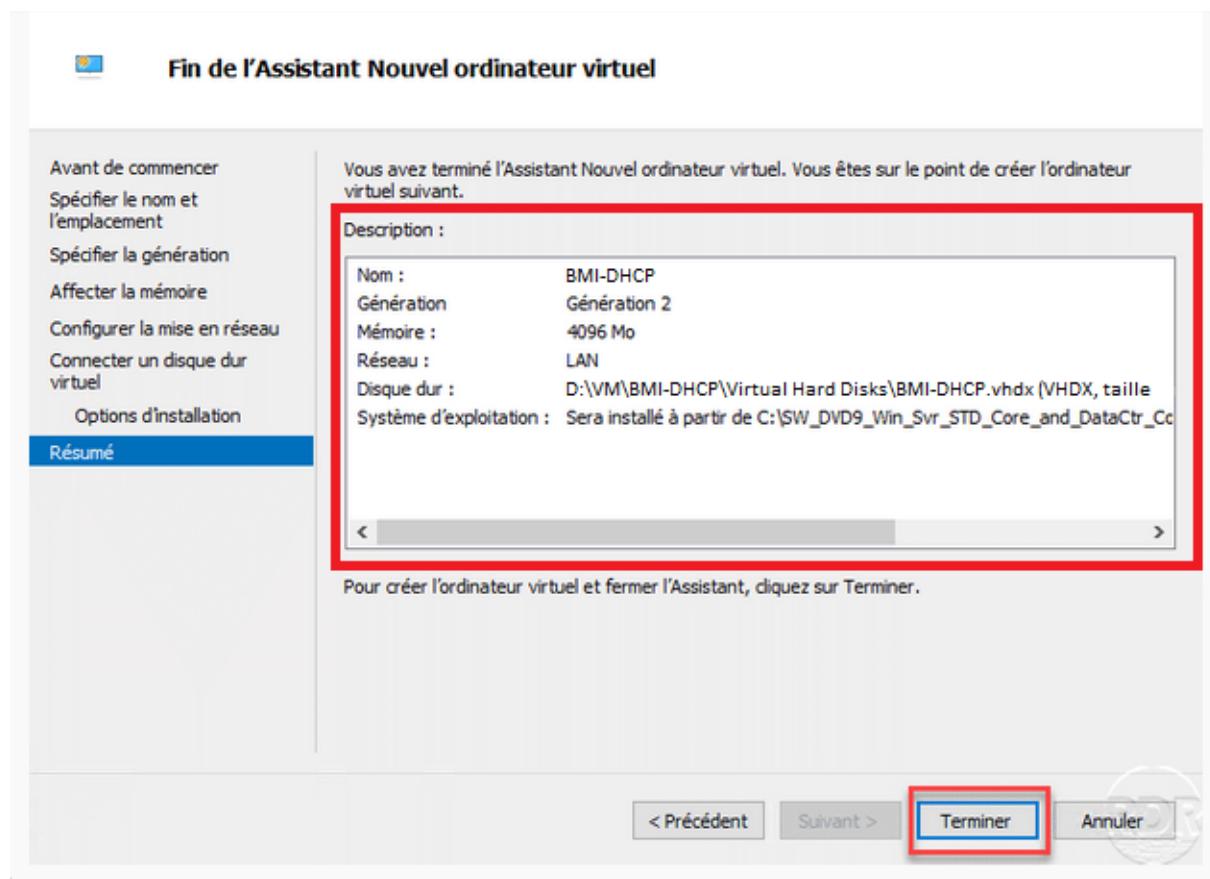
Pour ne pas perdre trop de temps et que la réinstallation des serveurs ne perturbent pas le travail des bibliothécaires, nous nous étions réparti les tâches. La mienne était de préparer les [VM \(Virtual Machine ou machines virtuelles\)](#) sur les nouveaux Hyper-V, avant leur mise en production.

- Les avantages de cette manière de procéder :
 - _ Permet de vérifier que le matériel soit opérationnel en conditions réels
 - _ Permet de tester les machines sans que ça ne perturbe les bibliothécaires si ça vient à mal se passer
 - _ Permet de gagner du temps le jour du remplacement des machines et de sa mise en production
- Les étapes de la mise en place des VM

➤ Ajout d'une machine virtuelle

Pour se faire, dans la console Gestionnaire Hyper-V, je clique sur le sous-menu « ordinateur virtuel » disponible dans le menu « nouveau » du volet « actions ». Ensuite je lui attribue :

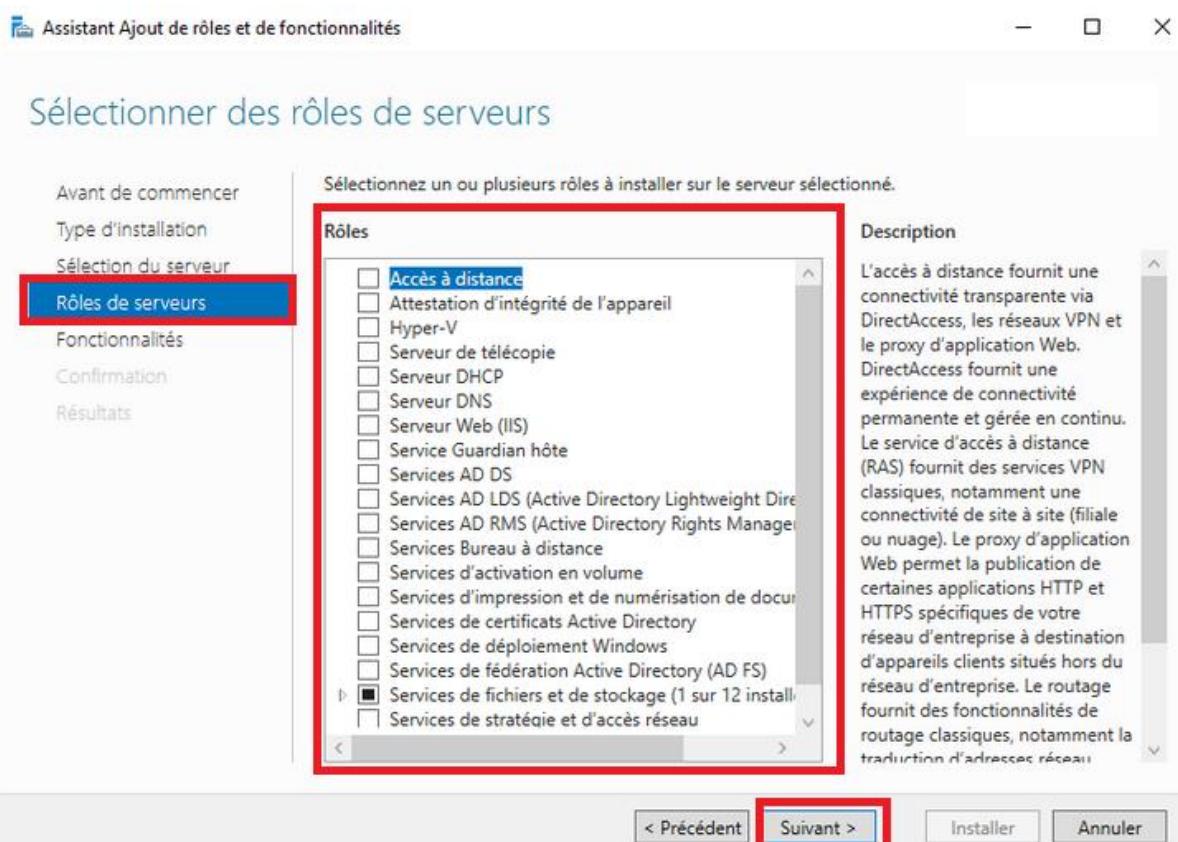
- _ un nom (en rapport avec la fonction du serveur qui sera installé dessus),
- _ un emplacement sur un des disques durs de l'Hyper-V
- _ une génération (En l'occurrence, je choisi la génération 2, plus récente, du fait que l'on va installer des OS 64 bits)
- _ une partie de la mémoire vive (ou RAM) de l'hyper-V qui lui sera dédiée
- _ un accès à la connexion Internet de l'Hyper-V grâce à la mise en place d'un LAN (Local Area Network) virtuel
- _ un disque dur virtuel avec une certaine capacité de stockage en fonction de sa fonction. Ce disque dur virtuel, sera en réalité une partie de l'espace de stockage de l'Hyper-V qui lui sera dédiée.
- _ Enfin, j'indique l'emplacement de l'ISO qui contient l'OS que je veux installer sur la VM



➤ Attribution des rôles et fonctionnalités des serveurs Windows

Pour se faire, j'ouvre l'écran correspondant au tableau de bord du gestionnaire de serveur. Je clique ensuite sur le menu « gérer » puis le sous-menu « ajouter des rôles

et fonctionnalités ». Après avoir déterminé le choix d'installation (« installation basée sur un rôle ou une fonctionnalité ») et le serveur du pool de serveur, je sélectionne les rôles. J'indique mes choix en cochant les cases correspondantes. Une fois les choix validés, une nouvelle fenêtre m'invite à valider l'installation des fonctionnalités essentielles à la prise en charge des rôles. Enfin, je peux, si je le souhaite, ajouter des fonctionnalités supplémentaires, que je sélectionne de la même manière que les rôles.



Aussi, la répartition des rôles et des fonctionnalités :

Rôles et fonctionnalités	Machines virtuelles concernées	Explicatifs
DHCP (Dynamic Host Configuration Protocol)	<ul style="list-style-type: none"> _ Serveur dédié au VLAN professionnel _ Serveur dédié au VLAN publication _ Serveur dédié au VLAN formation _ RéPLICATION du serveur dédié au VLAN professionnel 	Rôle qui permet au serveur de configurer automatiquement les paramètres IP aux terminaux autorisés à se connecter au VLAN. (Voir prochaine sous partie)

DNS (Domain Name System)	<ul style="list-style-type: none"> _ Serveur dédié au VLAN professionnel _ Serveur dédié au VLAN publication _ Serveur dédié au VLAN formation _ RéPLICATION du serveur dédié au VLAN professionnel 	Rôle qui permet de faire le lien entre les noms des machines et leur adresse IP
Service de fichiers de stockage	<ul style="list-style-type: none"> _ Serveur dédié au VLAN professionnel _ RéPLICATION du serveur dédié au VLAN professionnel 	Rôle qui permet à plusieurs utilisateurs d'accéder à un espace de stockage de fichiers communs
WSUS (Windows Server Update Service)	<ul style="list-style-type: none"> _ Serveur dédié au VLAN professionnel _ RéPLICATION du serveur dédié au VLAN professionnel 	Rôle qui permet de déployer les Mises à jour Windows des postes Windows du VLAN
Service AD DS (Active Directory Domain Service)	<ul style="list-style-type: none"> _ Serveur dédié au VLAN professionnel _ Serveur dédié au VLAN publication _ RéPLICATION du serveur dédié au VLAN professionnel 	Rôle qui met en place l'annuaire qui permet de gérer tous les objets contenus dans le domaine
Sauvegarde Windows serveur	<ul style="list-style-type: none"> _ Serveur dédié au VLAN professionnel _ RéPLICATION du serveur dédié au VLAN professionnel 	Fonctionnalité qui permet de sauvegarder tout ou une partie du serveur
RDS (Remote Desktop Services)	<p>Serveur dédié à la connexion à distance</p>	Rôle qui permet d'accéder à une machine du Réseau par le biais d'un terminal distant (Voir prochaine sous partie)

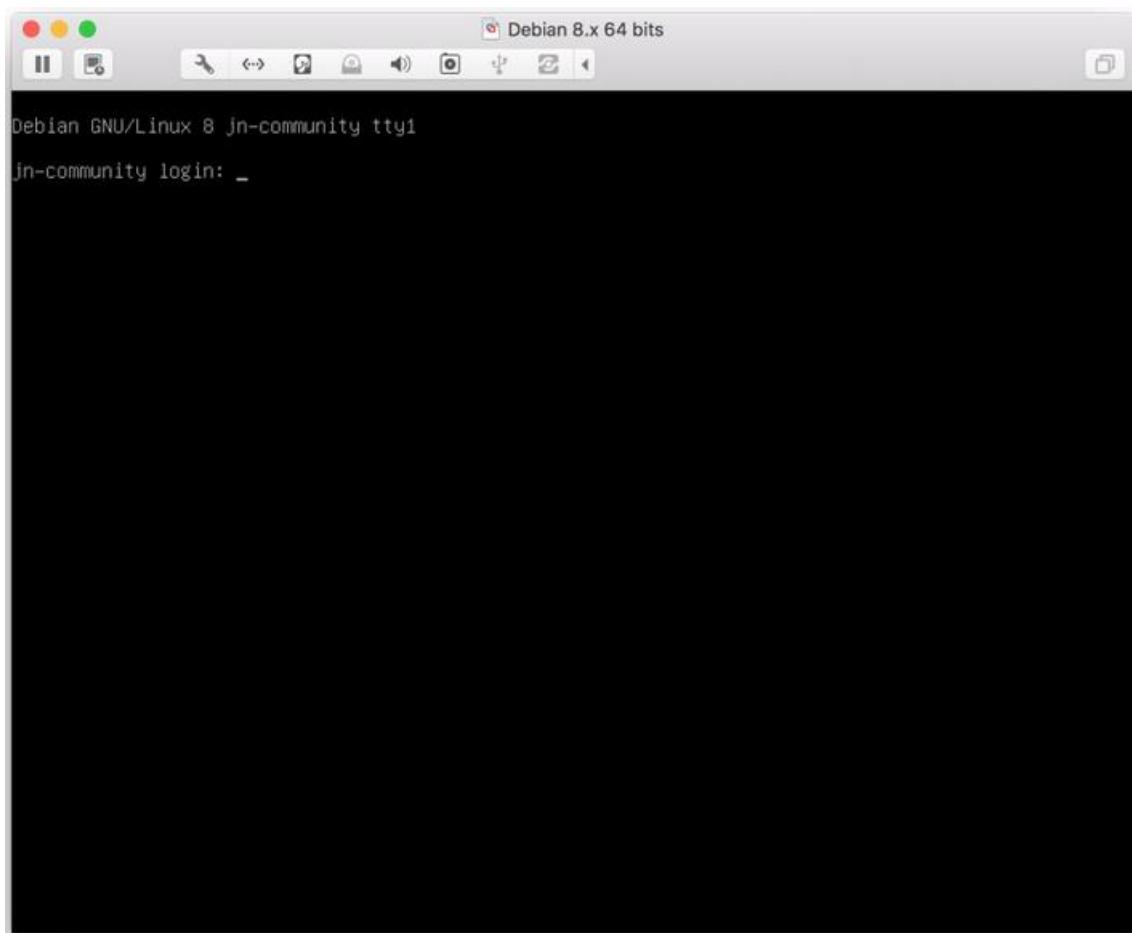
Installation d'un serveur d'applications sous distribution Linux

- La création de la machine virtuelle suit le même procédé que pour un serveur Windows
- J'ai téléchargé l'ISO d'un serveur de distribution Debian (stable et gratuit)
- Lors de l'installation je renseigne les informations suivantes :
 - La langue, pays et langue de clavier en français
 - La configuration IP (je choisis une IP fixe comme pour les autres serveurs Windows)

- Je nomme le serveur en fonction de son rôle (GLPI, Zabbix, Planno...)
- Je lui renseigne le nom de domaine professionnel, puisqu'il n'y aura que des applications destinées aux bibliothécaires
- Un mot de passe root

Root est le seul profil du serveur à avoir des droits administrateurs. Tous les autres profils (dont le mien) ne seront que des profils utilisateurs.

- Je crée ensuite mon profil utilisateur afin de pouvoir me connecter au serveur
- Je choisi de partitionner le disque de manière assistée et sur un seul disque (choix par défaut)
- Je désigne la France comme région pour le choix de la localisation du miroir Debian qui permettra l'installation des logiciels et mises à jour
- Une fois le serveur installé, sa gestion se fait par le biais d'une console de commandes



- J'installe ensuite des logiciels complémentaires :
 - Apache pour répondre aux requêtes HTTP
 - PHP qui est l'intermédiaire entre les pages web et les bases de données
 - Maria DB qui gère les bases de données
 - phpMyAdmin qui permet de gérer les bases de données de manière graphiques
 - Pour l'installation je tape les commandes :
 - « sudo » pour passer sur le profil administrateur

- « apt-get install xxx » pour installer les logiciels (xxx correspond au nom du logiciel que j'installe)
- « apt-get update » pour effectuer la mise à jour des listes des logiciels disponibles
- « apt-get upgrade » pour effectuer les mises à jour du système et des logiciels

- J'installe l'application souhaitée (par exemple GLPI)
 - Je télécharge l'application avec la commande « wget » suivi de l'URL complète du logiciel

URL (Uniform Resource Locator) c'est l'adresse Internet de la ressource

Pour GLPI : https://github.com/glpi-project/glpi/releases/download/X.X.X/glpi-X.X.X.tgz (X.X.X correspondant au numéro de version du logiciel)

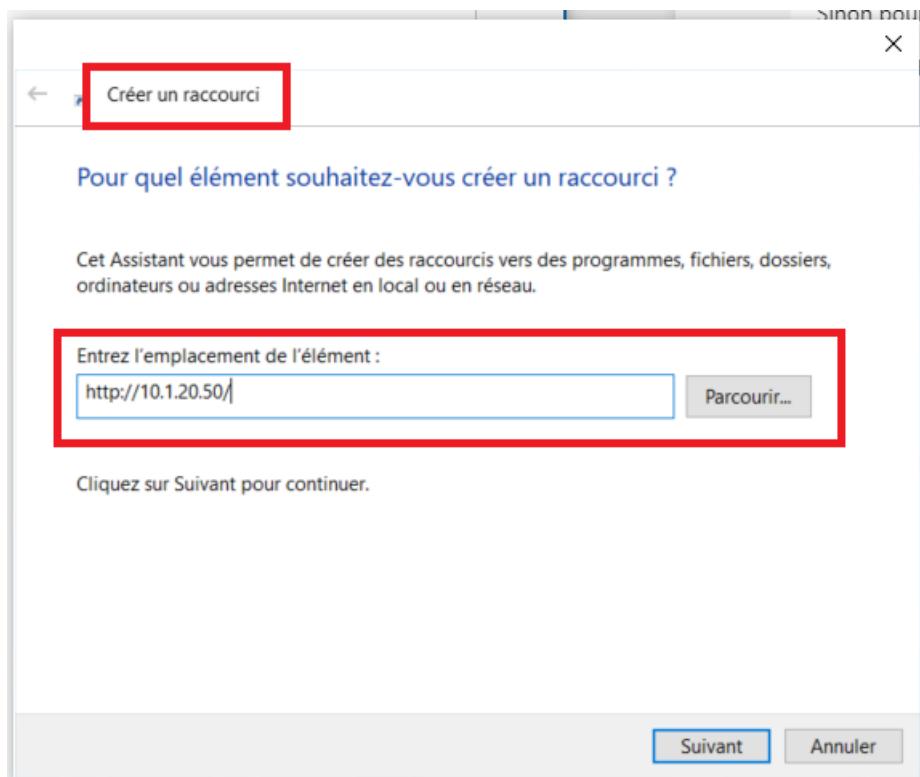
- Je décomprime l'archive avec la commande tar suivi du nom du logiciel
- Je modifie certains droits d'accès à certains dossiers en les réattribuant avec la commande « chown » auquel j'ajoute l'option « -R » (pour récursivité : c'est-à-dire que tous les objets à l'intérieur du dossier cité seront concernés par la modification des droits).

- Une fois l'installation réalisée, l'accès au logiciel se fait de manière graphique comme sur un Windows
- On y accède par le biais d'un navigateur web (bien qu'il ne soit pas sur Internet), en tapant l'adresse IP de la machine, suivi du '/' et du nom du logiciel.

The screenshot shows the GLPI web application interface. The URL in the browser bar is 192.168.1.49/glpi/front/passivedcequipment.form.php?id=1#. The main page title is 'GLPI'. The navigation menu on the left includes 'Parc', 'Assistance', 'Gestion', 'Outils', 'Administration', and 'Configuration'. The current page is 'Équipement passif'. The form is titled 'Tab01'. It contains fields for 'Nom' (Tab01), 'Lieu' (espace jeunesse), 'Responsable technique', 'Groupe technique', 'Numéro de série' (0123456789), 'Statut' (en service), 'Type' (tablette Android), 'Fabricant' (samsung), and 'Modèle' (Galaxy Tab A8). At the top right of the form, there are buttons for 'Cloner' and 'Amender le commentaire'. At the bottom of the form, there are buttons for 'Sauvegarder' (Save) and 'Mettre à la corbeille' (Delete).

Pour faciliter les accès aux collègues, je crée un raccourci dans le dossier en commun. Ainsi, lorsqu'un bibliothécaire clique sur le raccourci, il se retrouve directement sur la page de connexion du logiciel

Pour créer un raccourci, je réalise un clic droit sur le bureau Windows. Je sélectionne le sous menu « raccourci » du menu « nouveau ». Dans la nouvelle fenêtre j'indique la cible en entrant les mêmes informations que dans le navigateur précédent de 'http://'. Je donne ensuite un nom évocateur au raccourci.



Ces modifications dotent donc la bibliothèque d'Epinal d'un réseau rajeuni et plus performant.

Grâce à cela, elle peut ainsi devenir le cœur d'un réseau étendu permettant aux nouvelles arrivées de s'y greffer. Cela va aussi permettre l'intégration de nouvelles machines sur le site principal.

b) Les différentes connexions

Historiquement, la nouvelle bibliothèque d'Epinal, construite en 2009, a toujours eu un site distant relié à elle (la bibliothèque de Golbey). Toutefois, il n'était pas prévu, au départ, que les nouvelles bibliothèques qui intégraient la communauté d'agglomération, le soit.

Lors de leurs arrivées respectives en 2013 et 2015, les médiathèques de Thaon-les-Vosges et de Deyvillers fonctionnaient en complète autonomie vis à vis d'Epinal. Elles avaient leur propre SIGB ainsi que leur fond qui n'était pas intégré à celui d'Epinal.

Il y avait toutefois des signes d'une volonté de créer une entité unique :

- Les tarifs avaient été unifiés afin qu'un usager qui a une carte valide dans une médiathèque puisse bénéficier d'un abonnement gratuit dans toutes les autres.
- Il était tout de même possible de rendre ses documents dans n'importe quelle autre bibliothèque, même si ce n'était pas celle dans laquelle on l'avait emprunté.
- Des réunions étaient régulièrement organisées pour avoir un agenda d'animations cohérent.

Mais ce système, sans outils de travail collaboratifs en interne, a très vite montré ses limites :

- Il fallait sans arrêt téléphoner aux autres médiathèques pour vérifier les validités des abonnements. Aussi, on risquait que les bibliothécaires ne soient pas disponibles au moment de l'appel, laissant en suspend l'inscription.
- Il y avait un décalage entre le moment où un document est rendu dans une autre bibliothèque que celle du prêt et le moment où il est ramené par la navette pour être retiré du compte de la personne. Dû à cela, il y avait beaucoup de plaintes de lecteurs qui avaient des documents rendus depuis plusieurs jours, apparaître comme étant encore en leur possession.
- Il n'y avait aucune trace des retours des retours faits dans une autre bibliothèque que celle d'origine. Créant ainsi de nombreux conflits dû à des documents égarés ou à la mauvaise foi de certains lecteurs.
- L'absence d'un serveur de fichiers en commun ralentissait également le travail les projets d'animations entre bibliothèques. Aussi, a été mis en place un compte Google pour bénéficier d'un espace de stockage permettant le travail en collaboration. Toutefois, ça posait la question de la confidentialité des documents, vis à vis de la politique de Google. De plus, les documents n'étaient pas sauvegardés ailleurs que sur la plateforme, ce qui accroît le risque de pertes de données.
- Il n'y avait pas de portail commun sur Internet, rendant le projet incompréhensible auprès du public.

Avec la perspective d'une arrivée massive de nouvelles bibliothèques dû à l'expansion de la Communauté d'Agglomération imposée par la loi NOTRe, il n'était plus possible de fonctionner de cette manière. Surtout avec des établissements éloignés de plus d'une demi-heure de route. L'interconnexion devenait donc indispensable.

Connexions de sites distants

Il existe plusieurs manières de connecter des sites distants entre eux. Aussi, afin de choisir laquelle est la plus appropriée, il nous a été établie plusieurs contraintes à faire respecter.

- Le SIGB doit maintenant être unique pour toutes les bibliothèques et les fonds de chacune doivent pouvoir y être intégré. Cela va permettre :
 - Lors d'une recherche de document, de déterminer dans quels lieux il est disponible, ou, à défaut, à quelle date ils doivent être rendus.
Ainsi, on peut le lui réservé directement par le biais du logiciel et lui faire parvenir dans la médiathèque de son choix.
 - Que les retours puissent être enregistrés sur le logiciel au moment du dépôt des documents par le lecteur, quel que soit la bibliothèque choisie. Le logiciel garde un historique de la date et du lieu du retour en cas de litige ou de perte.
 - Avec une seule carte d'abonnement, les lecteurs sont reconnus dans n'importe quelle médiathèque du réseau.
- N'importe quel bibliothécaire ne n'importe quelle structure doit pouvoir :
 - Se connecter à n'importe quel ordinateur de n'importe quelle bibliothèque
 - Avoir accès à leur dossier personnel ainsi qu'aux dossiers partagés d'Epinal, où qu'il se trouve dans le réseau.
- Les bibliothèques doivent pouvoir fonctionner en autonomie, même si en mode dégradé, en cas de soucis techniques dans une autre. Notamment en cas d'une panne à Epinal.

La question est grandement simplifiée par la solution SaaS du logiciel. Grâce à lui, les bibliothécaires peuvent accéder à leur session professionnelle depuis n'importe quel terminal ayant simplement une connexion Internet, même si le bâtiment n'est pas relié à celui d'Epinal. Il permet ainsi :

_ D'être utilisé par toutes les bibliothèques du réseau. Simplement, son coût mensuel augmente, du fait du besoin grandissant de nombres de licences.

_ Un fonctionnement autonome de chaque structure. Chacune n'étant dépendante que de sa propre connexion Internet.

En ce qui concerne l'accès aux dossiers :

- *Une première solution aurait été de relier chacune des médiathèques à Epinal par une fibre. Comme c'est le cas à Golbey.*
 - Avantages :

Répond aux consignes que chaque agent puisse se connecter à n'importe quel poste du réseau et qu'ils aient accès aux fichiers partagés d'Epinal

_ La connexion se fait avec les mêmes identifiants qu'à Epinal, ce qui limite les risques de perdre un mot de passe

➤ *Inconvénients :*

_ Le coût de l'opération aurait été trop élevé par rapport à ce que ça apporte.

_ Une panne à Epinal aurait engendré une perte de service de toutes les médiathèques

Aussi, la solution du VPN qui a été choisie est pour moi la plus adaptée.

Le VPN

La solution qui a finalement été retenue est de configurer pour chaque site un accès à Epinal par VPN (Virtual Private Network).

- Géré par un pare-feu présent dans chaque site
- Caractéristiques :
 - IPSec

IPSec (Internet protocol Security) est un ensemble de protocole permettant un transport sécurisé des données.

➤ Site à site en étoile

C'est-à-dire que tous les sites distants ne sont reliés qu'à un site central (à savoir Epinal)

➤ Connexion par clés pré-partagées

C'est un mot de passe connu par les deux pares-feux, qu'ils s'échangeront au moment de leur connexion.

- Avantages :
 - L'achat des pares-feux à un coût moins élevé que la connexion par fibre
 - Répond à la problématique de l'accès aux dossiers partagés et dossiers personnels.
 - Permet aux structures de continuer à fonctionner de manière indépendante
- Inconvénients :
 - Engendre des frais annexes supplémentaires :

_ Contrat de maintenance pour chacun des pares-feux. Ça a été quelque peu compensé par le fait qu'ils ont tous été acheté en même temps chez le même prestataire. Ce qui a permis de profiter d'un tarif groupé

_ Location d'une adresse IP fixe pour chacune des boxes Internet présentes dans le réseau (exceptée la seconde fibre d'Epinal et celle de Golbey).

➤ Pour l'accès aux fichiers, les médiathèques du réseau sont toutes dépendantes de deux connexions Internet : la leur et celle d'Epinal.

Cette double dépendance est compensée par le fait qu'il est toujours possible de contacter un collègue de confiance, afin de faire transiter un fichier urgent, mais inaccessible depuis l'extérieur, par mail par exemple.

➤ Ne répond pas à la contrainte de la connexion sur tous les postes professionnels du réseau.

Pour résoudre ce problème, je configure les ordinateurs professionnels du réseau, différemment de ceux d'Epinal. Ceux-ci ne sont pas intégré à un domaine, mais dans un groupe de travail (voir explications plus bas dans cette partie). J'y crée deux sessions : une administratrice, pour moi configurer le système, et une simplement utilisatrice pour les bibliothécaires. De plus, je configure la connexion automatique à la session utilisatrice afin que ceux qui ont l'habitude de travailler à Epinal, n'aient pas un second identifiant et mot de passe de session à retenir (même procédé que pour les ordinateurs publics expliqué dans la première fiche). Pour se connecter aux fichiers, ils ont une icône de « connexion de bureau à distance » qui leur demanderont leurs identifiants d'Epinal.

Le seul inconvénient de cette méthode est qu'ils ne doivent pas laisser de documents personnels confidentiels sur l'ordinateur, au risque que le collègue qui prendra la suite aura accès aux informations ou sera perdu en cas de panne du PC. De plus, s'il n'en a pas fait une copie, ce document lui sera inaccessible jusqu'à sa prochaine connexion sur l'ordinateur

- Les différents composants :
 - La mise en place des tunnels VPN ainsi que les règles de filtrage sont réalisées par le prestataire qui fournit les pare-feux. Ils ont eu simplement besoin des informations suivantes :

_ Le nom du réseau local du site principal

_ Le nom réseau local du site distant

Ces deux noms sont donnés arbitrairement au moment du paramétrage des pare-feux. Simplement, il est convenu que leurs noms respectifs doivent être explicite par rapport au bâtiment auquel ils correspondent. De plus, ils doivent être notés exactement de la même manière dans chacun des appareils concernés.

_ L'adresse IP publique du Firewall principal

_ L'adresse IP publique du Firewall distant

Adresse IP publique : A ne pas confondre avec l'adresse IP privée du réseau (expliquée plus bas dans cette partie). C'est une adresse routable sur Internet que nous

attribue notre FAI. Il l'attribue par défaut de manière aléatoire en fonction de ses disponibilités qui peut varier d'une journée à l'autre.

Aussi, pour des besoins spécifiques comme celui-ci, il est impératif de louer une adresse publique fixe. C'est une option onéreuse disponible dans les abonnements business ou professionnels.

Le pare-feu se charge de faire la transition entre l'IP privée et publique, du fait qu'il gère le NAT.

NAT (Network Address Translation) est le processus de transition d'une adresse privée à une publique et inversement, au moment où un appareil lance une requête sur Internet et lorsqu'il reçoit la réponse.

_ L'adresse IP du serveur intranet à joindre sur le site principal

C'est l'adresse IP du serveur RDS, expliqué ci-dessous

➤ Sur un des hyperviseurs, je prépare une machine virtuelle dédiée au serveur RDS :

_ Je procède comme pour l'installation des rôles

_ Au moment du choix de type d'installation, je choisi « installation des services Bureau à distance »

_ Je choisi un « démarrage rapide » comme type de déploiement afin que tous les rôles soient installés sur le même serveur

_ Le scénario de déploiement est un « déploiement de bureaux basés sur une session »

Confirmer les sélections

Avant de commencer

Type d'installation

Type de déploiement

Scénario de déploiement

Sélection un serveur

Confirmation

Terminé

Pour terminer l'installation, les serveurs de destination doivent redémarrer.

Les services de rôle suivants seront installés sur le serveur nommé SRVRDS.bmi-local.local
Service Broker pour les connexions Bureau à distance
Accès Bureau à distance par le Web
Serveur hôte de session Bureau à distance

⚠ Le serveur va être redémarré après l'installation des services de rôle. Le groupe de sécurité Utilisateurs du domaine sera ajouté au groupe Utilisateurs du Bureau à distance sur le serveur.

Redémarrer automatiquement le serveur de destination si nécessaire

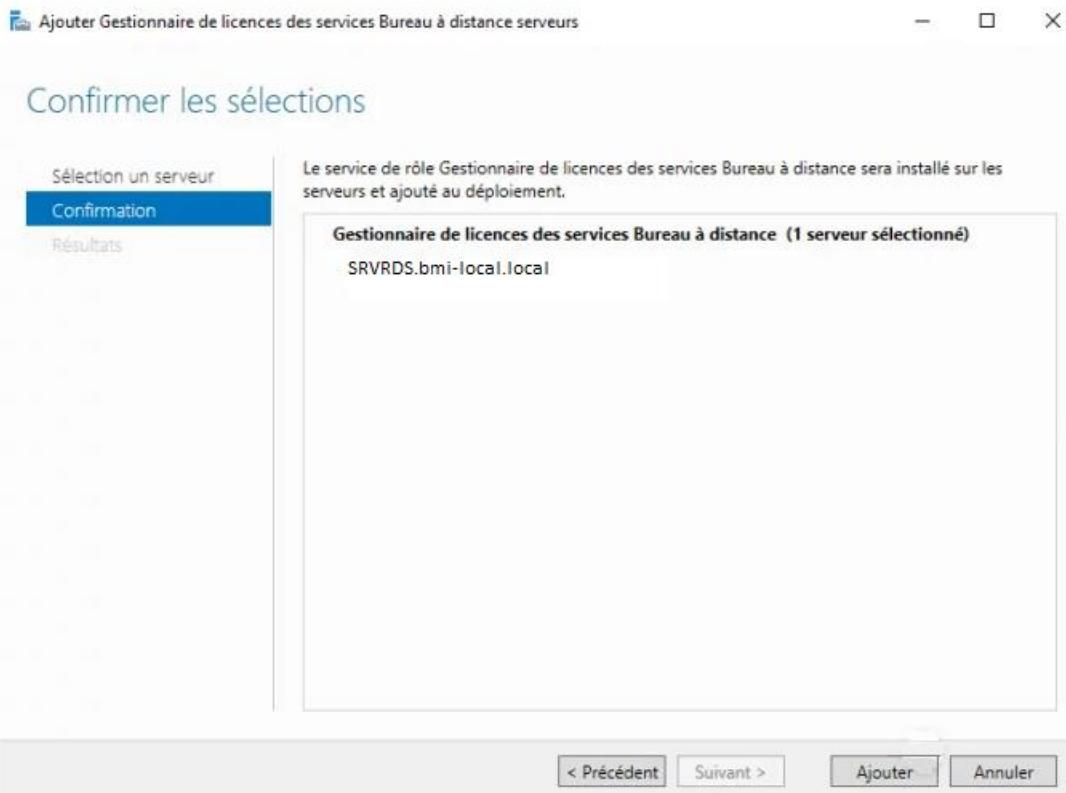
< Précédent

Suivant >

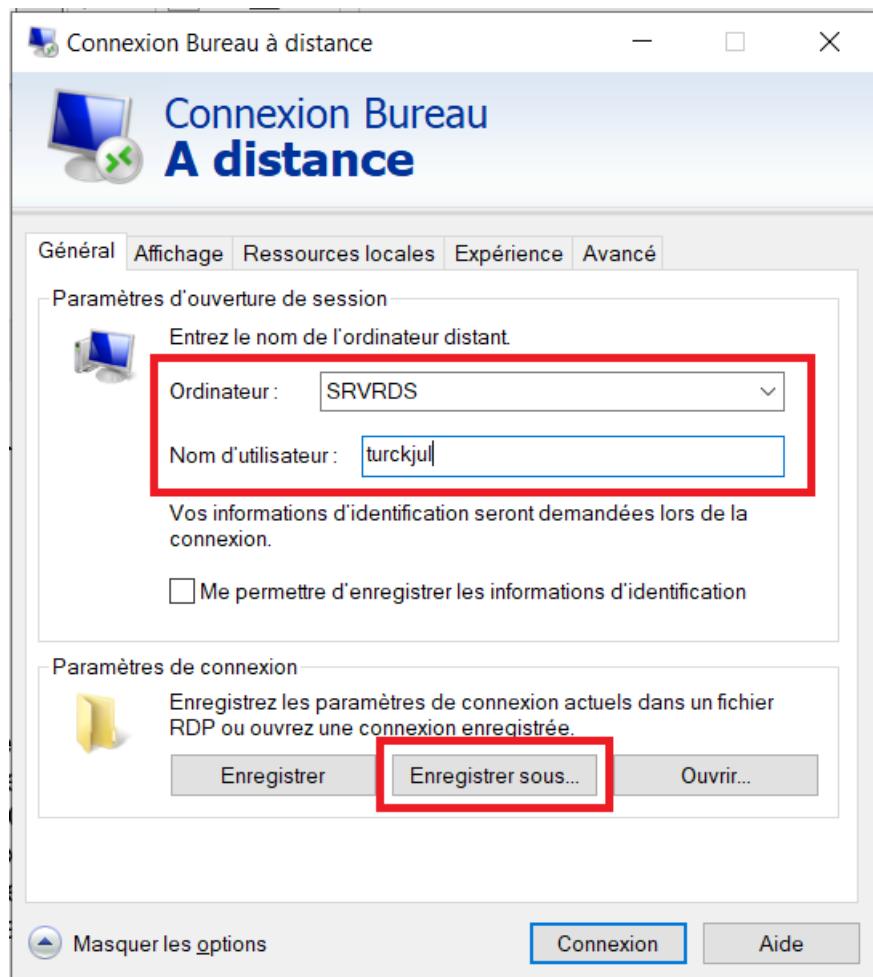
Déployer

Annuler

Une fois l'installation terminée, j'installe le gestionnaire de licences des services Bureau à distance. Je le fais à partir menu « Service Bureau à distance » du tableau de bord du gestionnaire de serveur.



- J'ajoute un raccourci de connexion de bureau à distance sur les bureaux de chaque PC professionnel :
 - _ Paramétré pour pointer directement sur ce serveur.
 - _ L'agent qui s'y connecte doit simplement renseigner ses identifiants de connexion d'Epinal
 - _ Pour se faire, je clique sur « connexion bureau à distance » qui se trouve dans le dossier « accessoires Windows » du menu démarrer.
Je clique sur plus d'options. J'entre l'adresse IP du serveur RDS à pointer. Je clique sur « enregistrer sous » et je choisi le bureau comme destination.



- Deux exceptions : La médiathèque de Golbey et la mairie d'Epinal sont connectés à la BMI d'Epinal par le biais d'une fibre :
 - Médiathèque de Golbey

_ S'explique par le fait que c'est la liaison « historique » et que la direction ne souhaitait pas la remettre en cause

_ Ne répond pas à la consigne de l'autonomisation des médiathèques du réseau vis-à-vis d'Epinal.

Pour y palier, une troisième prise RJ45, brassée sur le VLAN public, a été installée au niveau du poste professionnel. Ainsi, lors d'une panne à Epinal, il suffit au bibliothécaire de brancher le câble réseau de son PC dessus pour continuer à utiliser le SIGB, à partir de sa propre box.

Simplement, il ne peut plus utiliser sa platine RFID ni avoir accès aux fichiers partagés.

Cette solution n'est pas parfaite à la vue de la dégradation du service, le temps qu'Epinal redevienne opérationnel.

Toutefois, c'est pour moi le meilleur compromis qui pouvait être trouvé. En effet, relier Golbey comme les autres, aurait impliqué de réduire à néant l'investissement réalisé dans l'installation de la fibre à l'époque et engendré des frais non négligeables. Alors que le système fonctionne encore parfaitement.

➤ Mairie d'Epinal

_ Avoir accès à des applications hébergées par le SI de la mairie telles que la badgeuse de la ville. Pour la direction, avoir accès à certains dossiers du commun de la mairie.

_ Synchronisation de notre AD à leur serveur de messagerie. Ainsi, les boîtes mails professionnelles sont accessibles de la même manière que leur session SIGB. Cette modification de fonctionnement participe également à l'autonomisation des médiathèques

_ Envoie des sauvegardes sur le NAS qui nous est dédié dans leur baie et inversement.

Financièrement, il aurait été plus rentable de privilégier une connexion par le biais d'un VPN. En effet, les deux bâtiments sont déjà dotés d'un pare-feu qui le permet. Ça n'aurait couté que la prestation du paramétrage par le fournisseur.

Toutefois, l'envoi des sauvegardes par le biais d'une connexion Internet aurait été risqué : saturation de la bande passante durant plusieurs heures, risque d'une coupure Internet à tout moment. Aussi utiliser ce type de connexion, plus fiable, me semble nécessaire vis-à-vis de l'importance des données transitées et dans la mesure où les bâtiments sont géographiquement très proches.

Intégration des postes

Lors de la réception de nouveaux PC, je les configure afin qu'ils intègrent un des différents réseaux, en fonction de leur destination. Pour se faire, j'effectue deux paramétrages :

- L'intégration dans un domaine ou un groupe de travail :
 - L'intégration dans un domaine ne concerne que les ordinateurs professionnels et publics d'Epinal
En effet, seuls ces deux VLAN ont un serveur avec un rôle AD DS
 - Ceux concernés par les groupes de travail sont les PC publics d'Epinal et tous les ordinateurs des autres médiathèques
 - Je le réalise à partir du menu « système » des paramètres. Je clique ensuite sur le paramètre associé « renommer ce PC (avancé) que je trouve dans le sous-menu « à propos de ». Je clique ensuite sur « modifier » de la fenêtre « propriétés système ». Une ultime fenêtre s'ouvre me permettant de choisir l'option d'intégration ainsi que de renommer le PC afin de lui donner un nom qui suit la nomenclature choisie au départ (à savoir BMIxxx, xxx correspondant à un nombre à 3 chiffres qui rappelle son

ordre d'arrivé dans le parc et donc de retrouver avec quel lot il a été acheté si, par exemple, j'ai besoin de faire jouer la garantie).

- La configuration IP qui peut être soit dynamique, soit statique :

➤ La configuration dynamique :

_ Aussi appelée DHCP (Dynamic Host Configuration Protocol)

_ Fourni automatiquement les informations de configurations à la machine qui se connecte au réseau.

_ Je privilégie cette configuration pour les machines qui ne seront que cliente sur le réseau (c'est-à-dire qu'elles n'ont pas de service à offrir à une autre machine).

Ça va concerner les PC des utilisateurs, les appareils mobiles, les consoles de jeux vidéo

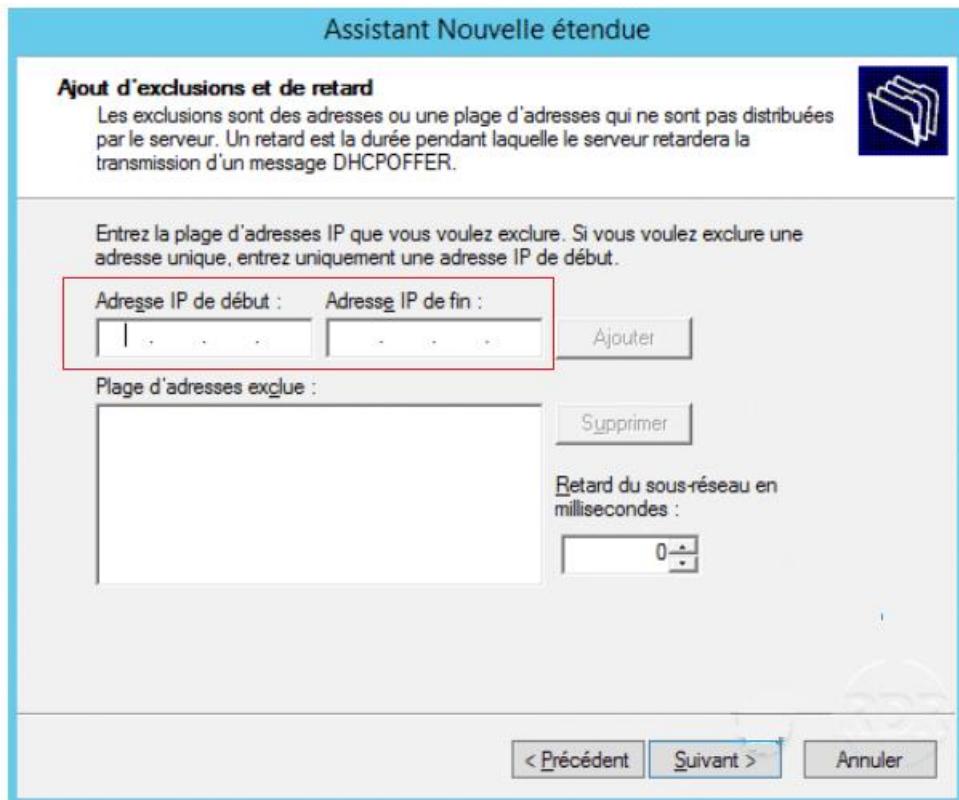
➤ La configuration statique :

_ Consiste à entrer les paramètres IP soi-même

_ Je privilégie cette configuration pour les machines qui ont un service à offrir (imprimantes, machines virtuelles qui font office de serveur, platines RFID)

_ Afin d'éviter qu'un serveur DHCP n'attribue une adresse que j'ai choisi pour un appareil en statique, j'exclue ces adresses de l'étendue DHCP.

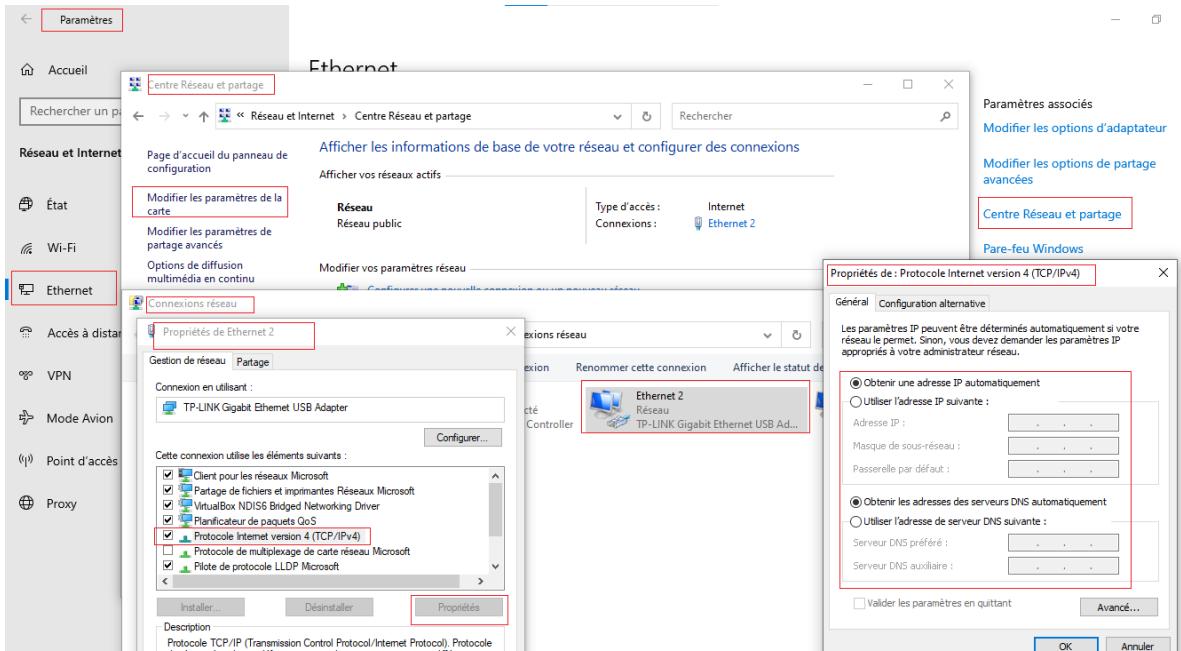
Pour se faire, j'ouvre le menu DHCP de la console d'administration du serveur. Je développe dans l'arborescence l'étendue à modifier et je fais un clic droit sur le pool d'adresses, puis je choisi le menu « Nouvelle plage d'exclusion ». Dans la nouvelle fenêtre, je renseigne les plages de début et de fin de l'étendue que je veux exclure du DHCP.



Les paramètres IP

Pour pouvoir affecter ses paramètres au PC, je fais un clic droit sur l'icône correspondant au réseau dans la barre de notifications. Je clique ensuite sur « ouvrir les paramètres réseau et Internet ». Je clique ensuite sur le menu « Ethenet » puis sur l'option « centre réseau et partage ». Dans la nouvelle fenêtre je clique sur « Modifier les paramètres de la carte ». Dans la fenêtre « connexions réseau », j'effectue un clic droit sur la carte réseau Ethernet puis sur « propriétés ». Dans la fenêtre « Propriétés », je clique sur « Protocole Internet version 4 (TCP/IP v4) » puis sur « Propriétés ». S'affiche alors la dernière fenêtre qui va me permettre d'affecter les paramètres IP.

Je vais alors soit cocher « choisir une adresse IP automatiquement si je veux un adressage dynamique, soit « utiliser l'adresse IP suivante » si je veux un adressage statique.



Ces paramètres sont au nombre de 5 :

- L'adresse IP (Internet protocol) :
 - Numéro unique au sein d'un réseau qui permet à chaque appareil de communiquer entre eux, sans se tromper « d'interlocuteur ».
Par exemple, c'est ce qui permet à un ordinateur d'envoyer l'ordre d'imprimer un fichier Word à l'imprimante souhaitée par l'utilisateur.
 - J'utilise des adresses au format IPv4. Il se constitue de 4 octets qui sont notés dans un format numérique allant de 0 à 255 séparés par un point (ex à la BMI : 172.27.9.15). C'est le format standard actuellement.
 - Le choix des plages d'adresses pour un réseau privé (c'est-à-dire qui n'est pas utilisable pour aller sur Internet) est régi par le RFC 1918 « Address Allocation for Private Internets ». Aussi elle impose des plages en fonction de la classe choisie.
 - Pour le réseau, j'utilise deux classes : La B pour Epinal, la C pour toutes les autres. Ainsi, les adresses d'Epinal commencent toutes par 172.27.x.x et dans les autres elles commencent toutes par 192.168.x.x

Je trouve le choix des classes pertinent car elles sont adaptées aux tailles des médiathèques, à leur capacité d'accueil et à la fragmentation logique des sous-réseaux.

En effet, pour définir la classe :

_ Je prévois le besoin du découpage en sous-réseau (VLAN). Aussi, seule Epinal est concerné par ce type de découpage qui oblige à ce que le 3^{ème} octet soit différent pour chaque.

_ Je défini un nombre théorique d'appareils pouvant fonctionner simultanément au maximum sur chaque VLAN et qui se compose du :

nombre d'équipements fixes déjà présent

nombre théorique d'équipements qui peut être ajouté, en me basant soit sur le nombre de prises RJ45 de libre, soit le nombre de ports disponibles sur les switches si celui-ci est inférieur

nombre d'appareils qui peuvent potentiellement se connecter en simultané sur le réseau en WIFI, en prenant en compte le nombre maximal de bibliothécaires et de visiteurs pouvant être présent en même temps dans un lieu. Pour ce faire, je me base sur les obligations légales des ERP (établissements recevant du public) qui préconise la présence d'une personne pour $2m^2$ d'espace circulable dans l'espace public. Aussi toutes les médiathèques sont des établissements de type S (Bibliothèques ou centres de documentations). Sauf qu'Epinal est la seul de catégorie 4 (permettant ainsi de recevoir jusqu'à 300 personnes, personnel compris) alors que les autres sont de catégorie 5, limitant la capacité d'accueil à 100 personnes, personnel non compris, maximum

De ce fait, aucun réseau ou sous-réseau, n'est donc amené à avoir plus de 255 adresses. Hormis le VLAN public qui est le seul qui s'étend sur 2 3^{ème} octet (172.27.11.x et 172.27.12.x)

- Masque de sous-réseau
 - C'est l'élément qui va permettre de définir la partie fixe des adresses IP de chaque machine sur un même réseau, voir sous-réseau de sa partie unique à chaque hôte.
Par exemple, à Epinal, 2 ordinateurs professionnels peuvent avoir les adresses 172.27.9.10 et 172.27.9.11 alors qu'un ordinateur public aura l'adresse 172.27.11.10.
On voit ici, que le réseau d'Epinal dans son ensemble sera entièrement adressé en 172.27.x.x. C'est rendu possible grâce au choix du masque 255.255.0.0. La différentiation entre les VLANs se fait grâce au 3^{ème} octet. Enfin, le dernier octet sert à différencier chacune des machines de chaque VLAN.
Pour les autres médiathèques qui sont de classe C, le masque est 255.255.255.0. Chacune à un troisième octet différent pour différencier les adresses (notamment lors du paramétrage des VPN des pares-feux). Par exemple, la bibliothèque de Deyvillers peut avoir la plage d'adresse 192.168.1.x, Thaon la plage 192.168.2.x ...
 - Il se note de deux manières : soit sous le même format qu'une adresse IP (par exemple 255.255.0.0) soit avec une **notation CIDR (Classless Inter Domain Routing)** qui se compose d'une adresse IP du réseau, suivie d'un /, puis d'un nombre représentant le nombre de bits disponibles pour l'attribution d'adresses. Pour mon exemple, avec la notation CIDR, une adresse du VLAN professionnel se note 172.27.9.x/16

Dans ce cas de figure, le choix du masque n'est pas optimal. En effet cette configuration permet en théorie d'avoir à sa disposition, $(256 \times 256) - 2 = 65534$ adresses IP

allant de 172.27.0.1 à 172.27.255.254. Certes ça donne une sacrée marge de manœuvre, mais c'est gâcher.

Un masque optimisé, pour moi, aurait été 255.255.248.0 ou 172.27.8.0/21 : Ça permet d'avoir (8 x 256) – 2 = 2048 adresses allant de 172.27.8.1 à 172.27.15.254. Ça laisse un peu de marge tout en étant plus raisonnable sur le nombre d'adresses de secours.

- Passerelle par défaut

C'est l'adresse IP de l'équipement qui est en charge de la fonction de routage. C'est-à-dire qui va faire transiter les paquets de données d'un hôte à un autre.

Dans mon cas, c'est l'adresse du pare-feu que je communique.

- Serveur DNS primaire

C'est l'adresse IP du serveur qui se charge de traduire les noms de domaines en adresses IP afin de nous connecter aux bons sites Internet.

Pour ma part, j'entre l'adresse du serveur DNS de chaque VLAN à Epinal.

- Serveur DNS secondaire

Serveur DNS de secours, au cas où le primaire ne serait plus disponible. Il n'est pas obligatoire de le renseigner.

Pour ma part, je ne le renseigne pas.

Le WI-FI

- WI-FI (WIreless FIdelity) est un protocole de communication IP sans fil. Par extension, c'est aussi devenu le nom de la connexion en elle-même.
- Régie par des normes du groupe IEEE 802.11 (Institute of Electrical and Electronics Engineers)
- Accessibles par le biais de bornes WIFI avec les caractéristiques :
 - Uniquement en DHCP, même pour les appareils appartenant aux médiathèques.
Ça me permet une plus grande souplesse dans la gestion des appareils qui peuvent être ainsi mis à la disposition d'autres médiathèques sans avoir à modifier les paramètres IP à chaque déplacement.
 - Alimentation PoE

PoE : Power of Ethernet. Elles sont alimentées par le câble réseau qui sert également à faire transiter les données.

- Émet sur la bande de fréquence 5GHz
- Aux normes 802.11ac aussi appelée WIFI 5

- Il n'est mis à disposition que pour offrir un WI-FI public gratuit, dans chacune des médiathèques.
- Aucune protection : Le SSID n'est pas caché et il n'y a pas de mot de passe. Toutefois, il se connecte à Internet par l'intermédiaire du Proxy Ucopia, dans chacune des médiathèques.

Ce manque de protection est une pratique courante dans les espaces publics. Je le trouve pertinent étant donné qu'il n'y transite aucune donnée sensible liée au service. Alors que ça permet une souplesse de connexion pour des personnes peu à l'aise avec l'outil informatique ou qui ne parlerait pas français par exemple.

- Une médiathèque ne propose pas de WIFI, celle de Deyvillers. Elle a la particularité d'être couplée à une crèche. Or la loi « abeille » interdit l'exposition aux ondes WI-FI des bâtiments accueillant des enfants de moins de 3 ans.

Loi « abeille » : Loi n°2015-136 du 9 février 2015 relative à la sobriété, à la transparence, à l'information et à la concertation en matière d'exposition aux ondes électromagnétiques. L'interdiction est stipulée dans l'article 7.

Dans un délai d'un an à compter de la promulgation de la présente loi, il est mis en place une politique de sensibilisation et d'information concernant l'usage responsable et raisonné des terminaux mobiles ainsi que les précautions d'utilisation des appareils utilisant des radiofréquences.

Versions ▾

> Article 7

I. - Dans les établissements mentionnés au chapitre IV du titre II du livre III de la deuxième partie du code de la santé publique, l'installation d'un équipement terminal fixe équipé d'un accès sans fil à internet est interdite dans les espaces dédiés à l'accueil, au repos et aux activités des enfants de moins de trois ans.

II. - Dans les classes des écoles primaires, les accès sans fil des équipements mentionnés à l'article 184 de la loi n° 2010-788 du 12 juillet 2010 portant engagement national pour l'environnement installés après la publication de la présente loi sont désactivés lorsqu'ils ne sont pas utilisés pour les activités numériques pédagogiques.

III. - Dans les écoles primaires, toute nouvelle installation d'un réseau radioélectrique fait l'objet d'une information préalable du conseil d'école.

Ainsi, toutes ces interconnexions permettent une meilleure communication entre les différents bâtiments ainsi qu'une mutualisation des ressources.

Pour mon quotidien, cela s'avère d'autant plus nécessaire que ça me permet une administration, où que je me trouve. Ainsi que de développer de nouveaux services qui peuvent être déployés dans l'intégralité des structures.

II. L'exploitation du SI

a) Son administration au quotidien

Durant l'activité n°1, j'ai présenté des outils qui me permettent d'administrer et surveiller les terminaux depuis mon poste de travail. J'ai également des outils adaptés pour me faciliter la gestion et la surveillance de l'ensemble du réseau.

Prise en main à distance

Un premier outil intéressant, est la prise de contrôle d'un appareil connecté à distance :

- Intérêts :

- Intervenir sur un poste sans avoir à se déplacer et ainsi :

- _ Gagner du temps sur des déplacements éviter dans les autres médiathèques du réseau

- _ Former à distance une personne sur une manipulation

- _ Economiser sur le carburant de la voiture de fonction et réduire ses émanations de CO2

- Intervenir sur un serveur sans aller dans la salle serveur ce qui permet de :

- _ Gagner du temps lorsque je ne suis pas à Epinal et économiser sur des déplacements évitables

- _ Ne pas avoir à brancher un écran, clavier, souris aux hyperviseurs. D'autant que le système de rack ne prévoit aucun espace pour aménager correctement des périphériques et avoir un poste ergonomique pour travailler.

- Outils :

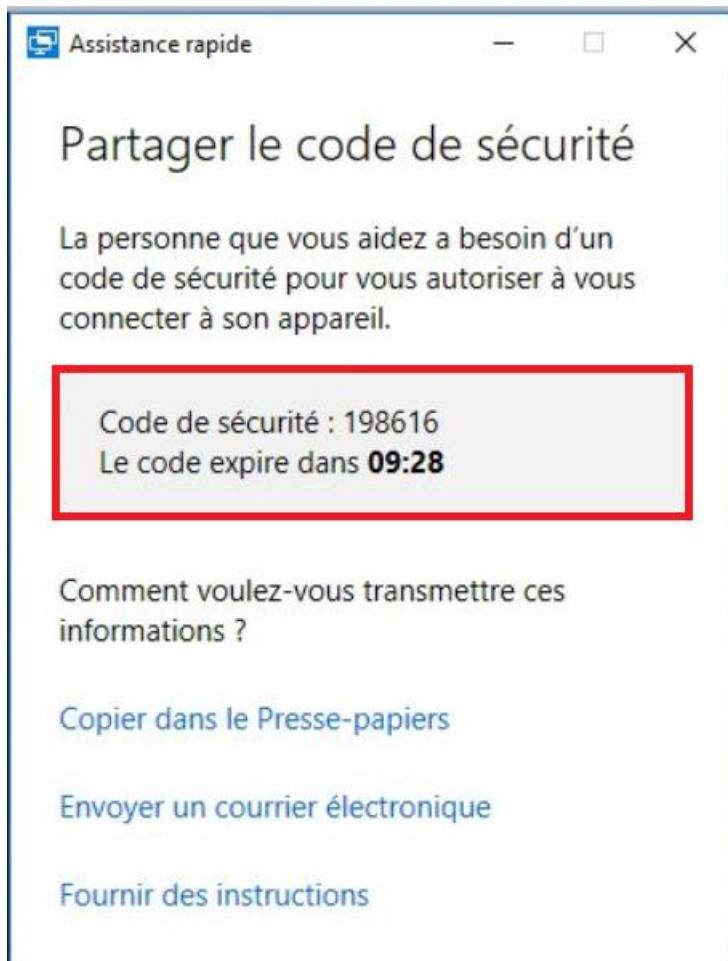
- Pour les PC, depuis l'apparition de l'OS Windows 10, Microsoft a intégré un outil nommé « assistance rapide » :

- _ Je l'utilise pour effectuer la mise à jour d'un logiciel qui requiert un mot de passe administrateur, effectuer et/ou expliquer une manipulation à un collègue ou essayer de déboguer un logiciel non critique

- _ Accessible depuis le menu démarrer, dans le dossier « accessoires Windows »

- _ Pour l'utiliser :

- _ En tant qu'aide, je dois me connecter avec un compte Microsoft que je me suis créé au préalable. Je reçois ensuite un code que je dois fournir à celui que je veux aider.



_ De son côté, la personne, que je guide par téléphone, ouvre le même outil et entre le code que je lui fournis. Enfin, il autorise le partage d'écran



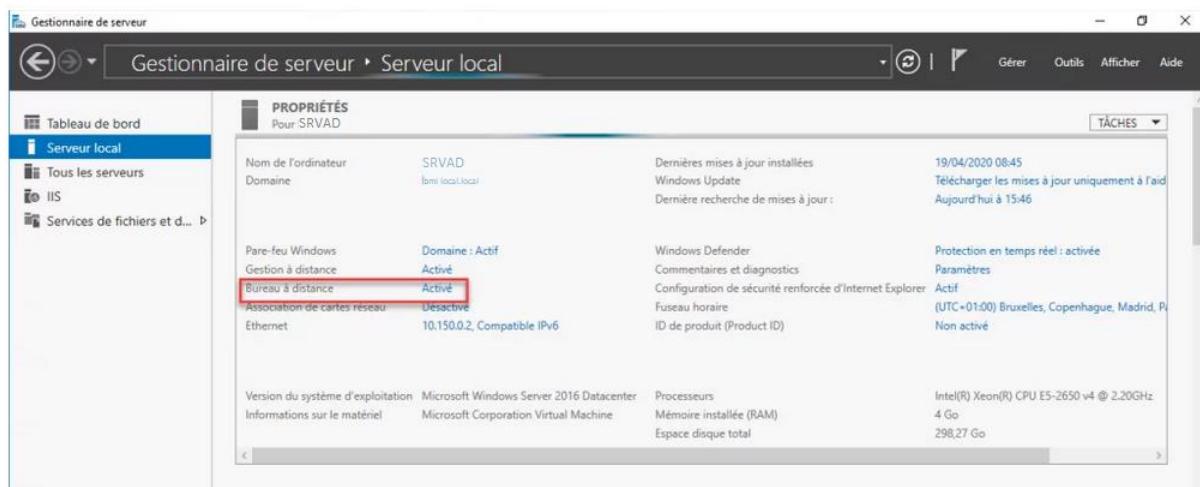
➤ Pour les serveurs, je dois activer le bureau à distance :

_ Manipulation que je réalise au moment de la préparation des machines virtuelles expliquée dans la première sous-partie de cette activité

_ Me permet d'administrer les serveurs, visualiser leurs journaux d'activités ou utiliser un de leurs outils

_ Pour se faire, j'ouvre le gestionnaire de serveur puis je vais dans le menu « Serveur Local ». Dans la fenêtre « propriétés », je clique sur « désactiver » qui se trouve à côté de « bureau à distance ». S'ouvre ensuite une boîte de dialogue dans laquelle je vais « autoriser les connexions à distance à cet ordinateur », puis je coche l'option « n'autoriser que la connexion des ordinateurs exécutant le Bureau à distance avec authentification NLA ».

NLA (Network Level Authentication) : fonctionnalité qui oblige un utilisateur à s'authentifier avec un identifiant connu dans l'AD, pour pouvoir ouvrir une session à distance sur le serveur.

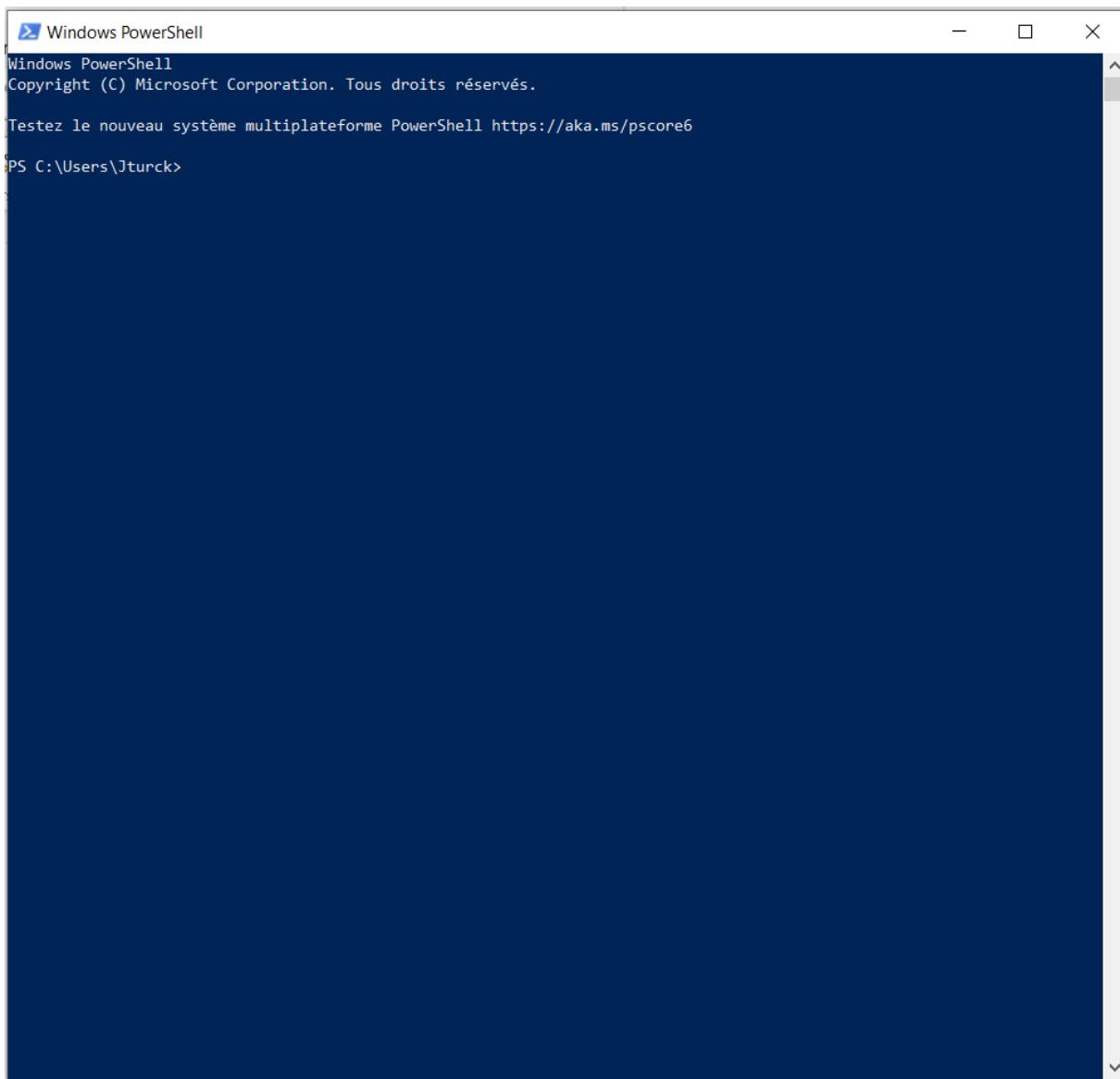


_ Je peux maintenant accéder à tous les serveurs Windows depuis n'importe quel poste en utilisant l'outil « connexion bureau à distance », de la même manière que pour accéder au serveur RDS depuis un site distant (voir deuxième sous-partie de cette activité »).

Powershell

- Powershell est un ensemble d'outils permettant de taper des commandes et écrire des scripts afin d'automatiser des tâches courantes sur les serveurs.
 - Inconvénients :
 - Demande de bonnes connaissances dans ce langage. Ne serait-ce pour comprendre un script déjà tout fait sur Internet et l'adapter à sa situation.
 - On perd parfois plus de temps à écrire le script plutôt que réaliser la manipulation soi-même.
- Aussi, cet outil est à réserver à des tâches très redondantes. C'est-à-dire des tâches que l'on va réaliser très souvent

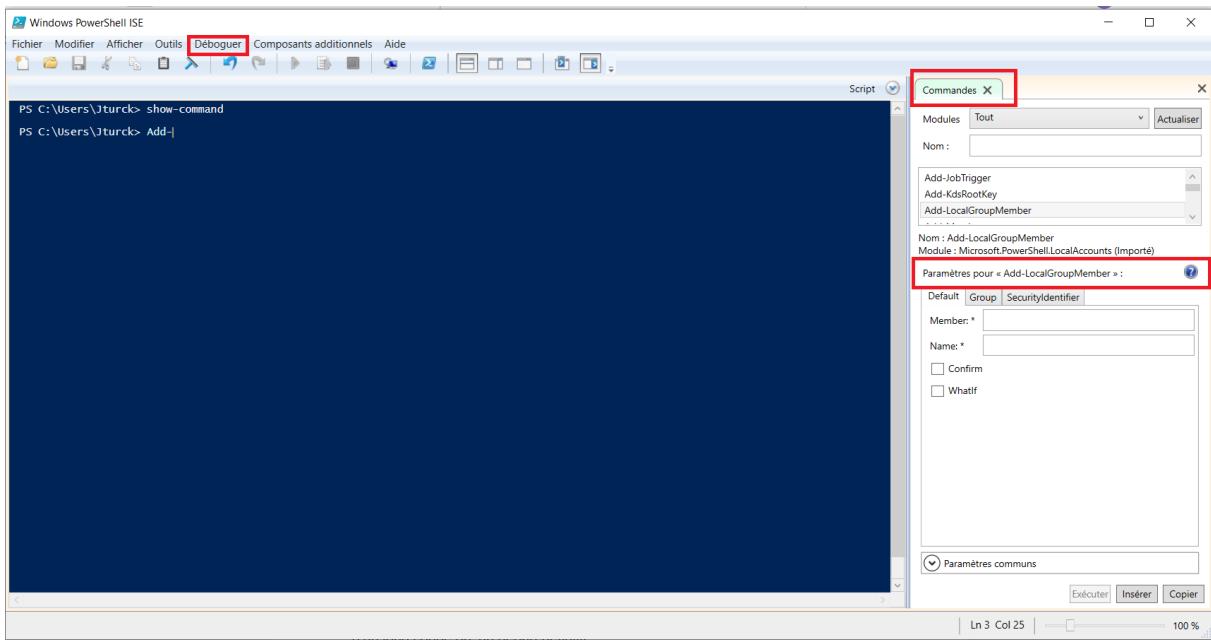
- Lors des premières exécutions d'un script, il est indispensable de vérifier les résultats obtenus
- Outils :
 - Les deux sont accessibles depuis le dossier Windows PowerShell du menu démarrer
 - Windows Powershell
- _ Console d'interprétation de lignes de commande
- _ A n'utiliser que lorsque l'on maîtrise le langage



A screenshot of a Windows PowerShell window. The title bar says "Windows PowerShell". The content area shows the following text:
Windows PowerShell
Copyright (C) Microsoft Corporation. Tous droits réservés.
Testez le nouveau système multiplateforme PowerShell <https://aka.ms/pscore6>
PS C:\Users\Jturck>

- Windows Powershell ISE
- _ **ISE (Integrated Scripting Environment)**:
- _ Propose : _ Une interface graphique
 - _ Des commandes préremplies
 - _ Une aide résume les paramètres pour chacune
 - _ Un débogueur

_ L'auto-complétions



_ Permet de prendre en main le powershell plus facilement et de mieux comprendre les rouages.

- Exemple d'utilisation dans mon quotidien : Création d'un nouvel utilisateur dans l'AD
 - Utile de l'automatiser car il y a beaucoup de mouvements. Ces mouvements sont dû :

_ A l'accueil de nombreux stagiaires tout au long de l'année dans différents domaines

_ A L'emploi de vacataires étudiants les weekends et durant les vacances scolaires. Toutefois, ces vacations ne sont pas stables.

_ Au mouvements de personnels à la suite de la création d'emplois, remplacement d'un long congé ou 'un départ définitif

- Les objectifs du script :

_ Créer un profil dont les seules variables seront le nom, prénom et l'UO d'affectation.

_ Création automatique du nom d'utilisateur à partir de la concaténation des 5 premières lettres du nom et des 3 premières lettres du prénom

Concaténation : En programmation, ça consiste à mettre bout à bout des chaînes de caractères

_ Création automatique d'un mot de passe, provisoire et unique à tous

_ Ajout de l'obligation à leur première connexion de modifier le mot de passe par un personnel

- Exemple de script :

```
$nom = Read-Host "Entrez le prénom et le nom de l'utilisateur" #une fenêtre apparaît et demande le nom et le prénom de l'utilisateur à créer
```

```
$uO = (Get-ADOrganizationalUnit -Filter *).DistinguishedName | Out-GridView -Title "Choisissez une UO pour cet utilisateur" -PassThru #permettra d'insérer l'utilisateur directement dans le bon UO
```

```
$prenom = $nom.Substring(0,2) #récupération des 3 premières lettres du prénom
```

```
$nomFamille = $nom.Substring(0,4) [1] #récupération du nom
```

```
$nomUtilisateur = $nomFamille+$prenom #création du login à partir de prénom et du nom
```

```
$nomUtilisateur = $nomUtilisateur.ToLower() #mettre en minuscule le login
```

```
$motDePasse = "m0tDeP@sse" #crée le mot de passe générique pour la première connexion
```

```
Try { #Si aucune erreur, crée le compte en renseignant le nom, le prénom, le login et l'UO
```

```
    New-ADUser -Name $nom
```

```
        -SamAccountName $nomUtilisateur
```

```
        -Path $uO
```

```
        -UserPrincipalName $nomUtilisateur@bmi-local.local
```

```
        -AccountPassword (ConvertTo-SecureString -AsPlainText
```

```
        $motDePasse -Force #force le mot de passe générique
```

```
        -Enabled $true #active le compte dès la création
```

```
        -ChangePasswordAtLogon $true #force l'utilisateur à modifier son mot de passe à la première connexion
```

```
    Write-Host "L'utilisateur $nom a été créé dans l'AD" #message précisant que tout s'est bien passé
```

```
}
```

```
Catch {
```

```
    Write-Host "Une erreur est survenue lors de la création de $nom" #message précisant qu'une erreur est survenue au moment de la création du compte
```

```
}
```

OS Zabbix

- C'est un logiciel de supervision et de monitoring qui permet de surveiller en temps réel les infrastructures du réseau.
- L'intérêt de la supervision
 - Anticiper des problèmes grâce au suivi en continu
 - Agir rapidement en cas de problème grâce au monitoring
 - Avoir des statistiques à froid et repérer les dysfonctionnements

Logiciel monitoring, car il est capable de m'avertir en temps réel d'un problème. Par email dans mon cas

Lors de la création de mon profil, je renseigne mon adresse e-mail. Pour se faire, dans l'onglet média, je précise le type « email », l'adresse à laquelle envoyer, les jours et horaires ainsi que les niveaux de criticités des alertes pour lesquels je veux être informé.

The screenshot shows a configuration form for a monitoring rule. The 'Type' is set to 'Email'. The 'Envoyer' field contains the email address 'turckjul@bmi.agglo-epinal.fr'. Below it, there are two 'Supprimer' buttons. An 'Ajouter' button is visible above a section for active times. The 'Lorsque actif' field contains the time range '1-7,00:00-23:59'. A large red box highlights the 'Utiliser si sévérité' section, which includes checkboxes for 'Non classé', 'Information', 'Avertissement', 'Moyen', 'Haut' (which is checked), and 'Désastre' (which is checked). The 'Activé' checkbox is also checked. At the bottom right are 'Ajouter' and 'Annuler' buttons.

- Il me permet de contrôler :
 - Tous les appareils que je juge d'importance critiques, car leur panne entraîne une dégradation du service :

- _ Hyperviseurs
- _ Serveurs (même en tant que machines virtuelles)
- _ Pares-feux
- _ Proxy
- _ Switches
- _ Platines RFID

Je fais le choix de ne pas surveiller les ordinateurs avec Zabbix, car j'ai déjà des outils de supervisions pour ces terminaux (voir activité 1). De plus, un ordinateur qui tombe en panne peut être très vite remplacé.

Le logiciel est capable de reconnaître tous les équipements présents sur le réseau. Toutefois, il faut lui signaler **les hôtes, c'est-à-dire ceux que l'on veut surveiller**.

Pour se faire, dans le sous menu « hôtes » du menu « configuration » je clique sur le bouton « créer un hôte ». Je renseigne le nom avec lequel je veux qu'il apparaisse (je garde son nom d'origine sur le réseau), son groupe (c'est-à-dire son type de matériel),

son adresse IP, adresse DNS et je renseigne la manière dont je veux qu'ils soient surveillés.

➤ Les composants qui me semblent les plus importants ainsi que leurs états

_ Ce sont des items accessibles en fonction du groupe que l'on a renseigné lors de la création de l'hôte

_ Je dois là encore, renseigner les éléments que je veux surveiller. Pour se faire, dans le même sous menu que précédemment, je clique sur « élément » puis « créer un élément ». Je renseigne, entre autres, un nom, une clé qui correspond au type d'information et le format de l'information. Je peux également renseigner le temps que je veux conserver l'information.

The screenshot shows the Zabbix configuration interface for creating a new item. The top navigation bar includes links for Surveillance, Inventaires, Reports, Configuration, Administration, and a search bar. The main menu on the left lists Groupe d'hôtes, Modèles, Hôtes, Maintenance, Actions, Ecrans, Diaporamas, Cartes, Découverte, and Services. The current path in the breadcrumb navigation is: Historique > Configuration des règles de découverte > Configuration des services > Configuration des groupes d'hôtes > Configuration des hôtes > Configuration des éléments.

The configuration page for 'Éléments' (Items) is displayed. A template named 'Template App:HTTP Service' is selected. The item details include:

- Nom:** HTTP service is running
- Type:** Vérification simple
- Codé:** net.tcp.service[http]
- Interface hôte:** 172.16.152.136 : 10090
- Nom d'utilisateur:** (empty)
- Mot de passe:** (empty)
- Type d'information:** Numérique (non signé)
- Type de donnée:** Decimal
- Unités:** (empty)
- Utiliser un multiplicateur personnalisé:** 1
- Intervalle d'actualisation (en sec):** 60
- Intervales flexibles:** Pas d'intervalle flexible défini.
- Nouvel Intervalle flexible:** Intervalle (en sec): 30, Période: 1-7:00:00-24:00, Ajouter
- Période de stockage de l'historique (en jours):** 365
- Trend storage period (in days):** 365
- Stocker valeur:** Tel quel
- Afficher valeur:** Service state
- Nouvelle application:** Applications -Autun-CPU, Filesystems, General, HTTP service, Memory
- REMPLIR le champ d'inventaire d'hôte:** -Autun-
- Description:** (empty)
- Actif:** checked

At the bottom, there are buttons for Sauver (Save), Clone, Effacer l'historique et les tendances (Delete history and trends), and Annuler (Cancel). A footer note states: Zabbix 2.2.9 Copyright 2001-2015 Zabbix SIA. A status message indicates: Connecté en tant que "Admin".

_ Les principaux items que je surveille :

_ Les disques durs : Où en est leurs taux de remplissage. En effet, un disque dur saturé ralenti la machine et n'accepte plus de nouvelles données.

_ Les CPU (Central Processing unit) ou processeurs : Où en est leur charge de travail. Une fois les 100% atteint, la machine ralentie fortement et fini par planter.

_ La RAM (Random Access Memory) ou mémoire : Pareil que pour le CPU

_ La bande passante, c'est à dire la quantité maximale de données pouvant transiter en même temps sur un laps de temps : Où en est-on dans son taux d'utilisation. Si son taux est à 100 %, les données mettront plus de temps pour transiter. Ça risque de ralentir fortement le service au public.

_ Les cartes réseaux : Les machines sont-elles joignables ? C'est-à-dire, sont-elles bien allumées et connectées ?

Il existe bien d'autres items tout aussi pertinent à surveiller. Toutefois, si on devait tout surveiller, on serait submergé d'informations et on risquerait de saturer le réseau. Il a donc fallu faire des choix.

Aussi, je trouve ces choix pertinents car ils ont été faits par rapport à de précédents incidents susceptibles de ressurgir.

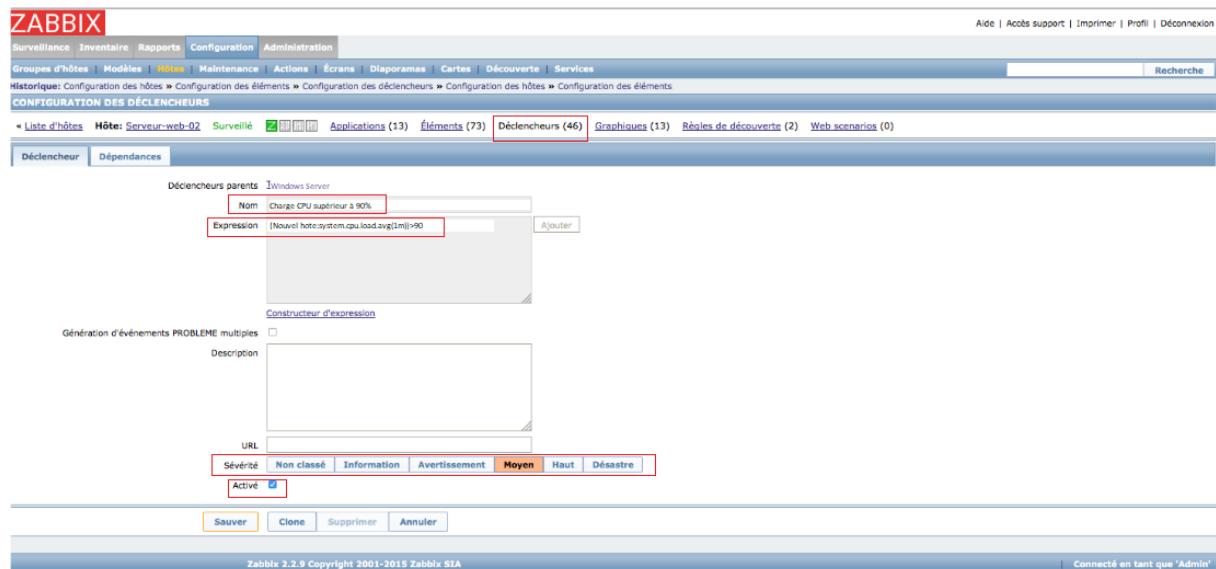
- Contrôler que les états n'atteignent pas un seuil critique

_ Je défini les seuils en créant des déclencheurs

— Pour créer un déclencheur, toujours dans le menu principal des hôtes, je clique sur déclencheurs puis sur le bouton « créer un déclencheur ». Je lui renseigne un nom, l'expression qui correspond à l'alerte souhaitée ainsi qu'un degré de严重性.

Par exemple, pour déclencher une alerte sur la charge de travail du CPU, je tape {Nouvel hôte:system.cpu.load.avg(1m)}>90

90 correspond à la valeur moyenne de la charge de travail du CPU et 1m (minute) correspond au temps maximum auquel est autorisé le CPU à atteindre cette charge.



— Les seuils que je privilégie sont :

— 90 % pour les charges de travail des CPU et des RAM. Ça me laisse une petite marge pour intervenir en stoppant un processus trop gourmand par exemple.

— 90 % pour le taux de remplissage d'un espace de stockage. Là encore, ça me laisse une marge pour le réduire en faisant du ménage.

— 90 % pour le taux d'utilisation de la bande passante. Ça me laisse le temps de repérer quelles activités sur le réseau sont trop gourmandes.

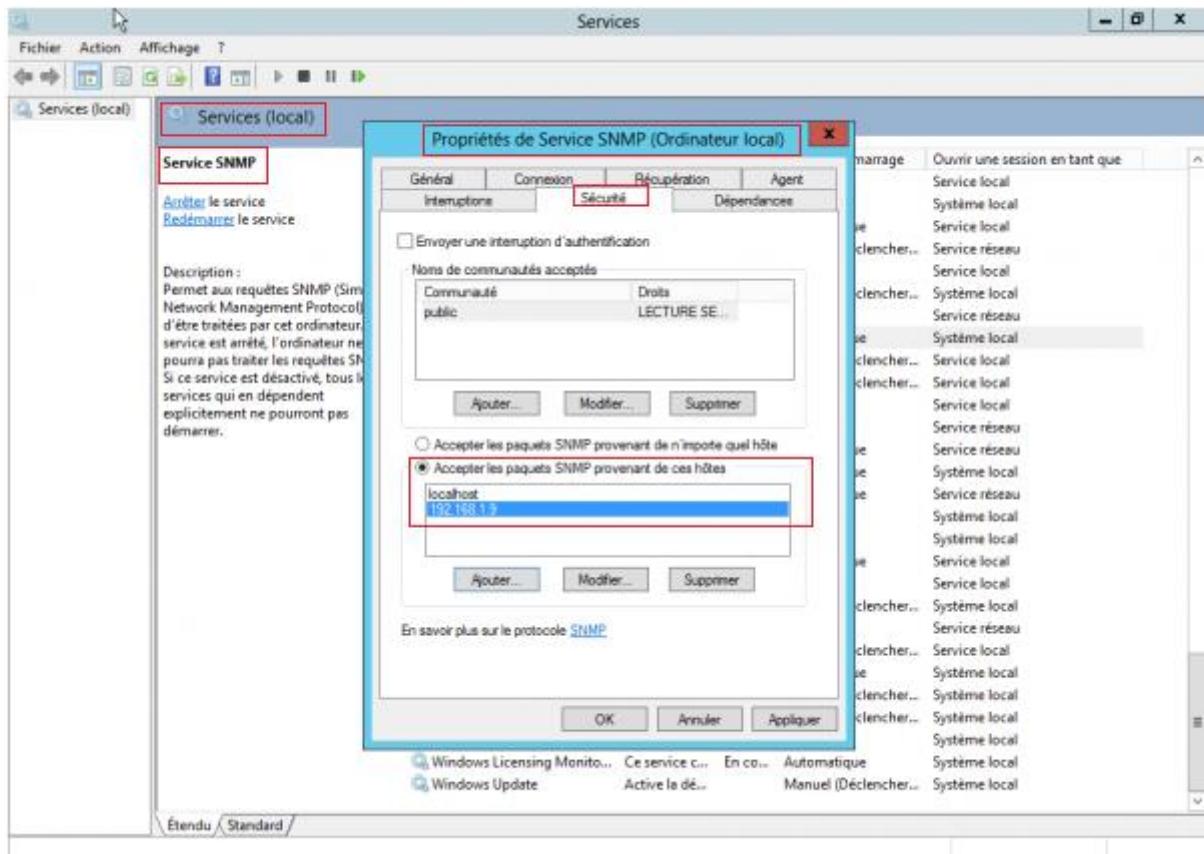
— Pour les déclencheurs liés aux pertes de connexions des hôtes, c'est simplement savoir s'il répond au ping ou non.

- Utilise le protocole SNMP
 - SNMP (Simple Network Manager Protocol) est un protocole réseau qui permet d'interroger tout équipement relié au réseau et compatible avec ce protocole.
 - Il est à activé sur chaque hôte
 - Exemple sur un serveur Windows 2016

Pour l'activer, je me rends dans le « gestionnaire de serveur » puis je clique sur « ajouter des rôles et des fonctionnalités ». Dans le sous-menu je sélectionne « service SNMP ».

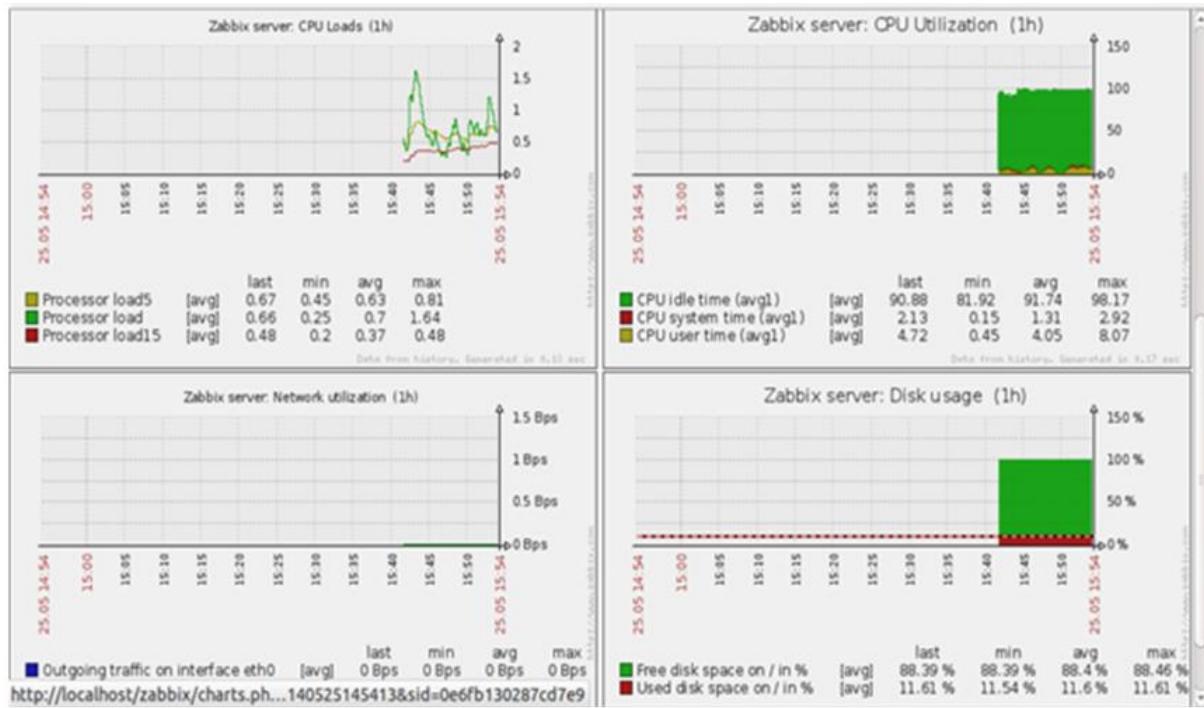
Une fois la fonctionnalité installée, je vais dans le sous-menu « services » du menu « outils ». Puis je fais un clic droit sur le service SNMP pour accéder à ses propriétés.

Dans la boîte de dialogue, je me rends sur l'onglet « agent » pour autoriser tous les services (physiques, applications, liaisons de données, Internet et bout en bout). Enfin dans l'onglet sécurité, je vais préciser que je n'autorise que les paquets SNMP du serveur Zabbix en précisant son adresse IP.



- Il propose des graphes résumant les activités des derniers jours
 - Ça me permet de pointer les problèmes les plus récurrents et de proposer des solutions pour y remédier avant que ça n'empire
 - Exemples de problèmes liés à mes alertes :
 - _ Les charges de travail des CPU ou des RAM des VM sont trop souvent au-dessus du seuil. J'ai donc alloué plus de ressources à ces machines.
 - _ Les espaces de stockages atteignent trop souvent le seuil, malgré les tris réalisés. Certains dossiers sont trop volumineux, surtout ceux du service patrimoine qui héberge des numérisations de documents anciens de très haute qualité. Je leur ai donc acheté des disques durs externes de plusieurs Terra octets afin de soulager le serveur de fichiers.
 - _ La bande passante disponible atteint son taux maximum de données à faire transiter. Aussi, le personnel a du mal de joindre le SIGB et les platines mettent beaucoup de temps à enregistrer les prêts et retours des documents. Grâce au logiciel de supervision du pare-feu (voir plus bas), je repère quels ordinateurs en consomme le plus et je stoppe leurs activités si elles sont non essentielles au service.

Une platine RFID se déconnecte très régulièrement tous les jours. Le graphique m'a permis de prouver un dysfonctionnement auprès du prestataire. J'ai fait jouer la garantie afin de la faire remplacer.



Ce logiciel est donc très important mais il ne me permet pas d'intervenir à temps si un problème survient durant mon absence (en soirée par exemple). Ni d'identifier précisément la cause d'un arrêt brutal d'une machine. Aussi, lorsqu'un incident s'est produit, il est tout de même important de retrouver une trace des événements qui y ont conduits.

La journalisation

Pour se faire, il existe pour chaque machine une journalisation des événements.

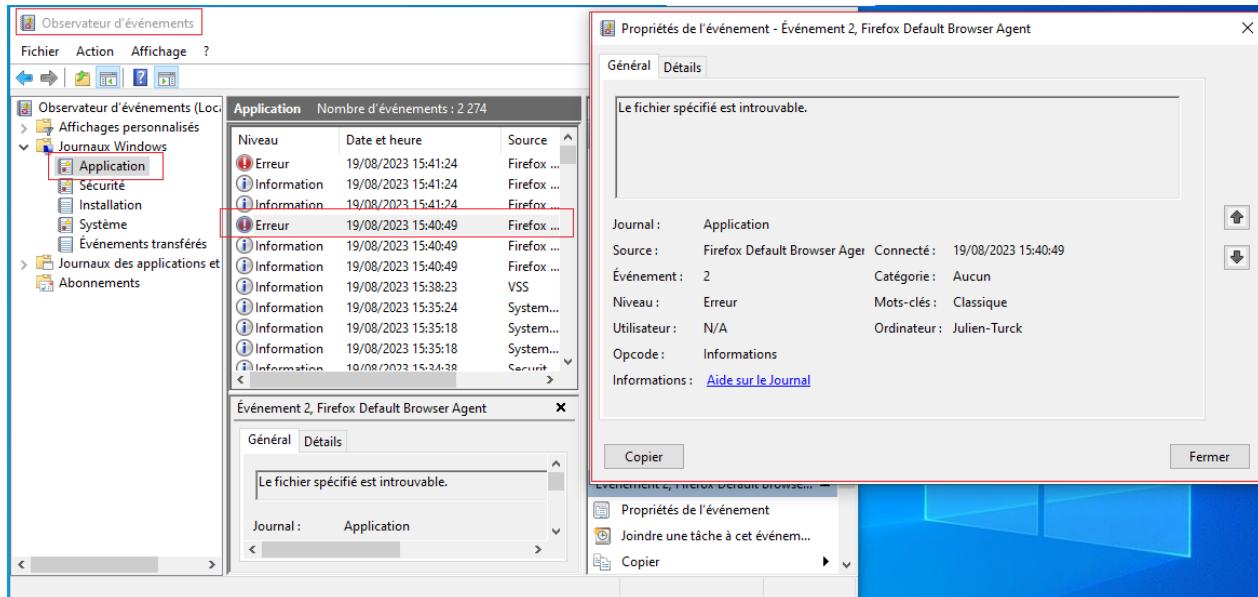
- Appareils sous OS Windows
 - J'utilise l'outil intégré qui se nomme « observateur d'évènements », auquel j'accède en tapant son nom dans la barre de recherche et cliquant dessus.
 - Il répertorie chaque évènement dans des journaux thématiques.
 - Ces journaux sont :

Le journal de sécurité, qui contient les évènements liés à la sécurité tels que l'ouverture d'une session ou l'utilisation d'une ressource ;

Le journal d'applications qui répertorie les évènements repérés par les applications et les programmes ;

Le journal système qui enregistre les évènements liés aux composants du système d'exploitation.

_ Pour y accéder, je clique sur le journal qui m'intéresse puis sur l'événement qui m'intéresse pour avoir plus de détails.



➤ Inconvénient :

_ Les journaux ne sont accessibles que si la machine est en état de redémarrer normalement

_ Exemples de cas de figure qui ne permettent pas d'y accéder :

- _ Échec lors du chargement de l'OS
- _ Panne du disque dur

Une bonne pratique pour éviter ces désagréments serait de centraliser les journaux, par le biais d'un outil comme ELK (ElasticSearch, Logstash et Kibana). Je pense toutefois, que la taille du réseau, ainsi que la fréquence des pannes ne justifie ce déploiement qui a un coût. De plus, il nécessite d'autres aménagements comme une synchronisation des horaires via un serveur NTP (Network Time Protocol).

- Les autres appareils

- Ça concerne notamment les pare-feux et le proxy
- Dans le cadre de leurs contrats de maintenance, les incidents sont pris en charge par le prestataire. Aussi, je me contente simplement de leur signaler les incidents. Je n'ai donc pas à gérer leurs journaux.

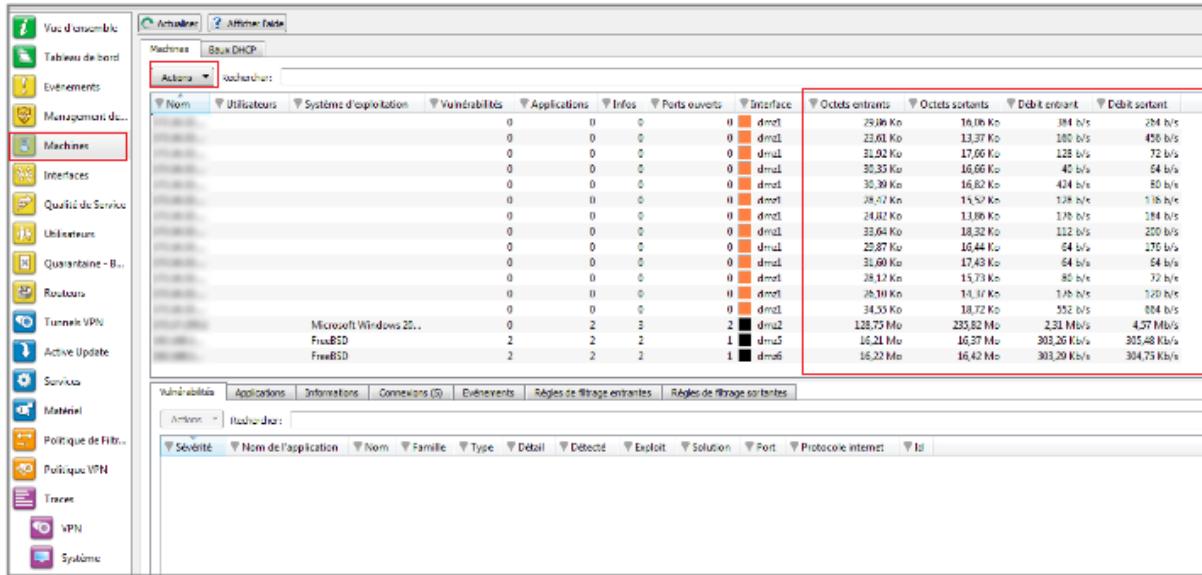
Stormshield Network Real-Time Monitor

Toutefois, j'utilise un logiciel de visualisation des activités du pare-feu. Il me permet :

- Visualiser les activités de chacune des machines sur le réseau
 - Je l'utilise notamment lorsque ma bande passante disponible arrive à saturation

- Pour y accéder, je clique sur le menu « machines »
- Ça me permet de vérifier si un ordinateur n'a pas une activité qui en consomme de trop à lui tout seul. Je peux ensuite vérifier l'activité auprès de l'utilisateur ou mettre en quarantaine l'ordinateur afin de stopper une activité non essentielle au service, le temps que l'activité sur le réseau diminue.

Pour mettre en quarantaine un ordinateur, je clique sur la ligne correspondant à la machine. Ensuite sur le bouton « actions » puis la commande « mettre en quarantaine ».



Nom	Utilisateurs	Systèmes d'exploitation	Vulnérabilités	Applications	Infos	Ports ouverts	Interface	Octets entrants	Octets sortants	Débit entrant	Débit sortant
dmz1	0	0	0	0	0	0	dmz1	29,16 Ko	16,06 Ko	384 b/s	284 b/s
dmz2	0	0	0	0	0	0	dmz2	23,61 Ko	13,37 Ko	180 b/s	450 b/s
dmz3	0	0	0	0	0	0	dmz3	21,92 Ko	17,05 Ko	128 b/s	72 b/s
dmz4	0	0	0	0	0	0	dmz4	30,33 Ko	16,06 Ko	40 b/s	64 b/s
dmz5	0	0	0	0	0	0	dmz5	30,39 Ko	16,62 Ko	424 b/s	80 b/s
dmz6	0	0	0	0	0	0	dmz6	28,47 Ko	14,57 Ko	128 b/s	116 b/s
dmz7	0	0	0	0	0	0	dmz7	24,02 Ko	13,08 Ko	176 b/s	114 b/s
dmz8	0	0	0	0	0	0	dmz8	33,04 Ko	18,32 Ko	112 b/s	200 b/s
dmz9	0	0	0	0	0	0	dmz9	22,87 Ko	16,44 Ko	64 b/s	170 b/s
dmz10	0	0	0	0	0	0	dmz10	31,60 Ko	17,43 Ko	64 b/s	64 b/s
dmz11	0	0	0	0	0	0	dmz11	28,17 Ko	15,73 Ko	80 b/s	72 b/s
dmz12	0	0	0	0	0	0	dmz12	26,10 Ko	14,17 Ko	128 b/s	120 b/s
dmz13	0	0	0	0	0	0	dmz13	34,55 Ko	18,72 Ko	552 b/s	884 b/s
dmz14	0	2	3	2	2	2	dmz14	128,75 Mo	233,82 Mo	2,31 Mo/s	4,57 Mo/s
dmz15	2	2	2	1	1	1	dmz15	16,21 Mo	16,37 Mo	303,26 Kb/s	305,48 Kb/s
dmz16	2	2	2	1	1	1	dmz16	16,22 Mo	16,42 Mo	303,29 Kb/s	304,75 Kb/s

- Vérifier que les tunnels VPN soient bien établis
 - Je les vérifie lorsqu'un bibliothécaire d'un autre établissement me signale ne plus avoir accès aux dossiers partagés
 - Pour se faire j'ouvre le sous menu « VPN » du menu « traces ». Les VPN entre établissements seront résumés dans l'onglet « Tunnels VPN IPSec ».

Source	Octets	Destination	Etat	Durée de vie	Authentification	Chiffrement
	6,47 Ko	9,00 Ko gw	mature	5sec	hmac-sha1	aes-cbc
	72,85 Ko	207,39 Ko gw	mature	3m 2sec	hmac-sha1	aes-cbc
	87,30 Ko	195,83 Ko gw	mature	7m 16sec	hmac-sha1	aes-cbc
	85,79 Ko	57,06 Ko gw	mature	13m 51sec	hmac-sha1	aes-cbc
	7,14 Ko	9,52 Ko gw	mature	21m 42sec	hmac-sha1	aes-cbc
	39,48 Ko	21,73 Ko gw	mature	22m 11sec	hmac-sha1	aes-cbc
0	0	0 gw	mature	1m 48sec	hmac-sha1	aes-cbc
	76,67 Ko	77,07 Ko gw	dying	49m 49sec	hmac-sha1	aes-cbc
	6,49 Ko	3,73 Ko gw	mature	9m 21sec	hmac-sha1	aes-cbc
	76,83 Ko	71,51 Ko gw	dying	57m 22sec	hmac-sha1	aes-cbc
	100,17 Ko	137,75 Ko gw	mature	10m 17sec	hmac-sha1	aes-cbc
	422,47 Ko	306,63 Ko gw	dying	58m 18sec	hmac-sha1	aes-cbc
	37,52 Ko	61,92 Ko gw	mature	18m 53sec	hmac-sha1	aes-cbc
	43,69 Ko	31,54 Ko gw	mature	19m 8sec	hmac-sha1	aes-cbc
	227,46 Ko	149,94 Ko gw	mature	19m 21sec	hmac-sha1	aes-cbc

- Je vais tout d'abord vérifier que les boxs Internet d'Epinal et de l'autre médiathèque sont opérationnelles. Si ça ne vient pas de là, j'ouvre un ticket de demande d'intervention auprès du prestataire.

Tous ces outils me permettent de prévenir d'éventuels arrêt de service, Comme pour la maintenance des terminaux, nous sommes ici dans la partie préventive de l'administration. Toutefois, cela n'empêche pas certaines pannes de survenir. A cela, il faut donc ajouter tout un panel d'outils et de méthodes afin d'assurer la partie curative de la maintenance du réseau.

L'invite de commandes

- Logiciel d'interprétation des commandes MS-DOS (Microsoft Disk Operating System)
- Pour y accéder, il suffit de taper « cmd » dans la barre de recherche et de cliquer sur « invite de commandes »

- Les commandes me permettent notamment d'obtenir des informations permettant de comprendre une situation anormale, obtenir des informations sur le PC ou encore donner des ordres au PC. Quelques exemples que j'utilise régulièrement :

Commandes	Résultat
ipconfig/all	Affiche notamment tous les paramètres de configuration IP de la machine. Elle me permet également de connaître l'adresse MAC de la carte réseau. Adresse MAC (Media Access Control) : adresse unique de chaque carte réseau attribuée par son constructeur. Elle ne peut pas varier au contraire d'une adresse IP.
Gpupdate /force	Force l'application des GPO
Ping xxx.xxx.xxx.xxx	Vérifie si une machine est joignable sur le réseau. xxx.xxx.xxx.xxx correspond à l'adresse IP de la machine que l'on veut joindre

Exemples d'interventions

Voici quelques situations auxquelles je suis confronté, avec les méthodes utilisées pour détecter le problème et le résoudre à plus ou moins long terme.

- Situation numéro 1 :
 - Problème : Toute une partie du parc de la bibliothèque d'Epinal s'est déconnectée du réseau.
 - Analyse de la situation : En tenant compte que les appareils sont répartis sur plusieurs switches, mon réflexe a été de tester leur réactivité.

Pour se faire, j'ai débranché quelques câbles réseau et regarder le changement d'état des leds associées à leur port.

Il s'est avéré qu'un switch sur les trois ne réagissait pas au changement de situation (les leds vertes des ports indiquant si un appareil y est connecté continuaient d'indiquer qu'un câble était soi-disant branché dessus).

- Résolution du problème : Après redémarrage de celui-ci, les postes de travail qui y sont associés se sont tout de suite reconnectés au réseau.
 - Pour que ça ne se reproduise pas : La garantie a été activée et le switch a été remplacé par le prestataire.
- Situation n°2 :
 - Problème : Aussitôt après intervention de ma part sur un PC, celui-ci ne se reconnecte pas sur le réseau. Très rapidement également des collègues ont couru me prévenir que leurs PC avaient perdu Internet et que les téléphones étaient hors-services.
 - Analyse de la situation. Le timing entre mon intervention et la perte de connexion était trop parfait pour que ça soit une coïncidence. Aussi, j'ai vérifié mon câblage qui inclus un petit switch. Je me rends compte alors que j'ai fait une boucle.
 - Résolution du problème : J'ai tout débranché et j'ai repris mon branchement en faisant plus attention à mes câblages.
 - Pour que ça ne se reproduise pas : Les switches sont maintenant capables de prendre en charge le Spanning Tree Protocol.

J'ai résolu rapidement le problème car l'erreur venait de moi. Si cela été venu de quelqu'un d'autre, la détection de la boucle aurait été plus longue. Dans le cas-là, un des signaux qui aurait pu me faire aboutir à cette thèse aurait été que tous les voyants de trafic (voyants oranges) des switchs seraient restés constamment allumés.

- Situation n°3 :
 - Problème : Après la réinstallation d'une image d'un PC, celui-ci ne se reconnectait pas au réseau.

Pour vérifier si un ordinateur est bien connecté au réseau, il suffit de regarder la petite icône indiquant l'état du réseau, située dans la zone de notification, à droite de la barre des tâches.

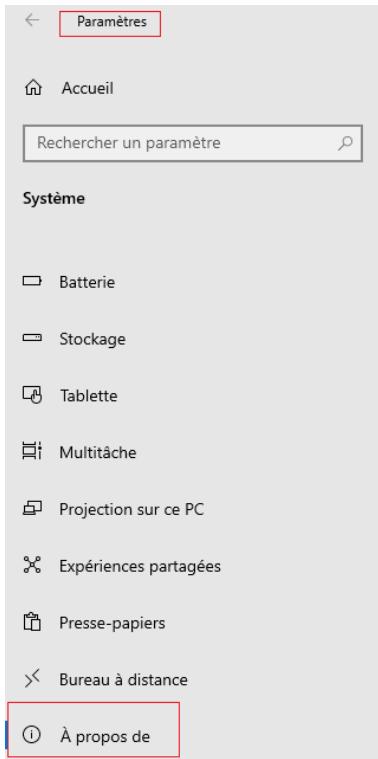


- Analyse de la situation : J'ai commencé par vérifier ses paramètres réseau. En tapant la commande : ipconfig/all dans l'invite de commande. Il s'est avéré que l'adresse IP qui lui avait été attribué commençait par 169.254.X.X soit une adresse APIPA (Automatic Private Internet Protocol Addressing).

J'ai pensé que le problème pourrait venir du serveur DHCP mais tous les ordinateurs qui se trouvaient à côté fonctionnaient correctement.

J'ai donc observé certains autres éléments de sa configuration, dont son nom de partage sur le réseau. En le comparant avec l'étiquette collée sur la tour qui indique le nom qu'il devait adopter, ceux-ci étaient différents. Il avait gardé le nom du PC qui m'avait servi à créer l'image que j'ai remonté.

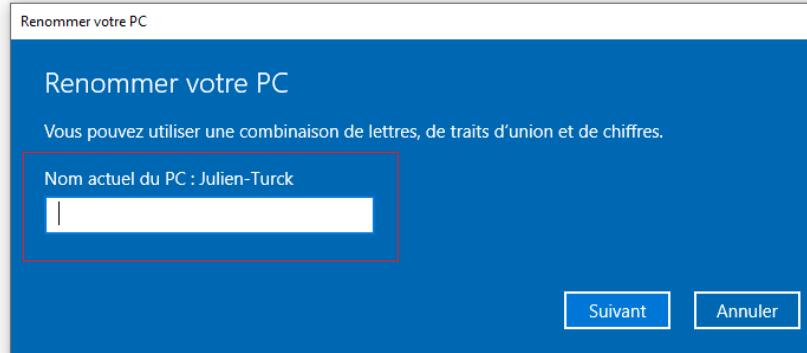
- Résolution du problème : J'ai renommé le PC. Pour ça, je suis allé dans le menu « système » des paramètres. Puis, dans « à propos », j'ai cliqué sur « renommer ce PC ».



À propos de

Votre ordinateur est surveillé et protégé.

[Voir les détails dans la sécurité Windows](#)



avec un stylet n'est pas disponible
sur cet écran

Copier

Renommer ce PC

- Pour que ça ne se reproduise pas : j'effectue l'enregistrement de mes images sur des postes types que je ne mets pas à disposition. Je garde leur nom de PC générique d'achat. J'effectue également un sysprep afin que mes images ne copient plus les données censées être unique pour chacun des postes présents sur un même réseau.
- Situation n°4 :
 - Problème : L'imprimante n'est plus disponible.
 - Analyse de la situation : Mon premier réflexe a été de vérifier sa connectivité au réseau en tapant la commande ping suivie de l'adresse IP de l'imprimante en question, dans l'invite de commandes. Il s'est avéré que la réponse était positive, le problème ne venait donc pas de ce côté.

```

c:\ Invité de commandes
Microsoft Windows [version 10.0.19045.3324]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\Jturck>ping 10.1.20.50

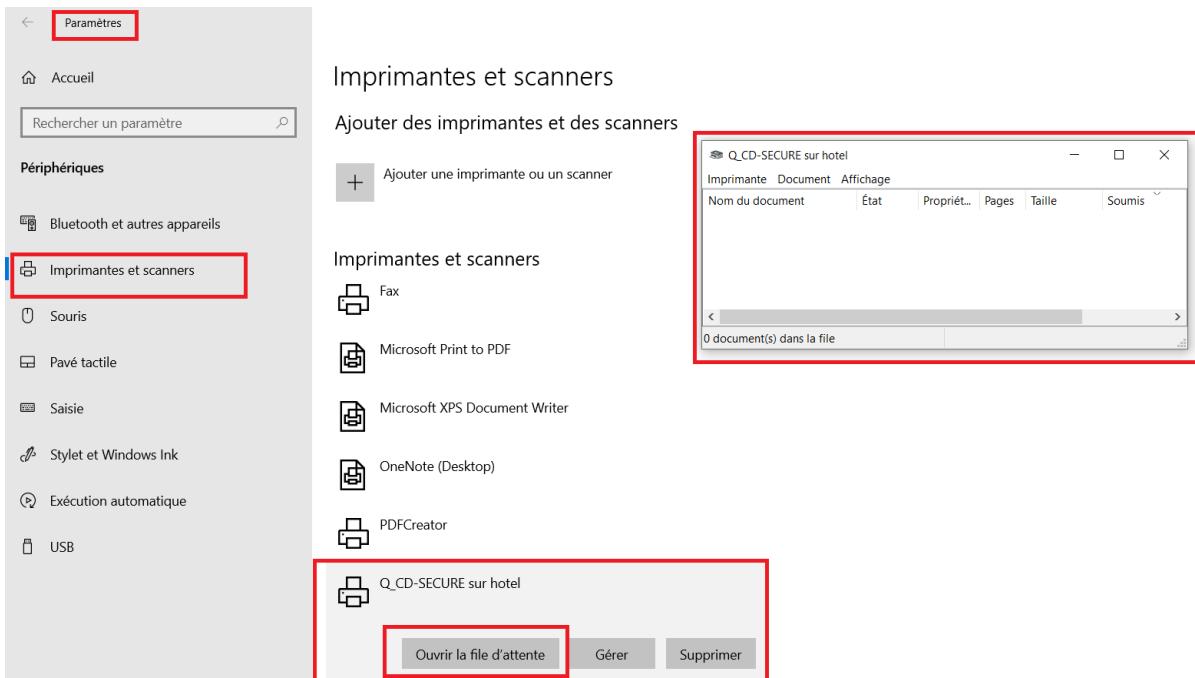
Envoi d'une requête 'Ping' 10.1.20.50 avec 32 octets de données :
Réponse de 10.1.20.50 : octets=32 temps=3 ms TTL=254
Réponse de 10.1.20.50 : octets=32 temps=26 ms TTL=254
Réponse de 10.1.20.50 : octets=32 temps=31 ms TTL=254
Réponse de 10.1.20.50 : octets=32 temps=4 ms TTL=254

Statistiques Ping pour 10.1.20.50:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 3ms, Maximum = 31ms, Moyenne = 16ms

C:\Users\Jturck>

```

J'ai donc ensuite parcouru sa file d'attente. Pour cela, je vais dans le menu « périphériques » puis le sous menu « imprimantes et scanners ». Enfin, je clique sur le bouton « file d'attente » de l'imprimante en question.



Je me suis ainsi rendu compte que celle-ci était simplement bloquée par un document de la veille qui n'avait pas pu être traité correctement.

- Résolution du problème : Il m'a suffi de le supprimer de la file puis redémarrer l'imprimante.

Ce problème n'était pas un souci lié au réseau mais grâce à cette commande qui test les connectivités entre appareils, j'ai pu écarter les mauvaises pistes liées à ce souci très rapidement et m'orienter sur la bonnes à suivre.

Heureusement, un réseau informatique n'est pas que source de problèmes. Il permet également de développer des services qui peuvent simplifier les tâches du quotidien des utilisateurs. Aussi, j'ai eu la chance de porter plusieurs projets en autonomie. C'est ce qui sera traité dans ma prochaine sous-partie.

b) Mise à disposition d'un service

Afin que la DRAC (Direction Régionale des Affaires Culturelles) valide le projet BNR présenté par la directrice, celui-ci doit également proposer le développement d'un service novateur. Le choix s'est porté sur la technologie RFID, son renouvellement quand existant et la mise en place de la technologie pour le reste du réseau. Ce projet m'a été confié dans le cadre de mon recrutement.

La RFID

RFID pour (Radio Frequency Identification Data) est une technologie qui permet d'identifier des objets à l'aide de puces que l'on intègre à son emballage ou que l'on glisse à l'intérieur de celui-ci.

Ces puces émettent des informations sur de courtes fréquences qui sont captées et interprétées par des lecteurs dédiés.

Cette technologie est notamment utilisée dans le commerce puisqu'elle permet :

- Une gestion des stocks :
 - Plus rapide, plusieurs puces pouvant être lues en même temps en quelques millisecondes
 - Plus fiable, car évite les erreurs de saisies manuelles
- Une réduction des pertes puisque :
 - Repère les objets précisément, donc permet de retrouver un objet perdu lors d'un déclassement
 - Compatible avec des systèmes antivols

Depuis plusieurs dizaines d'années les communes investissent dans cette technologie afin de simplifier la gestion de leurs bibliothèques. Par exemple, la ville de Rennes l'a adoptée dès 1984, afin de mettre en place un système antivol.

Epinal et Golbey en ont été dotés à leurs ouvertures en 2009 et Thaon-les-Vosges avait également quelques platines à mon arrivé en 2012.

Toutefois l'existant posait des problèmes :

- Epinal et Thaon avaient deux systèmes propriétaires incompatibles :
 - Epinal avait un des premiers systèmes de Nedap
 - Thaon un système de chez 3M, dont le service RFID a été racheté par Biblioteca en 2016
- Ces systèmes ne s'adaptent pas aux SIGB SaaS
Par exemple, ils ne permettent pas de communiquer directement avec le SIGB

Les objectifs que doivent atteindre le nouveau système sont :

- Simplifier le travail des bibliothécaires :
 - Allégement des tâches répétitives liées au prêt-retour
 - Réduction des tâches matérielles au profit de l'accueil des publics, en raccourcissant le temps passé au traitement des documents
 - Apport dans le rangement des collections ainsi qu'à la réalisation de ré-colemments
- Autonomiser le lecteur :
 - Permet à celui-ci d'effectuer seul l'enregistrement de ses opérations

- Assure la confidentialité des emprunts
- Sécuriser le Fonds documentaire
 - Permet de mettre en place un système antivol
- Permettre l'interopérabilité
 - L'interopérabilité est la capacité d'un système à fonctionner avec d'autres, existants ou futurs et ce sans restriction d'accès ou de mise en œuvre
 - L'encodage des puces doit respecter les normes ISO 28560-1 à ISO 28560-4
 - Les puces doivent respecter les normes ISO 14443 qui définit la fréquence en HF à émettre ainsi que leur structure.
Pour l'UHF, la fréquence a été définie avec la norme ISO 18000
 - Permettra d'inclure les systèmes RFID d'éventuelles nouvelles médiathèques dans le réseau.

La prospection

Afin de m'imprégner des évolutions de cette technologie, j'ai eu l'autorisation de visiter plusieurs grandes médiathèques qui avaient déjà mis en place cette solution.

Pour que ça soit pertinent, elles devaient également fonctionner avec des configurations similaires aux nôtres, à savoir gérer un réseau de médiathèques. J'ai donc visité Reims, Nancy et Strasbourg.

Les équipements

- De mes visites, j'ai retenu les solutions suivantes :
 - Les platines RFID :
- [Appareil permettant de lire les informations contenues dans les puces](#)
- Peu pratique au transport, je les privilégie pour des postes fixes
- Communiquent directement avec le SIGB
- Permettent d'enregistrer les prêts / retours des documents
- Permettent d'inventorier les nouvelles acquisitions



- Les douchettes RFID :
 - [Appareil permettant également de lire les puces RFID](#)
 - Plus facilement transportable, je les privilégie pour les installations temporaires ainsi que les tâches demandant des déplacements
 - Permettent de réaliser des inventaires et récolements directement dans les rayonnages
 - Permet d'aménager des postes temporaires sans paramétrages dans le SIGB



➤ Les automates de prêts :

- _ Ce sont des bornes tout-en-un (ordinateur + écran + platine RFID) tactiles avec une interface du SIGB simplifiée
- _ Permettent aux lecteurs d'effectuer leurs transactions seuls.
- _ Permettent de bloquer les prêts une fois les quotas atteint ou si des documents ne sont pas autorisés au prêt (réservé par quelqu'un, hors quota...)
- _ Lors des retours, prévient le lecteur lorsqu'il doit remettre un document aux bibliothécaires pour traiter de cas particuliers (réservations, document appartenant à une autre bibliothèque...)
- _ Permettent aux lecteurs d'autres actions comme la consultation de leur compte ou la prolongation de leurs prêts



- Les solutions que je n'ai pas retenues :
 - Les étagères intelligentes

- **Etagères capables de lire les puces des documents posés sur elles**
- Apport : Permet d'enregistrer automatiquement les retours sans passer par un enregistrement sur ordinateur (gain de temps pour le lecteur)
- Inconvénients :
 - _ Ne traite pas des cas particuliers (documents réservés par une autre personne, documents devant retourner dans une autre bibliothèque) obligeant les bibliothécaires à reprendre tous les documents posés dessus afin de repérer les cas particuliers.
 - _ Ne fonctionne qu'avec la fréquence UHF (voir explications plus bas)
 - _ Trop coûteux par rapport au peu d'apports



- Les boîtes de retours RFID
- **Bacs de retours capables de lire les puces des documents introduits**
- Apports : Permet d'enregistrer automatiquement les retours sans passer par un enregistrement sur ordinateur (gain de temps pour le lecteur)
- Inconvénients :
 - _ Ne traite pas des cas particuliers (documents réservés par une autre personne, documents devant retourner dans une autre bibliothèque) obligeant les bibliothécaires à reprendre tous les documents posés dessus afin de repérer les cas particuliers.
 - _ Trop coûteux par rapport au peu d'apports



➤ Robots de tri

— [Robots permettant de trier les documents](#)

— Apport : Trie les documents dans différents bacs en fonction de critères paramétrables. Elles peuvent donc séparer les cas particuliers des documents à remettre directement en rayon par exemple ou séparer les documents en fonction du secteur auquel le document est assigné

— Inconvénients :

— Demande un trop grand espace à dédier si je souhaitais autant de bacs que de critères de tris différents simultanément

— Trop couteux alors que le gain de temps est assez relatif. En effet, ce n'est pas le tri des retours qui prend le plus de temps, celui-ci étant fait au fur et à mesure des enregistrements.



Le choix des technologies

- Les connectiques

Les lecteurs de puces peuvent être reliés aux postes par le biais de deux connectiques :

➤ Ethernet

_ Ne concerne que les platines des postes fixes et des automates

_ Avantages :

 _ Communiquent directement avec le SIGB, sans avoir à manipuler un second logiciel servant d'intermédiaire

 _ Permet la lecture et l'écriture de puces simultanément. Ça permet ainsi un gain de temps durant les manipulations

_ Inconvénients :

 _ Plus coûteux

 _ Moins de flexible dans l'organisation des postes : Il doit y avoir une prise RJ45 à proximité et la platine est liée au poste dans le SIGB (voir installations plus bas dans le texte) ce qui complexifie la réattribution d'un lecteur à un autre PC.

 _ Dégradation du service si coupures Internet

 _ Perte du service si défaillances sur le réseau

➤ USB

_ Concerne les platines ainsi que les appareils mobiles

_ Avantages :

- _ Moins coûteux
- _ Installations logiciels plus simples
- _ Permettent de fonctionner sans être reliés à un réseau et sans connexion Internet, le tout sans dégradation de service

_ Inconvénients :

Ne peuvent pas lire et écrire sur la puce simultanément. Certaines tâches demandent donc plus de manipulations.

Par exemple, l'enregistrement des transactions des lecteurs : En effet, cette démarche demande au logiciel de lire le numéro d'inventaire du document afin que le SIGB comprenne quel document est emprunté ou rendu. De plus, le logiciel doit réécrire le bit de l'antivol afin de le réactiver si retour ou le désactiver si c'est un emprunt.

- Les fréquences

- La Haute Fréquence :

_ [La HF émet sur une fréquence de 13,56 MHz](#)

_ Avantages :

- _ Moins coûteuse
- _ Lecture sur de faibles distances (80cm maximum), limitant ainsi le risque d'erreurs
- _ Propose des lecteurs avec des connectiques RJ45

_ Inconvénients

- _ Les métaux perturbent cette technologie, ne permettant donc pas des étagères aluminium par exemple
- _ Offrent moins de possibilités dans les choix des services RFID
- _ Le peu de distance couvert offre moins de flexibilité dans l'organisation des postes
- _ Le système antivol est un système de portiques imposant et demandant des travaux au sol afin que les câbles ne soient pas visibles, ni dangereux en étant saillant et donc risquer que quelqu'un trébuche à cause d'eux.



➤ L'Ultra Haute Fréquence

— l'UHF émet sur une fréquence allant de 865 MHz à 868 MHz

— Avantages :

— Des distances couverts plus longues, permettant donc plus de flexibilités dans l'organisation des postes

— Offrent des possibilités de services plus innovants comme l'étagère intelligente ou des systèmes antivols plus discrets avec des dômes au plafond par exemple.



— Inconvénients :

— Ne proposent pas de lecteurs avec une connectique RJ45

— Plus coûteuse

- _ perturbées par la présence de corps conducteurs comme le corps humain
- Mes choix de technologies :

Aussi, j'ai fait le choix de m'orienter vers la HF avec des platines RJ45 et quelques lecteurs portables.

➤ La HF parce que :

- _ C'est la seule technologie à proposer des platines RJ45
- _ Répond aux objectifs à remplir par ma hiérarchie
- _ N'ayant pas utilité de services uniquement disponibles en UHF, je me suis donc tourné vers la fréquence la moins coûteuse
- _ N'est pas incompatible avec l'intégration de puces et de services UHF, si besoin plus tard. Simplement les documents devront avoir deux puces pour pouvoir être compatibles avec tous les services
- _ Les portiques antivol, étant plus imposant, sont plus dissuasifs. C'est un aspect important car la parade contre l'antivol est très simple : il suffit d'arracher la puce ou glisser le document dans un sac avec du métal à l'intérieur.

De plus, ils ont une autre utilité : ils permettent le comptage des passages et donc de connaître le nombre de personnes à l'intérieur du bâtiment. Ce qui retire une tâche à faire au personnel présent à l'accueil, dont le comptage était approximatif du fait qu'il gérait les abonnements des lecteurs en même temps.

Toutefois, Seules les médiathèques les plus grandes ont été équipés de ces portiques. Des caméras de comptages ont été installées dans les plus petites.

➤ Les platines Ethernet parce que :

- _ La notion de gain de temps dans les tâches est très importante pour la direction. Ce sont les seules platines qui permettent de communiquer directement avec le SIGB ainsi que la lecture et l'écriture simultanément. Ça permet donc de réduire les manipulations de manière significative
- _ Pour réduire les coûts, j'ai simplement ciblé les PC qui traiteront de manière permanente de grands volumes de document, afin de n'avoir que le nombre juste de platines. Ça ne comprend donc que les automates de prêts, les postes dédiés à l'accueil du public et les postes dédiés à la réception des commandes pour chacune des bibliothèques du réseau.
- _ Bien que ça soit en mode dégradé, elles permettent la continuité de service malgré une coupure Internet

➤ Les lecteurs en USB

- _ Permet les tâches demandant des postes mobiles (pour l'inventaire et le récolement qui se font directement dans les rayonnages par exemple).
- _ Permet d'être utilisé hors-les-murs, lorsqu'on participe à des événements en extérieur ou lorsqu'on se déplace chez des partenaires)
- _ Permet de prendre le relais d'une platine en cas de défaillance du réseau interne
- _ Je les garde dans mon bureau et je les mets à disposition sur demande ou durant une panne importante

- **Contacts des entreprises**

La commande publique

Étant agent de collectivité, je suis soumis au code des marchés publics.

L'Ordonnance n° 2018-1074 du 26 novembre 2018 régie ce code. Les marchés publics sont définis comme des contrats conclus à titre onéreux par un ou plusieurs acheteurs publics avec un ou plusieurs opérateurs économiques, pour répondre à leurs besoins en matière de travaux, de fournitures ou de services.

Il est prévu plusieurs procédures en fonction du seuil atteint par le montant hors taxe du projet. Début 2020, ces seuils avaient été rehaussés :

- Jusque 40 000€, pas de procédure
- A partir de 215 000 € pour les fournitures et les services, nous devons respecter les procédures formalisées avec des publicités réalisées dans le [Journal Officiel de l'Union Européenne \(JOUE\)](#) ainsi que dans le [Bulletin Officiel des annonces des marchés publics \(BOAMP\)](#)
- Entre les deux, seront appliqués des procédures adaptées avec des publicités jugées adéquates par les collectivités ([MAPA pour Marché A procédure Adaptée](#))

Aussi, pour éviter que mon projet ne dépassant pas les 40 000€, la direction me l'a fait découper par :

➤ Un allotissement (découpage en lot) avec un lot pour :

- _ Les lecteurs RFID
- _ Les consommables
- _ Les systèmes de comptages hors antivol

➤ Des achats en plusieurs phases :

_ Renouvellement de l'existant à Epinal. Durant cette phase, le matériel remplacé mais encore fonctionnel a été installé dans les autres médiathèques

_ Achat de matériel neuf pour les autres médiathèques

_ Développement de l'offre à Epinal avec la multiplication des automates de prêts.

➤ Ça m'a permis, de faire une demande de devis directement auprès des fournisseurs que j'ai choisis pour chacune des phases et des lots.

Pour les choisir, je me suis appuyé sur les entreprises qui ont équipées les bibliothèques que j'ai visité et qui étaient satisfait du fonctionnement de leurs matériels.

J'ai donc contacté les deux fournisseurs Nedap et de Bibliothéca qui se disputent l'essentiel du marché sur toute la France.

Le cahier des charges

Afin de formaliser ma demande, j'ai utilisé le cahier des charges prérempli proposé par l'ENSSIB (l'École Nationale Supérieure des Sciences de l'Information et des Bibliothèques).

- Sous licence Creative Commons

Les licences Creative Commons constituent un ensemble de licences régissant les conditions de réutilisation et de distribution d'œuvres.

- Admis par ces deux sociétés qui ont l'habitude de travailler avec des bibliothécaires
- Répertorie tout le matériel possible d'acquérir, les spécificités que je ne dois pas omettre de préciser, ainsi que les prestations à ne pas oublier.
- Je me le suis toutefois quelque peu réapproprié en précisant :
 - Les normes ISO à respecter
 - Quelques précisions sur le fonctionnement attendu :

_ Les platines doivent pouvoir communiquer avec le SIGB directement

_ Permettre une communication sécurisée

- J'ai demandé que du matériel soit prêté afin de tester les produits avant de les acheter.

- J'ai également précisé les prestations attendues :
 - Une première installation par le prestataire

_ Du matériel

_ Des différents logiciels qui seront pour mon cas :

_ Le driver des platines

Driver est un logiciel qui fait le lien entre le PC et l'appareil qui lui est relié avec lequel il ne sait pas communiquer nativement.

_ Le webservice de Nedap pour l'utilisation des lecteurs Ethernet

_ Le logiciel RFTestLite pour le paramétrage des platines

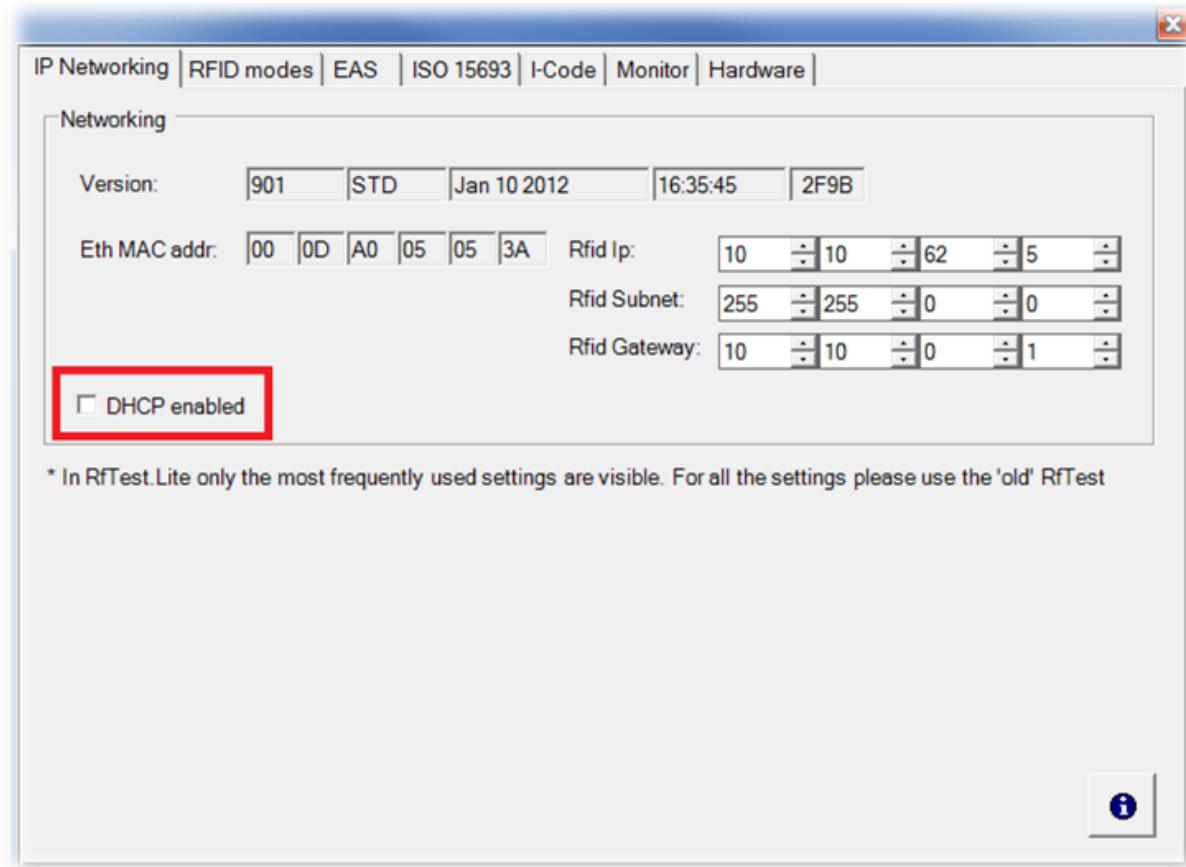
_ Le logiciel BilbioCheck4Lite pour l'utilisation des lecteurs USB et du prêt secouru

_ Le logiciel LibRid3 pour l'automate de prêt

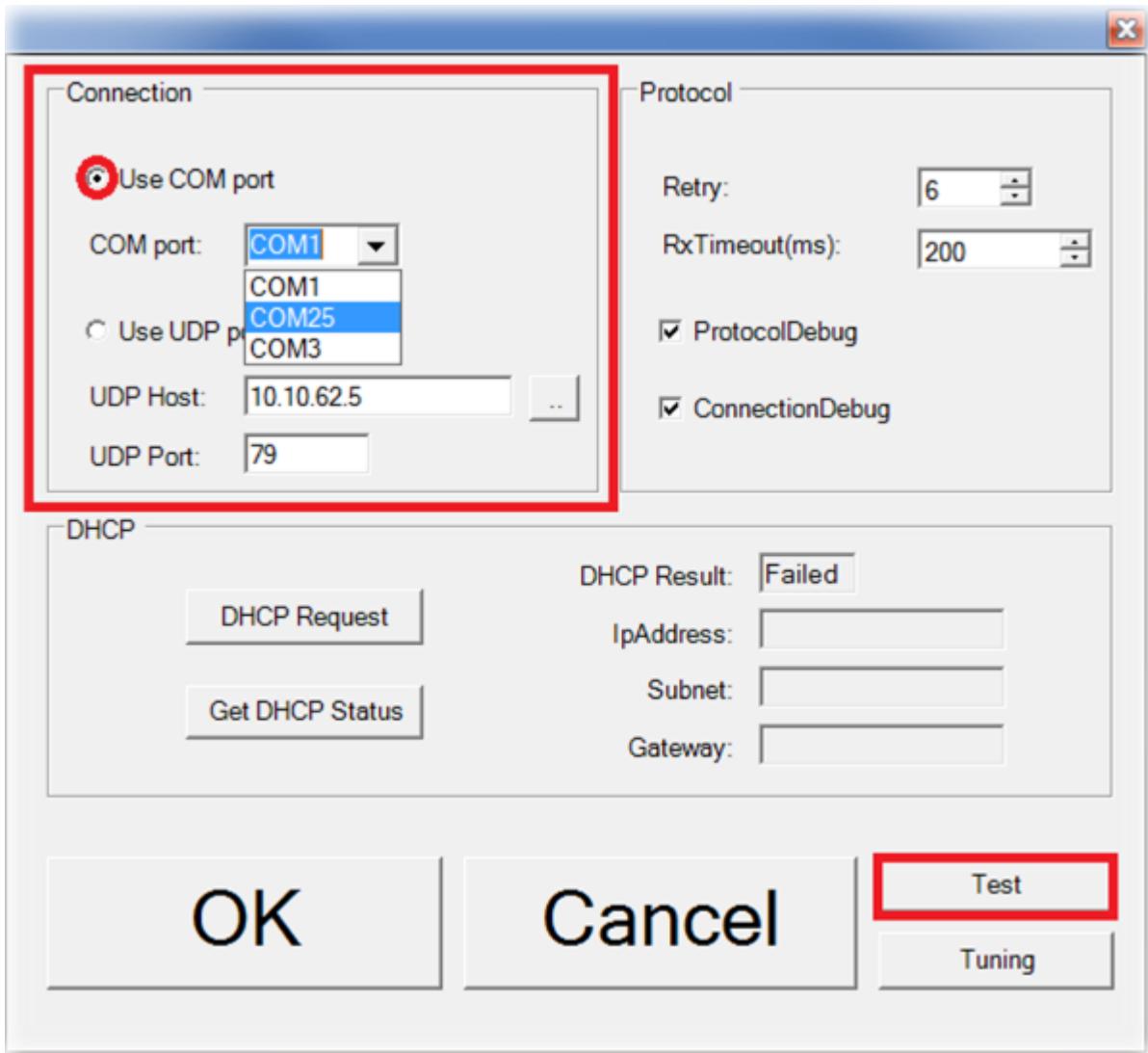
- Un transfert de compétence pour :

_ Le branchement et le paramétrages des platines :

_ Pour leur paramétrage, il faut les brancher une première fois en USB. Je me rends ensuite dans le gestionnaire de périphériques puis je clique sur « Silicon Labs CP210x USB to UART Bridge (COM 25) » qui se trouve dans le sous menu « Ports (COM et LTP). Dans la nouvelle boîte de dialogue j'ouvre l'onglet « IP Networking ». C'est ici que je vais leur attribuer une adresse IP fixe ainsi que le masque de sous-réseau et la passerelle. Les autres paramètres sont laissés par défaut.



Je quitte tout et je lance le logiciel RFTestLite. Je clique alors sur « CFG » et je sélectionne la connexion par UDP port en indiquant l'adresse IP de la platine qui lui sera associée si elle possède une connectique RJ45. Pour les postes qui n'accueillent que des lecteurs USB, je sélectionne le COM port. Dans les deux cas, je termine en cliquant sur « test » afin de vérifier que les deux machines communiquent bien.



Sur le SIGB, je renseigne où doit pointer le profil d'intégration pour trouver le webService dans la case « URL serveur ». L'URL précise que le webService se trouve sur la machine (localhost), que le web service écoute le port 80 (par défaut) et que son nom est NedapRfidWebService.asmx. Il faut également cocher la case « actif »

The screenshot shows a profile configuration screen with the following sections:

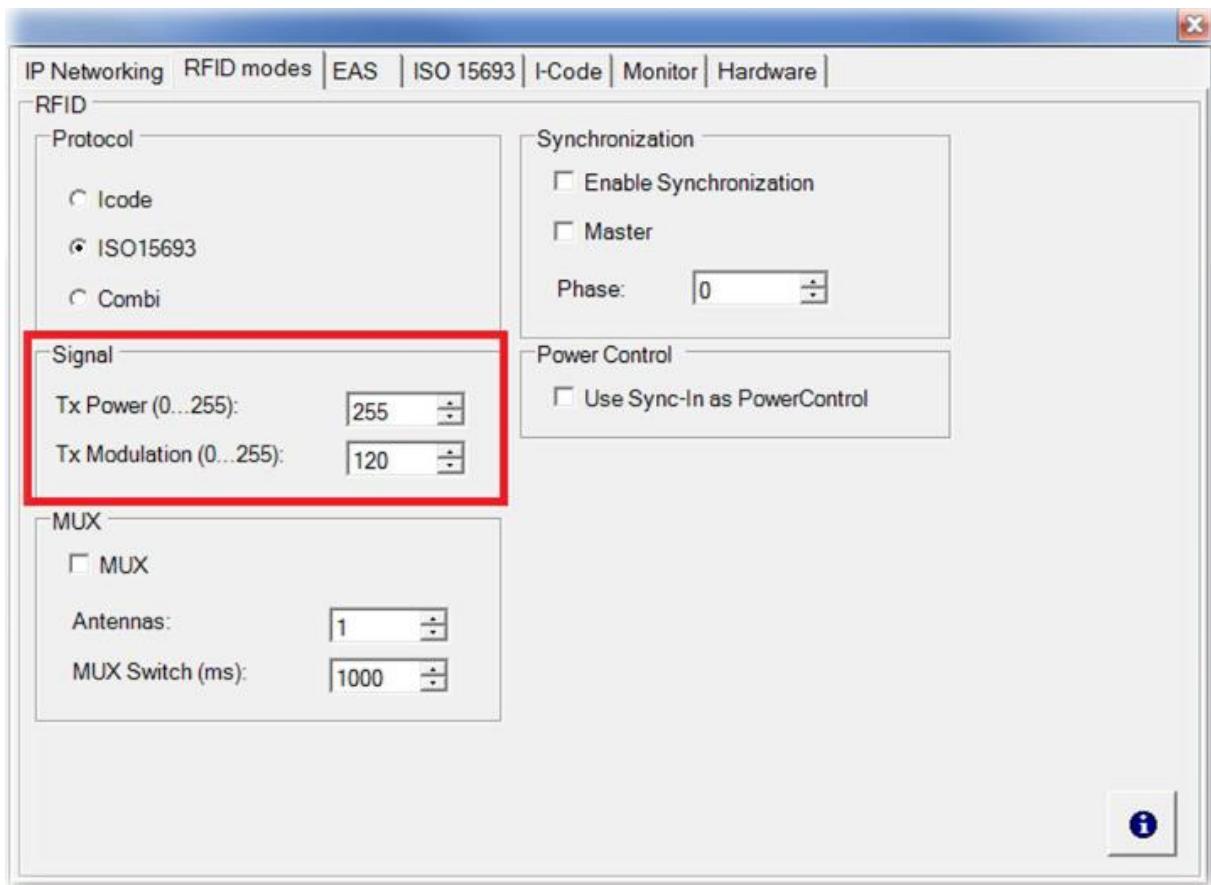
- Profile Name**: **NEDAP_RFID_1** (highlighted by a red box)
- Buttons**: **Information générale**, **Actions**, **Information de contact**
- RFID DEFINITIONS**
 - Checkboxes: **Actif** (checked)
 - Text field: **URL du serveur *** (**http://localhost:80/NedapRfidWebService.asmx**) (highlighted by a red box)

Il faut ensuite, pour chacune des machines répertoriées dans le SIGB, leur indiquer l'adresse IP de la platine vers laquelle elle pointe. Le champ se nomme « informations RFID Nedap » et s'affiche en double cliquant sur la machine concernée.

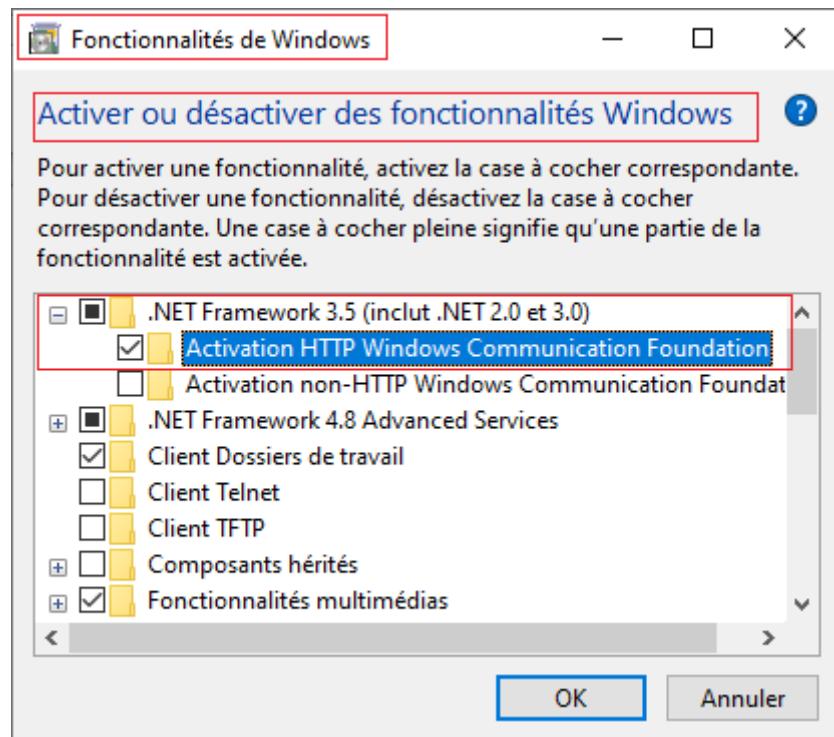
The screenshot shows a software interface for managing machine configurations. At the top, there are three input fields: 'Chèque' with an unchecked checkbox, 'Imprimer le reçu ?' with a dropdown menu set to 'Non', and 'E-mail des reçus' with a dropdown menu set to 'N'. Below these, a section titled 'Automate de prêt - Informations' contains a checkbox for 'Dispose d'un automate de prêt' which is unchecked. Underneath is a section titled 'Informations RFID Nedap' which contains an 'Adresse IP' field with the value '10.23.107.1'.

- _ Quelques éléments de maintenance :
 - _ Le réglage du faisceau de portée de la lecture des puces

Dans « Silicon Labs CP210x USB to UART Bridge (COM 25) », j'ouvre l'onglet « RFID modes ». Dans la partie signal, je modifie les valeurs de Tx Power et de « Tx modulation ». Je test en ensuite la portée du signal en approchant des documents de la platine concernée.

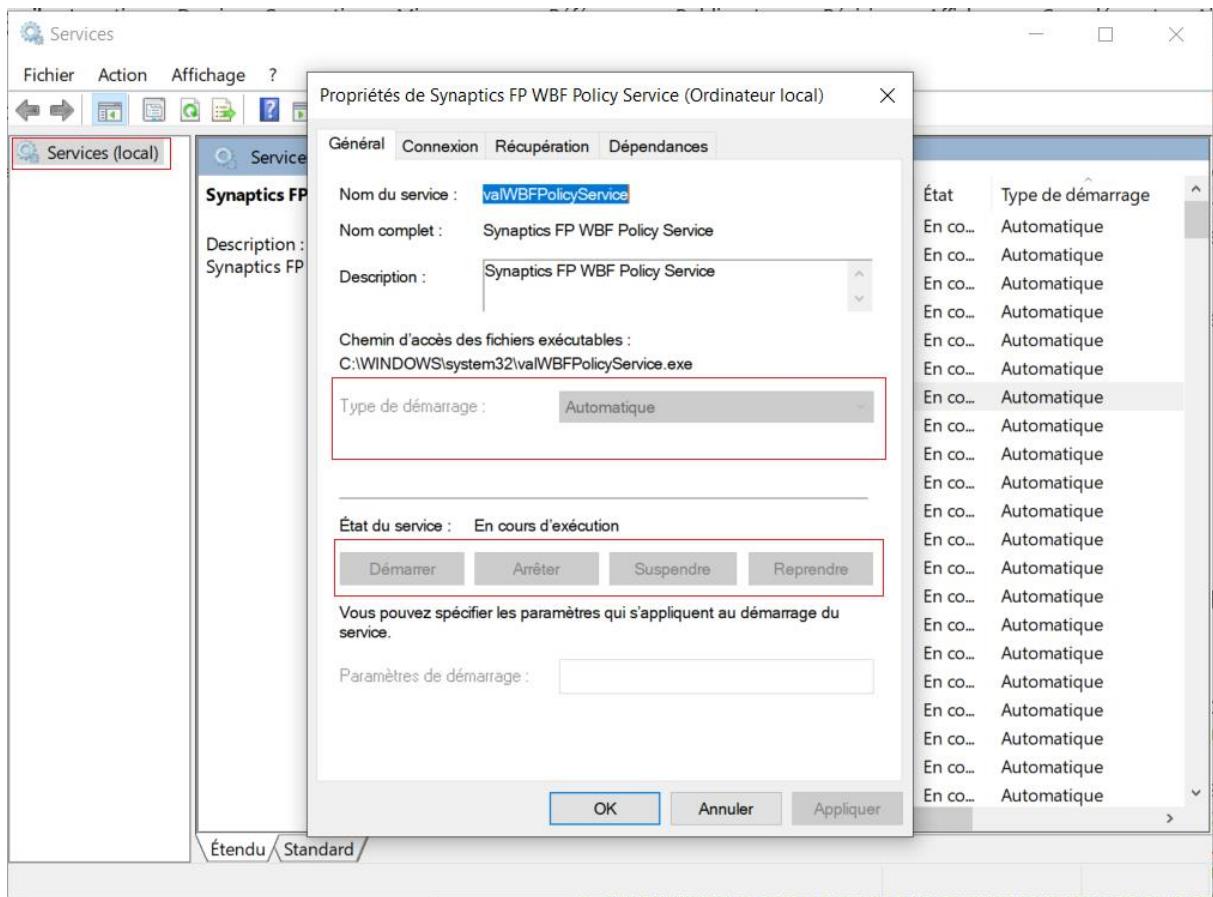


- _ Le raccordement des deux parties des platines.
- _ L'installation et l'utilisation des logiciels cités plus haut.
- _ Paramétrages des PC pour lesquels je dois effectuer :
 - _ L'activation la fonctionnalité Windows Net Framework 3.5
Pour cela, je tape « fonctionnalité » dans la barre de recherches et je clique sur « activer ou désactiver des fonctionnalités de Windows ». Je coche la case correspondante à la fonctionnalité et en déroulant à l'aide du « + » je coche également la case « Activation HTTP Windows Communication Foundation ».



_ L'activation/désactivation du web service dans les services Windows.

Pour cela, je tape « services.msc » dans la barre de recherches et je clique sur « services.msc ». Dans la boite de dialogue, je cherche NedapRFIDwebservice, je fais un double clic dessus. Une dernière fenêtre s'ouvre. Je peux alors le mettre n démarrage « automatique » ainsi que l'« arrêter » ou le « démarrer » en fonction des cas.



- Un SLA (Service Level Agreement) qui prévoit une plateforme permettant la création de ticket de demande d'intervention avec une première réponse dans les 24H et une intervention sur site dans les 48H ouvrés.
- Une visite de contrôle annuelle
- Une garantie matérielle les 3 premières années.

Cahier des charges

1. Informations générales sur la bibliothèque à équiper

Nom de la bibliothèque	
Nom de la commune	
Adresse pour la réponse	

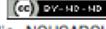
2. Personne à contacter en cas de besoin

Nom et prénom :	
Service	
Téléphone	
Mail	

3. Description générale de la bibliothèque

Surface de la bibliothèque	
Nombre de livres	
Nombre de documents sonores	
Nombre de DVD	
Nombre de CD-Rom	
Nombre de périodiques	
Nombre d'emprunteurs	
Nombre de prêts par an	
Composition et qualification de l'équipe de la bibliothèque	
SIGB de la bibliothèque	

104

 AGIE Sophie, DENEFLE Clémence, DUPONT Violette, FOURMEUX Thomas, KUCHMANN Emilie, NOUGAROL Lucile, ROEKENS Florence, ROZENMAN Philippe-Alexis, SAPIELAK Caroline, TAMAGNO Lise, THOMAS Valérie / Guide pratique RFID et automates prêt/retour en bibliothèque

4. Renseignements sur la demande

Demande	Nombre
RFID	
Logiciel	
Puce RFID pour les livres	
Puce RFID pour les documents sonores	
Puce RFID pour les DVD	
Platine	
Portail antivol	
Douchette	
Lecteur portable	
Cartes lecteurs	
Automate intérieur	
Automate de plain-pied	
Automate sur roulette	
Automate d'appoint	
Automate pour enfants	
Automate pour les personnes à mobilité réduite	
Etagère intelligente	
Carrousel de retour	
Boîte de retour extérieure automatisée	
Boîte de retour extérieur automatisée	
Trappe de retour extérieur automatisée	
Boîte de retour extérieur automatisée avec système de tri	

105

 AGIE Sophie, DENEFLE Clémence, DUPONT Violette, FOURMEUX Thomas, KUCHMANN Emilie, NOUGAROL Lucile, ROEKENS Florence, ROZENMAN Philippe-Alexis, SAPIELAK Caroline, TAMAGNO Lise, THOMAS Valérie / Guide pratique RFID et automates prêt/retour en bibliothèque

Autres prestations	
Installation du matériel	
Formation du personnel	

5. Fonctionnalités recherchées

RFID	
Dimensions des puces	
Puces actives ou passives	
Fréquence requise pour les puces	
Sur étiquette imprimée	
Dimension des cartes lecteur	
Fréquence requise pour les cartes usager	
Automate intérieur	
Prêt seul	
Retour seul	
Prêt/Retour	
Lecteur de carte	
Module de paiement	
Récapitulatif	
Langues	
Accès au compte lecteur (réservation, prolongement,...)	
Visuel de l'interface	
Design	

106

 AGIE Sophie, DENEFLE Clémence, DUPONT Violette, FOURMEUX Thomas, KUCHMANN Emilie, NOUGAROL Lucile, ROEKENS Florence, ROZENMAN Philippe-Alexis, SAPIELAK Caroline, TAMAGNO Lise, THOMAS Valérie / Guide pratique RFID et automates prêt/retour en bibliothèque

Boîte de retour extérieure automatisée	
Interface	
Système de tri avec bennes (nombre de bennes)	
Système de tri avec carrousel	
Autres	
Journée de formation	
Contrat de maintenance	
Assistance téléphonique	
Solution clé en main (logiciel + matériel + installation + formation+ maintenance)	
Garantie du matériel	

107

 AGIE Sophie, DENEFLE Clémence, DUPONT Violette, FOURMEUX Thomas, KUCHMANN Emilie, NOUGAROL Lucile, ROEKENS Florence, ROZENMAN Philippe-Alexis, SAPIELAK Caroline, TAMAGNO Lise, THOMAS Valérie / Guide pratique RFID et automates prêt/retour en bibliothèque

Le choix du prestataire :

A la réception des devis et du matériel d'essai, j'ai pu faire mon comparatif entre les deux offres. Pour définir l'offre la plus intéressante, j'ai opté pour un ratio :

- 30 % de la note allant au prix
 - Celui qui propose le tarif le plus bas à 0.3 / 1
 - L'autre prestataire à une note abaissé avec le pourcentage que représente son écart avec le plus compétitif

152

- Par exemple si j'ai une offre à 30 000 et une à 35 000, ça me donne les calculs suivants :

$$(30\ 000 \times 100) / 35\ 000 = 85\%$$

$$0.3 \times 0.85 = 0.26$$

$$0.26 / 10 = 0.026$$
- La note attribuée pour cette partie au plus onéreux est donc de 0.26 / 1
- 40 % de la note allant à la technique. Ça inclut :
 - La satisfaction du fonctionnement du matériel une fois installés dans leurs environnements définis.
 - La satisfaction des prestations complémentaires proposées
 - J'ajoute 0.2 / 1 pour chacun des deux critères respectés
- 30% de la note allant à l'interopérabilité avec les puces existantes
 - Les nouveaux systèmes peuvent-ils déchiffrer les puces existantes
 - Les nouveaux systèmes peuvent-ils réencoder les puces existantes
 - J'ajoute 0.15 / 1 pour chacun des deux critères respectés
 - Le but de cette partie de la note est de privilégier un système qui évitera au maximum de reprendre le fonds déjà pucé
 -
- J'additionne ensuite chacune des sous notes ce qui a donné :
 - Nedap : 0.3 (car le moins cher) + 0.2 (tout fonctionnait durant les tests) + 0.2 (propose les mêmes prestations que celles attendues) + 0 (tout le fonds de Thaon était à réencoder) + 0.15 (toutes les puces d'Epinal et de Thaon sont réencodables par le nouveau système proposé) = **0.85**
 - Bibliotheca : 0.26 (car plus cher d'un peu moins de 15%) + 0.2 + 0.2 + 0 + 0.15 (les offres techniques et de prestations étaient similaires) = **0.81**
 - C'est donc Nedap qui a été choisi, leur tarif plus avantageux ayant fait la différence.

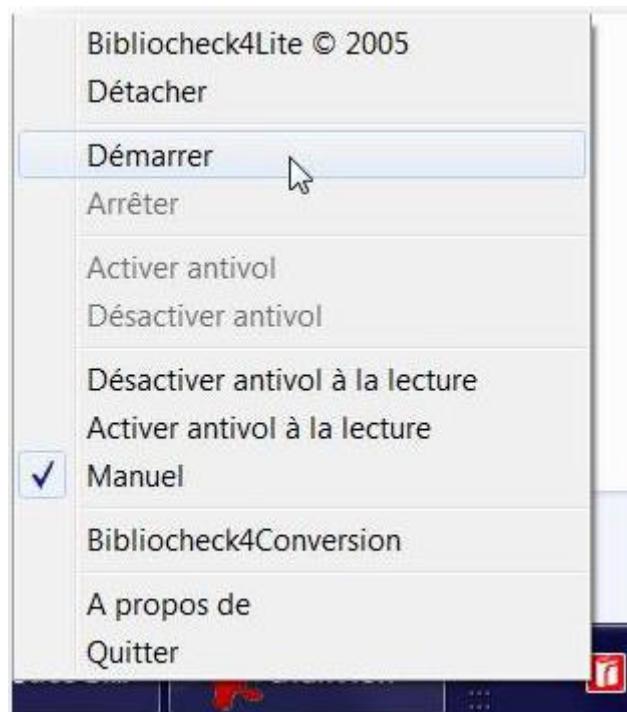
Formation des utilisateurs

Une fois les installations et les tests réussis, il me reste à former les agents avant de relancer officiellement le service. J'ai donc formé :

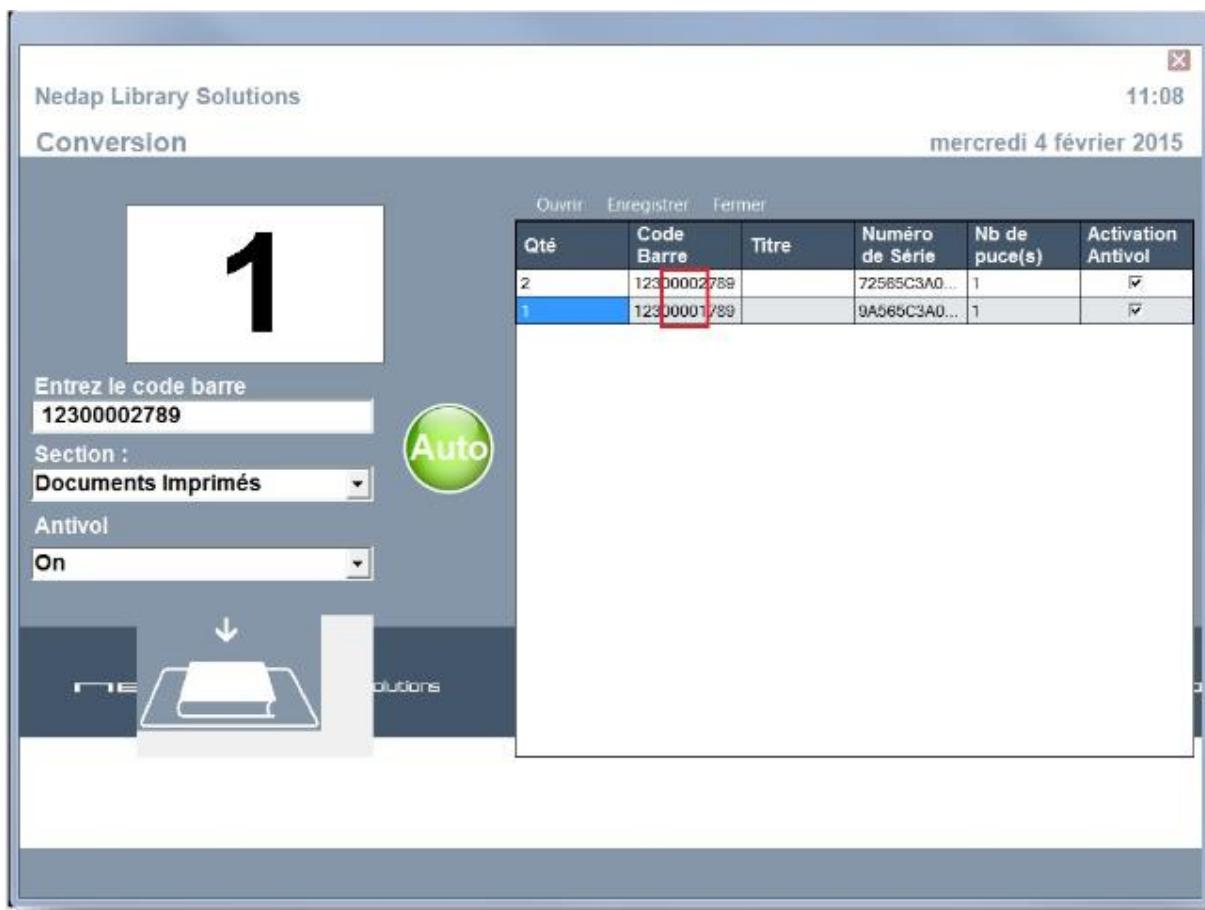
- Tous les agents sur le logiciel BiblioCheck4Lite :
 - Utilisé :
 - _ Lors d'une panne coupant d'Internet
 - _ Lors de l'utilisation des lecteurs USB
 - Permet :
 - _ La lecture automatique des puces à proximité du lecteur
 - _ L'activation ou la désactivation manuelle de la fonction antivol des puces durant les prêts et retours des documents
 - _ L'encodage de nouvelles puces
 - Fonctionnement au quotidien :
 - Une icône apparaît dans la barre de notifications.**

Pour que la lecture se fasse, il faut que l'icône soit orange. Si elle est rouge, je fais un clic droit pour ouvrir son menu contextuel et je clique sur « démarrer ».

Pour gérer l'antivol, toujours dans le menu contextuel, je clique sur « activer antivol à la lecture » ou « désactiver antivol à la lecture », en fonction de si c'est un prêt ou un retour.



Pour encoder une nouvelle puce, dans le menu contextuel, je sélectionne « BiblioCheck4Conversion ». Une nouvelle fenêtre apparaît. Dans cette fenêtre j'entre le numéro d'inventaire que je veux associer à la puce, ainsi que son type de document. Je pose la puce sur la platine. S'affiche alors le nombre de puces détectées qui doit être égal au nombre de puces posées sur la platine. Je clique sur « Auto ». A droite s'affiche alors un résumé de l'opération.



- Tous les agents sur LibRid3
 - Logiciel de gestion des automates de prêt
 - Les bibliothécaires doivent le maîtriser dans le cadre de l'accompagnement du public à son utilisation
 - Il permet de :

_ Effectuer un prêt :

Pour se faire, le lecteur appuie sur le bouton « prêt » de l'écran d'accueil. Il passe ensuite sa carte sur la platine. Il place ses documents sur la platine et vérifie que chacun apparaisse bien dans le listing dessous. Il peut ensuite imprimer un ticket de reçu en appuyant sur « Imprimer reçu ».



Prêt

BROSSARD Olivier

Placez votre document sur la cible

#	Titre	Retour le
1	Valency, l'homme aux mains chaudes / Harry Philippe Lebon	26/09/2016
2	Eaux fortes / Anne-Dauphine Du Chatelle	26/09/2016
3	Madras / Éric Nonn	26/09/2016
4	Félicité / Marie Borin	26/09/2016
5	PowerPoint 97	26/09/2016
6	Acouphènes / Géraldine Maillet	26/09/2016

Sortir

_ Effectuer un retour :

Les lecteurs appuient sur le bouton retour. Il passe ensuite ses documents sur la platine. Il vérifie que tous apparaissent bien dans la liste dessous. Lorsqu'ils ont terminé, ils appuient sur « sortir ».



Retour

Placez votre document sur la cible

#	Titre
1	Record à battre / Courtney Eldridge
2	Éblouie / Annick Le Floc'hmoan
3	Acouphènes / Géraldine Maillet
4	PowerPoint 97
5	Le plan qualité logiciel / Dominique Vauquier
6	Félicité / Marie Borin

Sortir

_ Consulter son compte :

Les lecteurs appuient sur le bouton « compte ». Il passe ensuite leur carte sur la platine. S'affiche alors le nombres de documents empruntés, en retard et les réservations disponibles. Ils peuvent ensuite quitter en appuyant sur le bouton « sortir ».



Votre compte

BROSSARD Olivier
olivier.brossard@nedap.fr

1 Réservation
Disponible

5 à la maison

0 Document(s)
en retard

Imprimer reçu

Prêt

Prolonger

Sortir

_ Effectuer une prolongation :

Lorsqu'ils sont sur leur compte, ils appuient sur le bouton « prolongation ». Ils peuvent alors sélectionner les documents qu'ils souhaitent conserver et appuient sur le bouton « prolonger ». Ils peuvent ensuite appuyer sur le bouton « fin ».



Prolongation

Prolonger

Retour le	Titre	Prolongation
23/08/2018	Play dead	<input checked="" type="checkbox"/>
23/08/2018	Mother / Luc Lang	<input type="checkbox"/>
23/08/2018	Notre-Dame de Paris / Victor Hugo	<input checked="" type="checkbox"/>
23/08/2018	La Maison des Secrets / Jacqueline West	<input type="checkbox"/>
23/08/2018	Une vie / Guy de Maupassant	<input checked="" type="checkbox"/>
23/08/2018	Contes de Perrault / Charles Perrault	<input type="checkbox"/>
23/08/2018	Frisson en eau trouble / R.L Stine	<input type="checkbox"/>

Page

< 1 2 >

Imprimer reçu

Fin

En conclusion de cette activité, j'ai démontré ma monté en compétences dans le domaine de l'administration des systèmes et des réseaux. J'ai explicité mes capacités à :

- _ Concevoir une solution d'infrastructure réseau
- _ Installer, tester et déployer une solution d'infrastructure réseau
- _ Exploiter, dépanner et superviser une solution d'infrastructure réseau

De plus, le projet RFID à démontrer mes compétences en matière de mise à disposition d'un service informatique.

J'évoque également rapidement un aspect important à prendre en compte, qui est la sécurité du SI. Toutefois, je dois l'expliciter beaucoup plus en détails et ce sera l'objet de l'activité n°3.

Fiche descriptive de l'activité 3

La sécurité au centre de nos préoccupations

ACTIVITÉ 3 : La sécurité au centre de nos préoccupations

La sécurité des systèmes d'information (SSI) est l'ensemble des moyens techniques, organisationnels, juridiques et humains visant à empêcher une utilisation non autorisée du système d'information et de ses données, afin d'en éviter son mauvais usage, toute perte ou modification de données, qu'elle soit involontaire ou intentionnelle ainsi que son détournement. Ses finalités sont une cohérence de l'ensemble du système d'information et de maintenir la confiance des utilisateurs et des clients. Elle s'appuie actuellement sur la norme ISO/CEI 27001.

Depuis quelques années, c'est devenu un enjeu majeur pour toutes les entreprises ainsi que pour l'ensemble des collectivités et des services de l'état. En effet, la cyber-criminalité est en forte augmentation tant la donnée numérique a aujourd'hui une valeur quasi-inestimable. Et pour arriver à leurs fins, les hackers, dont les motivations peuvent varier, développent toujours plus de moyens et de techniques. On recense différents types d'arnaques par le biais des mails et sms pour soudoyer les utilisateurs les plus crédules, comme l'hameçonnage et le FOVI (faux ordre de virement) par exemple. Voir forcer la main d'un utilisateur, pour infiltrer par le biais d'un virus ou d'un Trojan, l'infrastructure qui permettrait par exemple une attaque par déni de service (DDoS) ou l'installation d'un rançongiciel. La menace peut donc être aussi bien externe qu'interne au service, soit par négligence, soit par malveillance. La sécurité n'est plus confinée uniquement au rôle de l'informaticien mais concerne tous les utilisateurs du système.

Aussi, pour renforcer la sécurité des données et mettre devant leur responsabilité n'importe quelle entité qui collecte des données, l'Union Européenne a adopté depuis 2016 la loi dite RGPD, qui oblige à n'importe quelle structure ayant des données de citoyens européens à tout mettre en œuvre pour garantir la sécurité de celles-ci tout en respectant une charte de bonnes utilisations. Les collectivités et leurs services étant concernées, c'est le second enjeu de mon travail au quotidien que de mettre aux normes le réseau de lecture publique. Même si à priori, nos données ne présentent qu'un intérêt mineur.

A priori seulement, car deux évènements, dont un qui nous a touché directement nous ont démontrés que personne n'est à l'abri d'un accident ou d'une attaque.

C'est tout le propos de cette activité qui abordera dans un premier temps mes actions au quotidien pour maintenir un réseau sain et fiable, face à différents types de menaces. Dans un second temps, je présenterais à quel point la sécurité des données est un enjeu majeur, ainsi que la capacité d'un SI à pouvoir s'adapter en toute circonstances.

I. La sécurisation des installations

a) Les menaces internes

Certains éléments de sécurité ont déjà été évoqués durant les deux premières activités. En effet, mes actions de maintenance du parc et d'administration du réseau doivent constamment être pensées en incluant cette notion.

Toutefois, pour être efficace, il faut savoir contre quoi je dois protéger le service d'informations. Je les range en deux catégories : les dangers internes et les dangers externes.

Préventions contre les évènements exceptionnels

Il faut toujours avoir à l'esprit que le SI s'inclut dans un environnement dont on ne maîtrise pas toujours les paramètres.

La meilleure méthode pour contrôler ses variables et d'anticiper les problèmes qu'elles peuvent causer :

- Le courant électrique :
 - Tout le matériel est relié au réseau électrique du bâtiment dans lequel il se trouve.
Les plus grosses structures ont plusieurs compteurs
 - Les risques :
 - _ Surtensions qui consiste à une élévation, supérieure à la normale, de la différence de potentiel appliquée à un appareil
 - _ Sous-tension qui consiste à une diminution, inférieure à la normale, de la différence de potentiel appliquée à un appareil
 - _ Pannes de courant qui consiste en une absence totale de distribution d'électricité
 - Les causes :
 - _ Problèmes sur le réseau de distribution
 - _ La foudre qui tombe à proximité
 - _ Un compteur qui disjoncte
 - La solution appliquée est l'utilisation d'un onduleur
 - _ L'onduleur est un appareil qui transforme du courant continu en courant alternatif
 - _ Les avantages :
 - _ Couvre tous les risques évoqués simultanément.
 - _ Facilité d'installation : il s'installe entre les prises électriques et les appareils à protéger
 - _ Les inconvénients :
 - _ Une solution trop couteuse pour couvrir l'intégralité des bâtiments.

Dans ces conditions, le choix de ne couvrir que les locaux techniques informatiques s'impose pour moi. Le plus important étant de protéger les équipements réseaux essentiels.

_ Ne permet que très peu d'autonomie en fonction de la batterie choisie, elle-même très couteuse.

Là encore, il me paraît important de trouver le meilleur compromis possible. La disponibilités des fichiers n'étant pas nécessaire, le plus important pour moi est de disposer de quelques dizaines de minutes afin de pouvoir éteindre « proprement » les appareils. Aussi, pour connaître la puissance idéale pour 10 minutes d'autonomie environ, j'ajoute les puissances en Watts de tous les appareils à protéger. Je multiplie ensuite ce résultat par 1.6. Ça me donne la puissance en Volt-ampère (V.A)

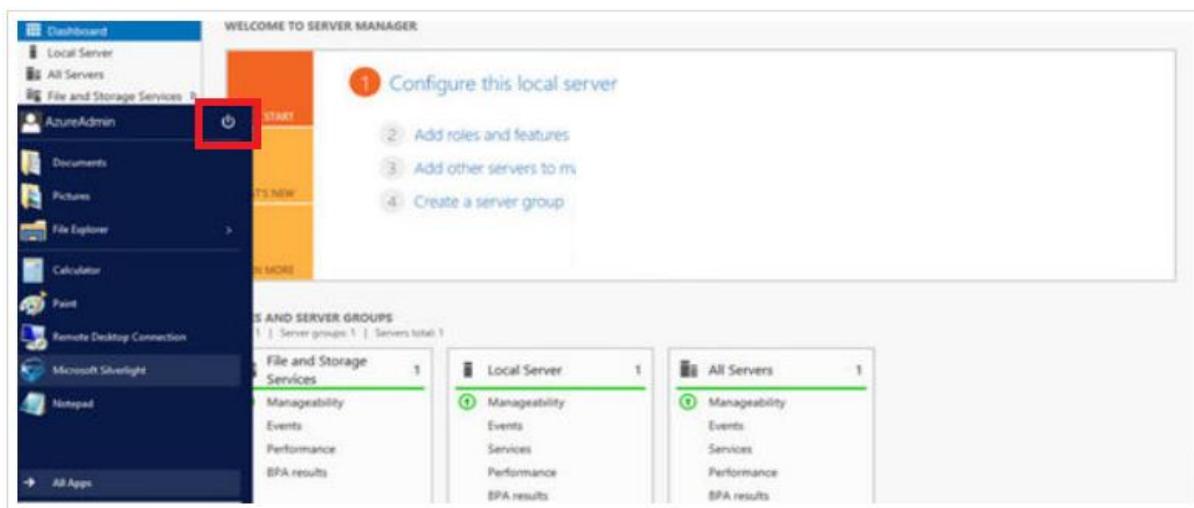
_ Inefficace si la coupure à lieu un soir ou durant le weekend, du fait de mon absence

➤ Mes actions :

_ Si je suis dans les locaux, je branche un écran, clavier et souris aux appareils et je les éteins par le biais de leur menu d'extinction.

_ Si je suis sur un site distant et que l'on m'a prévenu à temps, je fais de même par le biais de la prise en main à distance.

Par exemple, pour les serveurs Windows, je vais cliquer sur l'icône Windows, puis sur le bouton d'alimentation en haut du menu apparu et enfin sur « arrêter ».



Le but étant que toute modification soit bien enregistrée et éviter que le système soit coupé au milieu d'une tâche, ce qui pourrait entraîner un échec critique au redémarrage.

_ En ce qui concerne les ordinateurs des employés, j'effectue de la prévention en rappelant quelques bonnes pratiques :

 _ Enregistrer régulièrement leurs travaux

 _ Privilégier l'espace de stockage mis à leur disposition sur le réseau.

Ainsi, ils éviteront au maximum les pertes liées à une extinction trop brutale ou une panne critique de leur appareil.

- L'atmosphère de la salle serveur :

 ➤ La température :

_ Une température trop élevée de la pièce va entraîner une surchauffe des systèmes puis une casse matérielle.

_ Les causes :

- _ Concentration de matériels fonctionnant en continu 24H/24H, 7j/7j
- _ Températures extérieures élevées
- _ L'idéal est d'avoir une température comprise entre 18 et 27°C
- _ Régulée par un climatiseur, réglé pour maintenir la température autour des 23°C
Je trouve que c'est un bon compromis car il faut tenir compte d'éventuelles variations de températures et ainsi se laisser une petite marge. De plus, plus il ne faut pas trop descendre en température, au risque de gaspiller de l'énergie.
- L'humidité :
- _ Celle-ci peut provoquer des dysfonctionnements des appareils dans lesquels elle se serait introduite
- _ Un air trop sec crée des décharges électrostatiques.
 - _ *C'est un passage de courant entre deux objets possédants des potentiels électriques différents.*
 - _ Ca abime les composants
- _ Les causes :
 - _ Air extérieur très humide ou trop sec
 - _ Fuite d'eau dans une salle adjacente
 - _ Fuite du climatiseur
- _ L'idéal est d'avoir un taux d'humidité compris entre 40 et 60 % d'humidité
 - La surveillance
- _ Une sonde est installée dans chaque local informatique :
 - _ Contrôle les deux paramètres de température et d'humidité
 - _ Envoie par mail une alerte lorsque les seuils limites paramétrés sont atteints
 - Mes actions :
- _ Lorsque je reçois un mail, si je suis sur le site :
 - _ J'aère la pièce afin de modifier l'ambiance
 - _ Je vérifie qu'il n'y a pas de présence d'eau
 - _ S'il fait trop chaud, je contacte le prestataire du climatiseur
- _ Lorsque je ne suis pas sur le site :
 - _ Je contacte une personne susceptible d'ouvrir la porte du local
 - _ Me décrire l'ambiance de la pièce, présence de gouttes d'eau visibles
 - _ Je l'informe d'une personne à contacter si besoin
- Départ d'incendie
 - Risques :
- _ Destruction du matériel
- _ Pertes de toutes les données contenues dans ces appareils
 - Les causes :
- _ Un appareil qui a surchauffé
- _ Départ de feu criminel
- Prévention :
- _ Je ne stocke rien dans les locaux informatiques

- _ Présence d'un détecteur de fumée
- _ Présence d'un extincteur à neige carbonique permettant ainsi d'être projetée sans trop abîmer les appareils.

➤ Mes actions :

- _ Si ça sonne et que je suis à proximité, je tente de contenir le départ de flammes avec l'extincteur
- _ Si ça me semble trop dangereux, j'applique le protocole d'évacuation des lieux

Ces mesures de préventions me permettent d'anticiper des problèmes liés à l'environnement intérieur.

Cependant, ces problèmes ne sont pas les plus fréquents. Une, plus importante, menace constamment l'intégralité du système et est la cause de la plupart de mes interventions : les utilisateurs du SI

Prévention contre les actes malveillants

Avec ce terme, j'englobe toute personne qui se connecte d'une manière ou d'une autre à un appareil du réseau. Cela peut venir :

- _ D'un appareil mis à disposition
 - _ D'un appareil personnel qui se connecterait à une des bornes WI-FI
 - _ D'une prise de contrôle à distance
- Préventions à l'encontre des prestataires :
 - Accès au SI par le biais de la prise en main à distance du matériel qu'ils sont censés entretenir :
 - _ Pares-feux
 - _ Automate de prêt RFID
 - _ Proxy Ucopia
 - Le SLA cadenasse les champs d'interventions de ceux-ci :
 - _ Mises à jour du matériel
 - _ Par suite de l'ouverture d'un ticket incident
 - La journalisation des appareils :
 - _ Ceux-ci répertorient les logs aux appareils
 - _ Contiennent des informations permettant de prouver l'intervention d'une personne dont :
 - _ La date
 - _ L'heure
 - _ Le nom d'utilisateur
 - _ L'adresse IP de l'appareil utilisé
 - _ Cela permet également de prouver la faute si un problème surviendrait à la suite d'une intervention
- Préventions à l'encontre du personnel :
 - Accès au SI par le biais des PC mis à leur disposition

- Restrictions des accès avec :
 - _ Les agents n'utilisent que des sessions utilisatrices
 - _ Les connexions aux serveurs requiert le mot de passe administrateur connu que par mon chef et moi même
 - _présentés durant les deux premières activités
 - Les locaux informatiques sont fermés à clé. Seuls les responsables des médiathèques, mon chef et moi-même avons les clés.
 - Seules les prises Ethernets utilisées sont brassées
- Préventions à l'encontre du public :
 - Accès au SI par le biais :
 - _ Des ordinateurs mis à la disposition du public
 - _ Du WIFI
 - _ Dans tous deux cas, aucune identification nominative n'est requise, afin de simplifier l'utilisation du réseau public.
 - Les ordinateurs publics sont tous connectés sur des sessions utilisatrices.
Le public ne peut donc pas installer de logiciel tiers sur les PC.
De plus, le logiciel RebootRestore efface les modifications réalisées sur le système à mon insu, chaque soir.
 - L'accès au serveur public ne peut se faire sans le mot de passe administrateur
 - Seules les prises Ethernets des espaces publics utilisées sont brassées
 - Lors de la configuration du switch, j'ai isolé les ports dédiés aux espaces publics dans un VLAN qui ne communique pas avec les autres.
 - Tous les ordinateurs sont dans le champ de vision d'un bibliothécaire.
Ce qui reste dissuasif, bien qu'ils n'aient pas le droit de regarder ce qui se fait à l'écran
 - J'inspecte régulièrement les ordinateurs et vérifie qu'il n'y a pas une clé USB restante par exemple, qui pourrait contenir un Keylogger par exemple.

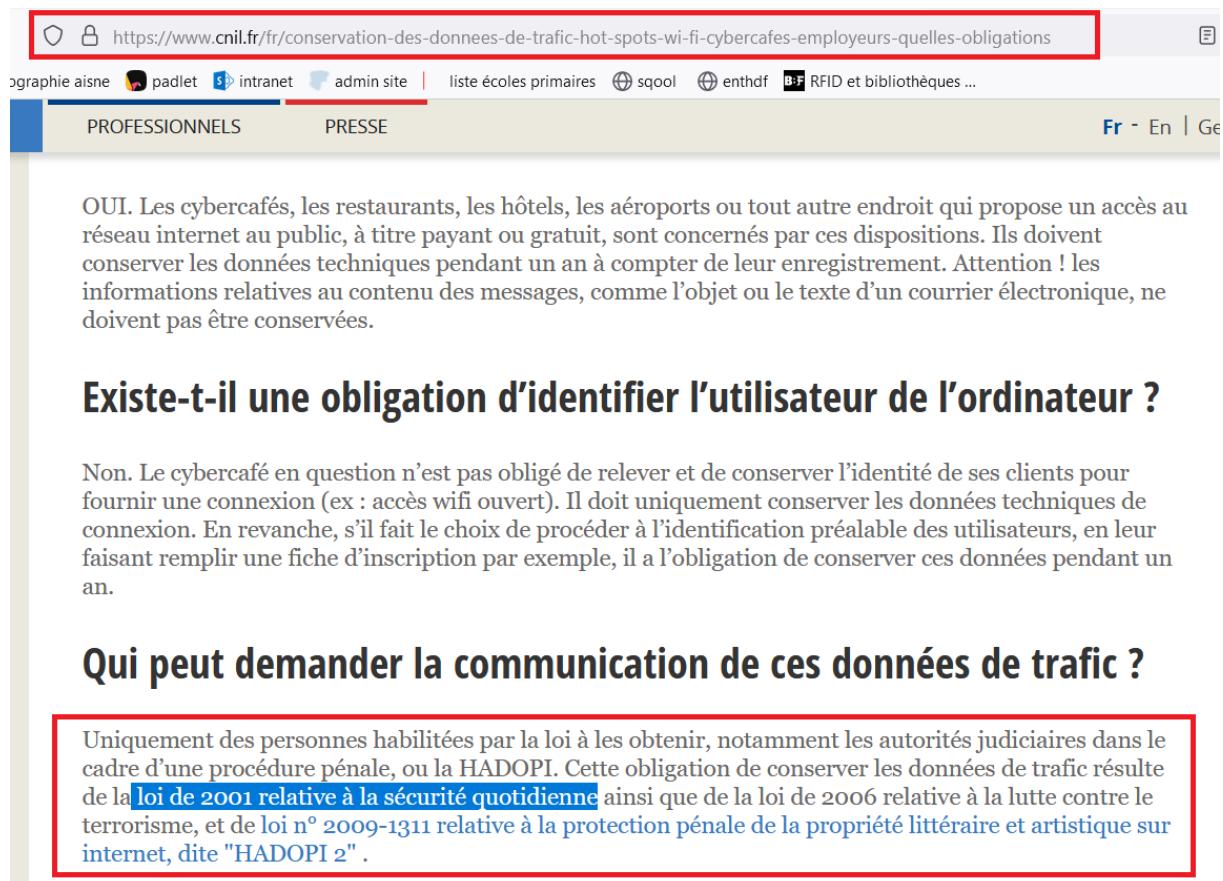
Keylogger : Dispositif informatique qui enregistre les suites de touches tapées sur un clavier

Préventions contre une mauvaise utilisation des accès Internet

Les établissements offrant des accès Internet publics sont tenus de conserver les données relatives aux activités faites à partir de celui-ci

- La législation :
 - Loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne
 - Décret n° 2006-358 du 24 mars 2006 relatif à la conservation des données des communications électroniques

- Loi n° 2009-1311 relative à la protection pénale de la propriété littéraire et artistique sur internet, dite "HADOPI 2"



OUI. Les cybercafés, les restaurants, les hôtels, les aéroports ou tout autre endroit qui propose un accès au réseau internet au public, à titre payant ou gratuit, sont concernés par ces dispositions. Ils doivent conserver les données techniques pendant un an à compter de leur enregistrement. Attention ! les informations relatives au contenu des messages, comme l'objet ou le texte d'un courrier électronique, ne doivent pas être conservées.

Existe-t-il une obligation d'identifier l'utilisateur de l'ordinateur ?

Non. Le cybercafé en question n'est pas obligé de relever et de conserver l'identité de ses clients pour fournir une connexion (ex : accès wifi ouvert). Il doit uniquement conserver les données techniques de connexion. En revanche, s'il fait le choix de procéder à l'identification préalable des utilisateurs, en leur faisant remplir une fiche d'inscription par exemple, il a l'obligation de conserver ces données pendant un an.

Qui peut demander la communication de ces données de trafic ?

Uniquement des personnes habilitées par la loi à les obtenir, notamment les autorités judiciaires dans le cadre d'une procédure pénale, ou la HADOPI. Cette obligation de conserver les données de trafic résulte de la [loi de 2001 relative à la sécurité quotidienne](#) ainsi que de la loi de 2006 relative à la lutte contre le terrorisme, et de loi n° 2009-1311 relative à la protection pénale de la propriété littéraire et artistique sur internet, dite "HADOPI 2".

- Mise en œuvre :
 - Le proxy Ucopia installé dans chacune des médiathèques enregistrent les logs effectués par chaque appareil qui s'est connecté par le biais des VLAN publics.
 - Il n'est pas obligatoire d'avoir le nom de la personne qui a effectué la connexion
 - Les logs sont conservés un an, à partir de la date d'enregistrement
- Si problème :
 - Seul un officier de police peut demander à avoir accès aux logs
 - Si ça se produit, je contacte le prestataire Ucopia qui doit m'envoyer sans délai le fichier à fournir à la police

Avec toutes ces actions, ainsi que celles décrites dans les deux autres activités, je m'assure de pouvoir contenir la plupart des menaces intérieures qui peuvent mettre en péril le système.

Toutefois, ces mesures sont loin d'être suffisantes. En effet, des menaces toutes aussi grandes peuvent également survenir de l'extérieur des murs. J'en ai fait la mauvaise

expérience, un petit peu après ma prise de poste. C'est le propos de la prochaine sous-partie.

b) Exemple de menace externe : le cybercriminel

Dans l'esprit du grand public, c'est sûrement la première idée qui vient en tête. Cette idée étant largement véhiculée par les séries et les films policiers dans lesquels vous avez souvent un super-informaticien capable de s'introduire dans n'importe quel système.

Les types de menaces

Bien que cette image soit très exagérée, il est tout de même imprudent de penser que ça n'arrive qu'aux autres et qu'une bibliothèque n'a rien à offrir à un internaute mal attentionné.

En effet, la bibliothèque emploie du personnel qui sont :

- Des cibles potentielles en vue d'une escroquerie, notamment par mail. Parmi ses escroqueries, je peux citer :
 - Hameçonnage :
[Technique de fraude visant à obtenir des renseignements afin d'usurper l'identité de la victime.](#)
Par exemple, un mail de sa banque qui aurait effacé toutes ses données bancaires par mégarde et qui invite à les redonner en suivant un lien frauduleux.
 - Usurpation d'identité :
La boîte mail de la personne peut être corrompue (son mot de passe a été deviné, par exemple) et peut servir à l'envoi de messages visant à escroquer ses contacts
Il peut lui-même recevoir des mails venant des boîtes de ses contacts corrompues. Il ne se méfiera donc pas des liens ou des pièces jointes.
 - Faux ordre de virement (FOVI) :
[Escroquerie visant à demander la modification des coordonnées bancaires du véritable créancier dont le paiement est ainsi détourné](#)
Cette fraude concerne surtout le personnel administratif
- Des utilisateurs d'un SI dans lequel ils peuvent, malgré eux, aider le cybercriminel à y introduire un logiciel malveillant.
 - Les introductions peuvent se faire par le biais :
 - _ D'un mail, en téléchargeant, par exemple, une pièce jointe frauduleuse
 - _ D'un appareil de stockage corrompu (clé USB, disque dur externe)
 - _ D'un téléphone, relié au PC
 - Les logiciels malveillants (Malwares) peuvent être :
 - _ Des virus : [Logiciels qui ont pour but de perturber le bon fonctionnement d'un système](#)

- _ Des Trojan (cheval de Troie) : Logiciels qui ont pour but de permettre au malfaiteur de s'introduire dans un système.
- _ Des Ransomwares : Logiciels qui ont pour but de prendre en otage les données
- _ Des vers : Logiciels qui ont le même but qu'un virus mais qui ont la particularité d'être capable de se propager à l'intérieur d'un système
- _ Des Spywares (logiciel espion) : Logiciels qui ont pour but de collecter des informations

De plus les bibliothèques, comme n'importe quelle autre entité, possède des données numériques qui sont :

- Exploitables pour les malfaiteurs
Les données que l'on collecte, bien que non sensibles, restent des données personnelles

Donnée personnelle : C'est toute information se rapportant à une personne physique identifiée ou identifiable. Que ça soit directement ou indirectement, avec une information ou le croisement de plusieurs.

Donnée sensible : sont des informations qui révèlent :

- _ L'origine raciale ou ethnique
- _ L'opinion politique, religieuses ou philosophiques
- _ L'orientation sexuelle
- _ L'appartenance syndicale
- _ Les données génétiques et biométriques
- _ Les données concernant la santé

- Nécessaire au fonctionnement du service et qui justifie un rançonnage

Rançonnage : Le fait de prendre en otages des données contre rançon

Le rançonnage peut être fait par le biais :

- Du vol des données : C'est-à-dire qu'elles sont effacées du système d'origine et le malfaiteur se retrouve à être le seul en possession d'une copie
- Du cryptage des données : C'est-à-dire quelles sont toujours sur le système d'origine, mais encodées de manière à être illisible en l'état. Le criminel étant le seul à posséder le logiciel permettant de les déchiffrer

Enfin, les bibliothèques sont dépendantes de leur SI, régulièrement connecté à Internet et donc :

- Sensibles aux attaques par déni de services

DoS attack (Denied of Service attack) est une attaque visant à rendre inutilisable un service, en le saturant par exemple.

- Exposées aux renifleurs et scanners

Sniffer (renifleur) : logiciel permettant de surveiller le trafic entrant et sortant d'un système sur Internet

Scanner : j'évoque ici le logiciel permettant de scanner un réseau afin de connaître les ports ouverts ou connaître son plan d'adressage

- Vulnérables aux attaques de l'homme du milieu

Man-In-The-Middle est un procédé consistant à se positionner entre deux systèmes communiquant et d'y intercepter tous les messages.

Le but peut être de voler les données transmises ou de les modifier avant de les relâcher par exemple.

Ateliers de préventions

Afin de limiter les risques qu'ils n'ouvrent une brèche à leur insu, je mise avant tout sur la formation des agents.

En tant qu'animateur multimédia, j'organise plusieurs fois dans l'année des journées de sensibilisations et de rappels des bonnes pratiques à adopter :

- Ne pas télécharger ou transférer de fichiers personnels depuis le SI professionnel :
 - Privilégier le stockage sur un appareil personnel (téléphone)
 - Utiliser le WIFI public ou ses données mobiles pour les faire transiter depuis Internet

- Ne pas utiliser un appareil de stockage personnel (clé USB, disque dur)
 - Les données professionnelles n'ont pas à être extraites du SI, même dans le cadre du télétravail
 - Privilégier les outils mis à leur disposition par le SI :

_ Ordinateur paramétré pour avoir un accès aux fichiers à distance

_ Matériels de stockage acheté par le SI qui sont formatés à chaque retour

- Ne pas utiliser sa boîte mail personnelle au travail :
 - Elle n'est pas protégée par le logiciel antispam
 - Très souvent utilisée pour renseigner les formulaires d'inscriptions, elle est donc beaucoup plus sujette aux mails frauduleux

- Faire très attention à leurs mots de passe :

- Utiliser un différent pour chaque compte possédé
 - Respecter les règles pour un mot de passe fort :

_ 12 caractères

_ Utilisation de minuscules, majuscules, chiffres et caractères spéciaux

- Ne pas divulguer sa boîte mail professionnel sur Internet, même à des fins utiles dans le cadre de leurs tâches, comme s'inscrire à la newsletter de LivreHebdo. En effet, on n'est pas à l'abri qu'ils se fassent voler leur base de données et que les adresses se retrouvent disponible sur le darkweb

Darkweb : partie du web caché, accessible que par le biais de logiciels et des protocoles spécifiques.

C'est le plus souvent depuis ici que se réalisent les activités illicites.

- Eviter de cliquer sur des liens ou télécharger des pièces jointes qui ne sont pas attendues de votre part. ce, même s'ils proviennent d'une boîte mail de confiance. Celle-ci a très bien pu être corrompue.
- Ne pas répondre à des sollicitations par mail ou SMS demandant des informations personnelles.
- Verrouiller son ordinateur lorsqu'ils s'absentent de leur poste de travail afin d'éviter que quelqu'un n'utilise leur session à leur insu.

En suivant tous ces conseils, ils peuvent déjà limiter les risques qu'une faille proviennent de leurs agissements.

Cependant, je ne peux pas me contenter de ces rappels. Je m'appuie également sur les paramétrages pour limiter les actions en cas d'introduction illicite.

L'apport de la restriction des accès

Plusieurs fois évoquées dans les activités précédentes, les restrictions des accès que j'applique ne limitent pas que les agents. Elles empêchent également la propagation des malwares et bloquent certains accès aux utilisateurs malveillants :

- La session uniquement utilisatrice des postes :
 - Empêche l'installation de logiciels malveillant à l'insu de l'utilisateur
 - Protège le système de modifications pouvant lui nuire
- L'utilisation de sessions utilisatrices uniquement sur le réseau
 - Moi-même, je me connecte à une session utilisatrice, même en cas de d'intervention en tant que technicien
 - Limite de la même manière les possibilités sur les PC que la session utilisatrice des postes
 - Ne permet pas de d'ouvrir d'autres sessions enregistrées sur un poste que la sienne, ni avoir accès aux bureaux des autres ordinateurs du même réseau
 - Ne permet pas d'accès privilégiés aux serveurs
- Limiter les accès aux dossiers et fichiers :
 - Ne permet pas le vol, la modification et la destruction de fichiers auxquels l'agent n'a pas d'accès

- Le morcelage du réseau en VLAN
 - Ne permet pas la communication entre appareils de VLAN différents
 - Limite la propagation d'un malware ainsi que les actions d'un malfaiteur à celui infecté

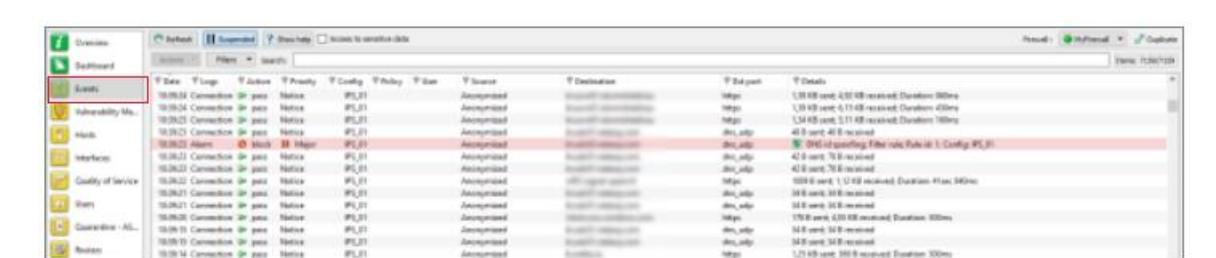
L'apport des logiciels et du matériel

Je m'appuie enfin sur des logiciels pour faire avorter les tentatives de pénétrations ainsi qu'agir très vite en cas de signaux alarmants.

- Les logiciels et le matériel proposent des mises à jour que je réalise très régulièrement :
 - Donnent accès à d'éventuelles nouvelles fonctionnalités
 - Comblent les failles de sécurités
 - Celles des antivirus ajoutent à leur base virale tous les nouveaux virus répertoriés
Base virale : dictionnaire contenant les signatures virales (bout de code d'un virus) des malwares connus.
C'est elle qui permet à l'antivirus de détecter leur présence dans un système
 - L'antivirus :
 - Je programme les antivirus pour qu'ils analysent les systèmes et détectent la présence de programmes malveillants
 - Les résultats sont compilés dans la console de gestion présentée dans l'activité 1. Elle me permet de mettre en quarantaine à distance ces programmes afin qu'ils ne puissent plus nuire.
 - Je les programme également pour qu'ils analysent le contenu de tous les appareils de stockages reliés aux PC
 - Stormshield Real-Time Monitor :
 - Déjà évoqué dans l'activité 2, logiciel de supervision des pare-feux Stormshield

➤ Сенокос

- _ En ouvrant le menu « Events »
Affiche les alertes déclenchées par des évènements normaux



_ L'activité des machines :

_ Evoqué dans l'activité 2, les activités suspectes peuvent être repérées grâce aux débits très importants d'une machine.

Malheureusement toute ces mesures ne protègent pas d'une défaillance. C'est ce qui nous est arrivé en début d'année 2018 qui nous a amené proche d'une catastrophe industrielle.

L'attaque de la nuit du 4 et 5 février 2018

La BMI et ses deux relais ont en fait été victimes d'une cyberattaque

Vosges Matin | 05 févr. 2018 à 15:13 | mis à jour le 05 févr. 2018 à 19:32 – Temps de lecture : 1 min



La BMI ne peut momentanément pas procéder à des prêts de documents suite à une cyberattaque. [Retour à la normale vendredi. Archive E. Th.](#)

- Contexte :

Le 4 au soir, je suis resté plus tardivement pour accueillir un technicien de chez Orange, afin qu'il vienne faire une mise à jour des deux pare-feux.

Normalement les mises à jour sont transparentes, leur redondance permet à ce que le pare-feu qui n'est pas concerné prenne le relais.

Cependant, il y a eu un problème au moment de la prise en charge du pare-feu principal : le secondaire n'a pas pris tout de suite le relais. Il venait d'être mise à jour et peut-être que le technicien est allé trop vite et n'a pas assez attendu que le firewall redémarre tous ses services. Aussi le basculement n'a été effectif qu'au bout de plusieurs dizaines de secondes.

Les conséquences n'ont été visibles que le lendemain matin.

- Détection de l'attaque

Lors de leur prise de poste, les bibliothécaires se sont tous plaints qu'il n'avait plus accès au logiciel qui était encore hébergé en interne à ce moment-là.

Je me suis rendu aussitôt dans la salle serveur. La machine a été allumée. Je me suis alors connecté pour regarder ce qui pouvait clocher avant d'appeler le prestataire. Seulement, la première chose qui s'est affiché, c'est un message me précisant que toutes les données avaient été cryptées et qu'elles seraient décryptées, à la seule condition qu'une rançon de quelques dizaines de milliers d'euros leur soit versée dans les 48 heures. Passé ce délai, la rançon augmenterait.

Le temps de mon inspection sur le serveur d'autres collègues viennent se plaindre que leurs fichiers ne sont plus lisibles. Je constate alors que le malware s'est répandu sur tout le VLAN professionnel

- Mesures d'urgence

- Mon premier réflexe a été d'éteindre ce serveur afin qu'il ne fasse pas plus de dégâts.
- J'ai rassemblé tout le personnel pour expliquer le problème et mes premières directives :

_ J'ai demandé à certains de mes collègues de m'aider à faire le tour des ordinateurs et de débrancher le câble réseau de chacun, ceux des autres VLAN compris.

_ J'ai demandé qu'un collègue parte à Golbey pour faire de même (les autres médiathèques n'étaient pas encore connectées à ce moment-là)

_ Certain a été chargé d'accueillir les collègues qui arrivaient plus tardivement pour leur expliquer les soucis.

- Parallèlement, j'ai appelé le service informatique de la mairie afin qu'ils mettent en suspend nos liens.
- J'ai également appelé mon chef de service qui était initialement de l'après-midi le jour là
- J'ai participé à une réunion de crise avec le cabinet du maire, la direction et mon chef de service, pour :

_ Expliquer la situation ainsi que les circonstances

_ Faire un premier bilan :

_ Toutes les bases de données du logiciel présent sur le serveur étaient perdues, ainsi venait de s'envoler pratiquement 10 ans de travail

_ La base des transactions étant inaccessible, ce sont des milliers de documents empruntés qui sont perdus dans la nature

_ Il n'était pas possible d'assurer une continuité de service, ce qui détériore forcément l'image du service et de sa collectivité

_ Expliquer les démarches afin de régler au mieux la situation.

- Mise en place d'un PRA

PRA : Plan de Reprise d'Activités. C'est un document qui spécifie toutes les étapes qui devront être réalisées afin de relancer un service à l'arrêt.

Jusqu'à ce jour nous n'en avions pas. La réunion a donc permis :

- D'expliquer toutes les étapes nécessaires afin de pouvoir rouvrir les médiathèques dans de bonnes conditions.
- De les faire valider par la direction et par le cabinet.
- D'écrire un document qui est conservé afin d'avoir la marche à suivre en cas de récidive.

- Le rétablissement du service s'est fait en plusieurs phases :

- Accord du cabinet pour maintenir la médiathèque fermée le temps nécessaire :

Nous avons eu de la « chance » que ça soit arrivé un jeudi :

_ Les deux médiathèques d'Epinal et de Golbey n'ouvrent pas les jeudis matin, ni les vendredis matin.

_ En ne fermant que le jeudi après-midi ça me laissait une journée pour rétablir la situation et une demi-journée de tests avant réouverture.

_ Cette courte fermeture n'a eu aucun impact sur l'activité des employés qui se sont adonnés aux tâches de manutentions des documents ou qui ont avancés leurs réunions internes. Une tolérance avait aussi été accordé aux employés qui souhaitaient poser leur journée (hormis mon chef de service et moi-même).

- Rassembler des sauvegardes exploitables des machines

_ Sauvegarde des postes :

_ Présents sur un disque dur externe non connecté au système, donc viable

_ Permettra de remonter une image saine sur tous les postes infectés

_ Toutes les données présentes sur le PC en local et non sauvegardées sur un stockage externe ou sur le dossier en commun sont perdues. De même pour les configurations spécifiques (logiciels particuliers, raccourcis, fond d'écran personnalisé...)

_ Sauvegarde des machines virtuelles :

_ Celles présents sur le serveur professionnel ont été cryptées

_ Celles sauvegardées à Epinal n'ont pas été infectées

_ Aucune modification n'avait été réalisées sur les serveurs depuis un petit moment. Le fait de ne pas avoir de sauvegardes de la veille n'a eu aucun impact

- Analyser tous les postes et identifier ceux à remonter :

_ Tous les postes étaient isolés du réseau depuis le débranchement du câble RJ45

_ Tous les postes professionnels allumés le matin ainsi que les serveurs ont été automatiquement remontés, afin de ne prendre aucun risque

_ Les autres postes ont été scanner par l'antivirus.

Heureusement, le fait de séparer les VLAN a permis à ce que les postes publics, qui s'allument automatiquement à mon arrivé, ne soient pas infectés. De plus, aucun ordinateur éteint au matin n'a présenté le moindre signe de risque. Tout ceci a permis de réduire le travail à réaliser.

➤ Remonter les sauvegardes :

_ Les machines virtuelles ont été effacées puis remontées à partir des sauvegardes faites par Veeam. Ainsi, les nouvelles VM redémarreraient directement avec tous les serveurs déjà configurés.

_ Parallèlement j'ai commencé à remonter l'image pour chaque PC professionnel. J'ai également fait une copie du disque dur des images afin d'en remonter plusieurs en même temps.
J'ai commencé par les PC professionnels des espaces publics afin d'être sûr que ceux nécessaires à la réouverture au public seront opérationnels le lendemain.

_ Le prestataire du SIGB a été contacté en urgence pour réinstaller le serveur SIGB et les bases de données disponibles de leur côté.

➤ Vérifier les nouvelles installations :

- _ Vérifier que les VM démarrent avec la bonne configuration
- _ Vérifier que les serveurs jouent bien leur rôle
- _ Vérifier que le serveur du SIGB redémarre correctement et qu'il se synchronise avec le serveur web
- _ Vérifier que les ordinateurs se reconnectent bien au réseau
- _ Vérifier que le cryptage des données à bien été enrayé sur chacune des machines
- _ Vérifier que Golbey se reconnecte bien au réseau et n'a pas été infecté entre temps
- _ Vérifier que les PC professionnels ont de nouveau accès au SIGB

➤ Rétablir le lien avec la mairie d'Epinal qui a permis de retrouver l'accès au NAS et :

_ D'effectuer une sauvegarde des nouvelles machines

_ De remonter la sauvegarde des dossiers commun et des agents

En effet, les copies que j'avais à la BMI étaient cryptées.

Cependant, je ne les ai volontairement pas récupérés en même temps que les VM car j'aurais perdu beaucoup de temps, du fait du poids total des dossiers. De plus, ils ne sont pas essentiels au redémarrage du service.

Malheureusement les sauvegardes de la veille se sont effectuées après l'infection. Celles-ci n'étant pas viable, je n'ai pu utiliser que celles de l'avant-veille.

➤ Effectuer un bilan du PRA

_ Du fait que ce sont les sauvegardes de l'avant-veille qui ont pu être remontées :

 _ Seules les transactions de la veille n'étaient plus enregistrées.

Ce n'est pas grave pour les retours. C'est plus dommageable pour les documents empruntés qui sont perdus dans la nature.

 _ Les formulaires papier ont permis de reprendre manuellement toutes les inscriptions de la veille. Idem pour les créations et modifications des notices des documents faites la veille.

 _ Seules les créations de documents ou les modifications de la veille n'ont pas pu être récupérées. Cela n'implique que quelques heures de travail de perdues pour certains agents.

 _ Pour la collectivité, ça n'aura occasionné qu'une demi-journée de fermeture au public

En conclusion, je possède tout un arsenal pour tenter de contrer toutes les situations pouvant mettre à mal le système d'information des médiathèques. Que ça vienne de l'intérieur ou de l'extérieur des murs. Que ça vienne d'un évènement exceptionnel ou d'une intervention humaine.

J'ai également appris à mes dépends qu'il ne sera jamais complètement à l'abri. Aussi, qu'il est primordial de penser des PRA en amont, afin d'être le plus réactif possible en cas de crise.

Cependant, protéger les accès au matériel ne suffit pas. En effet, les données sont également en danger lorsqu'elles transitent sur Internet. Il faut également sécuriser leur acheminement. C'est d'autant plus important que l'Europe va renforcer la responsabilités des services, vis-à-vis des données personnelles qu'elles possèdent. Ce sera tout le sujet de la seconde partie.

Il n'est toutefois pas question de l'enfermer dans une bulle hermétique. Dans un monde toujours plus connecté, il faut réussir à l'armer suffisamment afin de pouvoir l'y insérer et lui permettre de s'adapter au maximum de situations imprévues.

II. Insérer le SI dans un monde hostile et changeant

a) Sécuriser ses trafics avec l'extérieur

On l'a vu avec l'attaque de la BMI, que ce qui peut paralyser le service c'est la perte de ses données. Faisant du SIGB le point le plus sensible du système. Cependant l'isoler totalement ne rime à rien. S'il n'est pas exploité, il n'a aucune utilité. De plus, il alimente le site web des bibliothèques qui est un outil devenu indispensable que ce soit pour sa visibilité qu'il permet ou les services au public complémentaires qu'il permet. L'objectif est donc de contrôler les flux entrants et limiter les accès depuis l'extérieur.

IPS, IDS, DMZ

Ces trois acronymes correspondent à des outils du pare-feu permettant des configurations plus subtiles des limitations des flux :

- **IDS (Intrusion Detection System) :**
 - C'est un mécanisme qui a pour but de détecter des trafics potentiellement malveillants à partir d'une norme qui lui aura été définie. *En cas d'anomalie, il lance une alerte.*
 - Se base sur une normalité de fonctionnement qui lui a été défini
 - Il analyse une copie du trafic d'une cible qui peut être :
 - _ Une machine précise
 - _ Un réseau isolé
- **IPS (Intrusion Prevention System) :**
 - Mécanisme qui analyse les données entrantes elles-mêmes et bloquent celles qui lui semblent suspectes
 - De la même manière qu'un antivirus il s'appuie sur une base de signatures pour reconnaître un contenu malveillant
 - Il n'analyse pas une copie du trafic comme l'IDS mais bien le trafic lui-même qui passe à travers lui.
 - Les cibles sont les mêmes que l'IDS

L'IPS à deux défauts :

- *Il peut bloquer du contenu légitime en cas d'erreur d'analyse*
- *Il est vulnérable aux attaques et peut être facilement contourné*

J'aurais donc tendance à plutôt m'appuyer sur l'IDS pour l'analyse du réseau. Je trouve que c'est un bon complément au monitoring de la bande passante.

L'IPS, j'aurais plutôt tendance à le privilégier pour l'analyse de machines spécifiques (comme un serveur de base de données) pour lesquels les trafics sont plus limités.

Pour les machines qui ont des activités plus variées, je préfère m'appuyer sur un antivirus qui ne bloquera que les signatures jugées malveillantes par sa base virale

- **DMZ (DeMilitarized Zone) :**
 - Sous-réseau créé par le pare-feu, accessible depuis Internet mais isolé du reste du réseau (appelé zone de confiance)
 - Son objectif est que si un pirate infiltre la DMZ, il n'ait aucun accès aux autres machines par ce biais-là.
 - Son contexte à la BMI :

Lorsque j'ai pris mes fonctions, le site Internet était hébergé à la BMI.
Or, le site Internet est un service qui a nécessairement besoin d'être accessible en permanence sur Internet. N'importe quel internaute doit pouvoir consulter son contenu, n'importe quand.
C'est donc une importante faille de sécurité pour le réseau internet, d'autant plus dommageable pour nous qu'il communique directement avec le serveur SIGB. Celui-ci lui fournissant la plupart de ses informations (comptes lecteurs, catalogue des documents).

La DMZ avait donc pour but d'empêcher tous les trafics entrant sur le serveur SIGB depuis le serveur web.
 - La DMZ disparaîtra avec la suppression du serveur web de la BMI.
En effet, une fois basculé sur le logiciel SaaS, je n'ai plus eu besoin d'héberger le site web localement.

Le fait de ne plus héberger le SIGB a été un véritable soulagement.

En effet, l'intégrité du serveur est maintenant déléguée aux sous-traitants de notre fournisseur SIGB. De plus, ça nous a permis de refermer beaucoup de portes d'entrées au réseau depuis l'extérieur, que ça soit avec la suppression du serveur web ou la backdoor du fournisseur SIGB.

La Backdoor (porte dérobée) est une ouverture dans un logiciel permettant à celui qui l'a installé de s'y introduire par la suite.

Dans mon cas, elle était connue et légitime. Le prestataire SIGB faisait des sauvegardes de nos bases de données ainsi que des mises à jour du serveur et du logiciel à distance.

Ça reste cependant une grosse faille de sécurité car ça veut dire faire confiance en l'entreprise. Or elle peut elle-même se faire pirater ou avoir un employé avec de mauvaises intentions.

C'est un procédé que je n'utiliserais que dans des cas très spécifiques, lorsque je suis certain de ne pas pouvoir réaliser certaines tâches moi-même. De plus son utilisation devra être spécifiée et limitée par le contrat signé avec le prestataire.

Le Cryptage

Malgré tout, la BMI reste responsable des données personnelles qui lui ont été confiées par ses lecteurs.

De plus, la nouvelle version du SIGB pose nouvelles problématiques :

_ Comment sécuriser des données qui transitent sur de grandes proportions de réseaux sur lesquels je n'ai pas la main ?

_ Comment protéger l'intégrité de données qui pourront être traitées par des terminaux nomades ou n'appartenant pas au service ?

Je ne peux pas garantir qu'il n'y aura pas un vol ou un détournement de celles-ci. En revanche, je peux faire en sorte que si ça se produit, elles ne seront pas exploitables. Pour se faire, je m'appuie sur la technique du cryptage (ou chiffrement).

Cryptage : procédé consistant à rendre incompréhensible un message à quiconque ne possède pas la clé pour le déchiffrer.

J'applique plusieurs moyens pour le mettre en place, en fonction de la situation :

- HTTPS

La première chose à sécuriser est la transmission entre le serveur et les clients qui le sollicite.

➤ Plusieurs cas de figure à ses sollicitations :

_ Le bibliothécaire ou le lecteur qui se connecte à son compte professionnel depuis l'un des postes des bibliothèques

_ Ce même bibliothécaire depuis un terminal qui lui appartient personnellement

_ Le lecteur qui se connecte à son compte personnel depuis chez lui

➤ Des données personnelles transitent :

_ Identifiants et mot de passe du compte

_ données personnelles du lecteur au moment de créer ou modifier son compte

➤ Mise en place du protocole HTTPS

_ [HTTPS \(HyperText Transfer Protocol Secure\)](#). C'est la version sécurisée du protocole HTTP qui est le protocole qui permet l'affichage des pages web par le biais d'un navigateur Internet (Mozilla Firefox ou Edge, par exemple)

_ Son principe de fonctionnement :

 _ [Chiffrement asymétrique](#) : Chiffrement qui requiert l'utilisation de 2 clés : une publique et une privée

 _ Au moment de la demande de connexion du navigateur au serveur, celui-ci fourni au navigateur son certificat afin de prouver qu'il est reconnu comme site de confiance, ainsi que sa clé publique.

[Clé publique](#) : c'est la clé qui sert à déchiffrer les données transmises.

Elle est distribuée à tous les systèmes qui en font ma demande.

 _ Le serveur chiffre, à l'aide de sa clé privée, les données relatives aux requêtes du navigateur.

[Clé privée](#) : clé qui sert au chiffrement des données.

Le serveur est le seul à la posséder, garantissant que c'est bien de lui que viennent les informations.

_ Le navigateur déchiffre les données et affiche les informations demandées par l'utilisateur.

_ Le certificat :

_ Fichier attribué par une autorité compétente et reconnue de confiance.

Également appelé certificat SSL/TLS (Secure Sockets Layer / Transport Layer Security) qui sont les deux protocoles utilisés par le HTTPS pour sécuriser ses transmissions.

_ Le site des bibliothèques étant un sous domaine de la communauté d'agglomération, il est géré par le service informatique de la ville d'Epinal.

Celui-ci me le transmet afin que je puisse à mon tour le fournir au prestataire SIGB qui l'intégrera au module dédié.

_ Parmi les informations que l'on y retrouve, on peut voir l'autorité émettrice ou le chiffrement utilisé, le RSA (Rivest, Shamir, Adleman) pour mon cas.

_ A une date de fin de validité.

Mon rôle, vis-à-vis de ça, est de l'anticipé en sollicitant le service informatique quelques jours avant la date fatidique.

Sinon je risque que le site soit rejeté par les navigateurs. De plus, ça peut amener à une perte de confiance des lecteurs par rapport au service.

- TLS/SSL

Un problème s'est posé lors du passage du site en HTTPS :

- Les platines ne communiquaient plus avec le SIGB
- Après ouverture de tickets aux prestataire SIGB et RFID, on m'a expliqué que le web service de Nedap n'est prévu que pour communiquer en HTTP.
- Le prestataire RFID m'a expliqué comment y remédier, en installant un logiciel appelé Stunnel.

C'est un logiciel libre qui crée des tunnels chiffrés TLS/SSL (les mêmes protocoles que ceux utilisée par les connexions HTTPS) à des services qui ne les possèdent nativement.

➢ Pour l'installer :

_ Lors de son installation il demandera d'indiquer : le pays, la ville, l'organisation, le service et la localisation sur le PC. Je réponds alors : FR, Epinal, BMI, informatique, localhost (pour indiquer qu'il est installé en local sur la machine).

_ Une fois installé, apparaît une icône dans la barre de notifications. J'effectue un clic droit dessus et je sélectionne le menu « Edit configuration ». Apparaît alors le fichier de configuration. Aux lignes, 117, 118, 119, 120 et 124 je supprime le point-virgule du début de ligne. J'enregistre le fichier et je relance le programme.

```

[https]
accept = 443
connect = 80
cert = stunnel.com
-----
TIMEOUTclose = 0

116 ; TLS front-end to a web server
117 [https]
118 accept = 443
119 connect = 80
120 cert = stunnel.pem
121 ; "TIMEOUTclose = 0" is a workaround for a design flaw in Microsoft SChannel
122 ; Microsoft implementations do not use TLS close-notify alert and thus they
123 ; are vulnerable to truncation attacks
124 TIMEOUTclose = 0
125

```

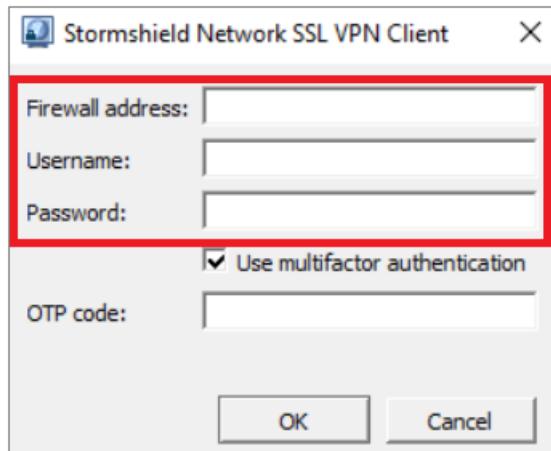
- Une fois ce dernier activé, la connexion entre les platines et le SIGB a été rétablie.
- VPN

En plus du SIGB, il faut également offrir un accès sécurisé au serveur de fichiers.

- Dans deux cas il peut être sollicité depuis l'extérieur des murs d'Epinal :
- _ Soit pour un bibliothécaire présent dans une autre médiathèque du réseau
- _ Soit pour un bibliothécaire depuis l'extérieur, dans le cadre du télétravail.
 - Dans les deux cas, je m'appuie sur les pare-feux Stormshield et leur possibilité de mettre en place des tunnels VPN. Bien que chaque situation nécessite sa propre solution.
 - Le premier cas de figure a été évoqué dans l'activité 2, au moment de l'interconnexion des sites distants.
 - Le second cas de figure est plus complexe du fait que le lien n'est pas établi depuis un réseau de confiance :
 - _ Il peut travailler chez lui
 - _ Il est possible de travailler sur un WIFI Public
 - _ La connexion VPN va s'établir avec un agent nommé Stormshield_Network_SSL_VPN_Client
- Cela nécessite que l'agent travaille avec un des ordinateurs portables que je leur mets à disposition, dans le cadre du télétravail, et sur lesquels j'ai paramétrés l'agent.
- _ Pour le paramétrer :
 - Sur le pare-feu : Je me rends dans le sous-menu Configuration > Utilisateurs > Droits d'accès. Dans l'onglet « Accès par défaut », champ « Politique VPN SSL », je sélectionne « Interdire ». Dans l'onglet « Accès détaillé », je clique sur « Ajouter ». Je sélectionne la personne concernée. Dans la colonne « VPN SSL », je sélectionne « Autoriser ». Enfin, j'active la règle en double-cliquant sur la colonne « état ».

Sur l'ordinateur : Une fois l'installation faite, j'effectue un clic droit sur l'icône apparue dans la zone de notifications. Je clique ensuite sur « connexion automatique ». Je modifie également la clé de registre : HKEY_CURRENT_USER \Software \STORMSHIELD \SSL VPN Client \address.

Grâce à cela, s'affiche automatiquement l'adresse du Firewall à renseigner dans la fenêtre apparue pour établir la connexion. Ainsi, l'utilisateur n'a plus qu'à entrer son nom d'utilisateur et mot de passe que je lui ai fourni avec le PC.

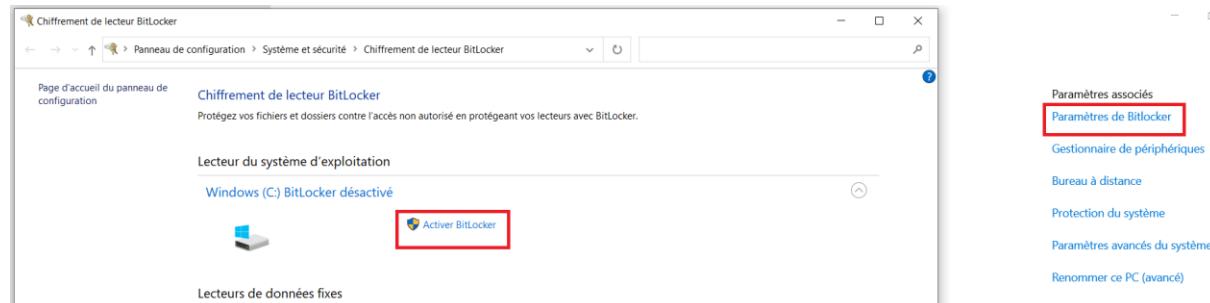


- BitLocker

➤ BitLocker est une solution de chiffrement des disques durs proposé par Microsoft sur ses OS Windows versions Professionnelle, Education et Entreprise.

➤ Pour l'activer, je vais dans le sous-menu « paramètres », « système », « à propos de ». Je clique ensuite à droite, sur « Paramètres de bitlocker » puis sur « activer ».

Pour le mode de déverrouillage, je choisi le mot de passe que j'enregistre sur un fichier. Je conserve ce fichier et je donne le mot de passe à l'agent à qui je confie l'ordinateur. Je trouve ce déverrouillage moins risqué que la clé USB qui peut être perdue par l'agent. Enfin je choisi de chiffrer que « l'espace disque utilisé » qui est permet un chiffrement plus rapide, avec l'option « nouveau mode de chiffrement » qui est celui recommandé par l'assistant de cryptage.



- L'intérêt est que l'ordinateur peut être volé. Ce qui implique que si des données confidentielles y sont conservées, elles deviennent accessibles au voleur.
- De plus, ça va rendre plus compliqué l'utilisation de l'appareil à celui qui a commis le méfait ou sa revente.

Prévention

- On ne peut limiter les risques de pertes ou de vols de données que si les agents respectent les bonnes pratiques d'utilisation
- Aussi j'organise des sessions de formations sur les ordinateurs destinés au télétravail. Je leur explique :
 - Comment démarrer l'ordinateur et décrypter le disque
 - Comment activer le VPN et pour quelle utilisation
 - Les bonnes pratiques à adopter :

_ En déplacement, ne jamais garder à proximité l'ordinateur et les différents mots de passe de connexion (session, VPN et BitLocker)

_ Eviter d'utiliser l'ordinateur dans un espace public au risque :

- _ De se faire voler si on le laisse peu de temps sans surveillance
- _ De se faire subtiliser des informations par un œil indiscret

_ Eviter d'établir une connexion sur Internet avec un compte professionnel sur un WIFI-public au risque que l'identifiant et le mot de passe soit intercepté (SIGB, boîte mail, compte réseaux sociaux de la BMI)

_ Eviter d'utiliser l'ordinateur pour des consultations personnelles afin d'éviter des accidents tels qu'ouvrir un SPAM venant de sa boîte mail personnelle ou télécharger par mégarde un malware.

_ Je leur rappelle que tous les fichiers sauvegardés sur le bureau, ne sont pas synchronisés sur le commun. Il faut donc enregistrer leurs fichiers personnels sur un autre support de secours.

Redondance des données

- La redondance des données est le fait de dupliquer des données sur un autre support.

Un des buts est de garantir un accès aux données, lorsque le support principal devient inaccessible. Cela nécessite une synchronisation des différents supports.

Lors de l'attaque de la BMI, la fermeture au public aurait pu être évitée si le serveur avait eu une réplication.

Ça aussi été un argument au moment du choix du passage au SaaS. En effet, OVH offre la possibilité de louer un second serveur, dans un autre local que celui qui héberge le serveur principal. Bien que cela ait un coût non négligeable, il est apparu nécessaire après l'incendie qui a touché le local d'OVH de Strasbourg et qui a paralysé plusieurs services publics plusieurs jours.

- Depuis, tous les éléments critiques d'Epinal sont doublés :
 - Les pares-feux : Lorsque le principal connaît une défaillance, le second prend le relais
 - Les Boxes Internet : Si une des deux perdent sa connexion, l'autre redistribue toute sa bande passante pour compenser.

Lorsque les deux fonctionnent, elles se partagent les connexions afin de pouvoir offrir plus de bandes passantes. On est ici dans une démarche de haute disponibilité

Haute disponibilité : démarche qui garantit une accessibilité au service de tous les instants avec un degré de performance satisfaisant.

- Le serveur du VLAN professionnel à une réPLICATION sur le second Hyperviseur qui prend le relais en cas de défaillance de la VM principale ou du premier Hyperviseur.
- Les machines sont réparties sur 3 switches, garantissant que toutes les machines ne soient pas impactées en même temps si l'un d'eux viennent à tomber. Et pour celles impactées, il me suffit de les rebrancher sur un des deux autres switches opérationnels pour qu'elles retrouvent leur connexion.
- Les fichiers des agents sont présents sur 3 jeux de données. Ça permet de récupérer un fichier ou un jeu complet si celui qui est exploitée vient à subir une modification non voulue ou malveillante.
- Le RAID 50 du NAS permet de tolérer la panne d'un des disques durs.
- Les appareils tels que les pares-feux, le proxy ou les Hyperviseurs ont également des composants doublés tels que la carte réseau ou l'alimentation afin de permettre une certaine tolérance aux pannes de ceux-ci.

Tous les autres éléments non-cités ne sont pas nécessaire au bon fonctionnement du service. Leur panne n'entrainera pas un arrêt total du service mais simplement une dégradation de celui-ci. Le tout est de trouver un juste équilibre entre la sécurité et les coûts.

PCA

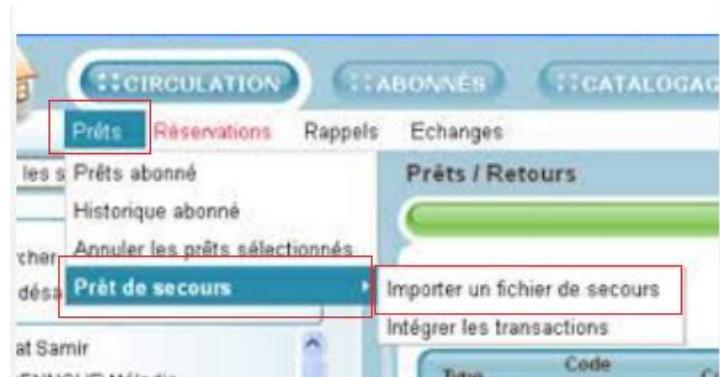
Cette haute disponibilité est également nécessaire dans le cadre des PCA.

- PCA (Plan de Continuité d'Activités) sont des plans de secours pour permettre au service de fonctionner malgré la défaillance de tout ou une partie du système.
- Exemple de PCA, lors de la panne d'Internet
 - Très préjudiciable, du fait que le logiciel SIGB n'est plus accessible
 - Mise en place du prêt secouru :

_ Installation d'un module dédié fourni par le prestataire SIGB :

- _ Un petit logiciel qui s'installe sur les machines

- _ Crée en local des fichiers .txt, un pour le prêt, un pour le retour
- _ Inventories la liste des documents rendus ainsi que la liste des documents empruntés accompagné du numéro de carte du lecteur.
- _ Une fois Internet revenu, il suffit de synchroniser ces fichiers avec le SIGB



- _ Pour que les platines RFID puissent lire et écrire en local, il faut également démarrer un module installé sur chaque machine : BiblioCheck4Lite. Celui-ci prend le relais du webservice inefficace.
- Il permet également d'utiliser les appareils de lecture RFID reliés en USB.

- _ Ce PCA permet donc de maintenir les services essentiels au public à savoir :
 - _ Le prêt de documents
 - _ Le retour des documents
 - _ Les inscriptions qui sont réalisés par papier
- _ Toutefois nous sommes en mode dégradé puisqu'il n'est plus possible :
 - _ De consulter le catalogue des bibliothèques
 - _ De consulter les comptes lecteurs
 - _ De générer des numéros de compte pour les nouvelles inscriptions et donc d'encoder leur carte le jour de l'inscription.
 - _ D'assurer le service de mise à disposition d'une connexion Internet gratuite

Ces pratiques viennent donc compléter les protections des accès aux réseaux, en sécurisant l'acheminement des données. Soit par le biais du cryptage pour éviter l'interception et la falsification des échanges. Soit par le biais de la haute disponibilité pour rendre ses « routes » plus fiables.

Tous ces dispositifs sont indispensables au bon fonctionnement du SI et à la protection des données, notamment celles concernant nos abonnés. Cette protection qui est devenue obligatoire en 2018 avec l'adoption de la loi RGPD par l'Union Européenne.

Aussi le SI doit pouvoir s'adapter à de nouvelles contraintes comme celles-ci. C'est le propos de la dernière sous-partie.

b) L'adapter aux situations nouvelles

La première chose à laquelle le SI doit pouvoir s'adapter, est à l'évolution de la législation.

En 2018, une nouvelle loi va nous contraindre à revoir nos pratiques vis-à-vis des données personnelles des lecteurs.

La RGPD

RGPD (Règlement Général sur la Protection des Données) est un règlement ratifié par le parlement européen en 2016 et mis en application à partir de mai 2018.

Il a pour objectif d'ériger un cadre légal à la collecte et à l'utilisation des données personnelles des citoyens européens. Il précise tous les droits des utilisateurs concernant leurs données. Enfin, il prévoit tout un panel de sanctions pour l'entreprise ou la collectivité qui ne le respecterait pas.

Il s'inspire très largement d'une loi française de 1978, pionnière en la matière, dite loi « Informatique et Libertés ».

Le règlement implique beaucoup de modifications dans les processus. Aussi, une période de tolérance a été accordée, afin que tout le monde ai le temps de s'adapter. Dans mon cas, la remise aux normes s'est déroulée an plusieurs phases :

- Dans un premier temps, il est obligatoire de déterminé un DPO (Data Protection Officer) :

➤ DPO (Data Protection Officer) est la personne chargée au sein d'une entité, de veiller à ce que celle-ci respecte la RGPD dans tous ses processus.

➤ Ces missions sont :

- Tenir informer tout le personnel de leurs obligations vis-à-vis de la loi
- Contrôler le respect de celle-ci
- Prodiguer des conseils en ce qui concerne les analyses d'impact

Analyse d'impact : étude menée sur un traitement de données susceptible d'engendrer des risques élevés sur les libertés individuelles des personnes concernées.

- Être l'interlocuteur privilégié de l'autorité de contrôle, la CNIL.

CNIL (Commission Nationale de l'Informatique et des Libertés) est une autorité administrative indépendante qui veille au respects des lois régissant les pratiques informatiques en France.

- La Communauté d'Agglomération à décider de prendre en charge sa nomination pour l'intégralité des services de son territoire, qu'ils soient communaux ou intercommunaux.
- Afin de l'aider, des référents ont été également désignés dans chaque service conséquent et communes.

Pour le réseau BMI, la direction a désigné la responsable du secteur patrimonial. S'étant portée volontaire elle cochaient les deux cases primordiales aux yeux de la direction :

- _ Étre à l'aise avec le domaine numérique
- _ Ne pas travailler dans le secteur informatique (c'est pourquoi je ne pouvais pas me proposer).

- A la suite de sa rencontre, il nous a été demandé de cartographier les données récoltées :

- Un groupe de travail a été créé, regroupant un représentant de chaque service (sans forcément être le chef du service) et pour lequel je représente le service informatique et multimédia du réseau.
 - L'objectif est de faire un listing exhaustif de chaque pratique impliquant l'utilisation de données personnels, en précisant :

_ Les personnes qui l'effectue

_ Les outils

_ La finalité du traitement

_ Le types de données récoltées

_ Les destinataires si besoin

- Exemple de traitements effectués par les bibliothécaires :

_ L'inscription des lecteurs par le service accueil et prêt. Ils produisent deux documents pour chaque individu inscrit, un papier et une saisie dans le SIGB.

La finalité est de créer un compte lecteur pour leur permettre d'emprunter les documents. La version papier permet d'avoir leur dossier, s'il y a un problème avec le SIGB.

_ Un fichier d'inscriptions aux événements de type Excel, est tenu par les différents secteurs.

La finalité est de pouvoir contrôler le jour de l'événement que les personnes qui se présente, sont bien celles qui se sont inscrites. Il permet également de remplir les tableaux de statistiques de fréquentation des médiathèques.

_ Un fichier de suggestions d'achats est également tenu par les différents services. Ces suggestions sont nominatives et sont émises par les lecteurs, à l'aide d'un formulaire en ligne notamment.

La finalité est de mettre à disposition les nouveaux achats à ceux qui l'ont suggéré.

_ Les secteurs conservent des traces des personnes et sociétés avec lesquelles ils ont déjà travaillé ou sont en contact.

La finalité est de pouvoir les recontacter si les bibliothécaires veulent renouveler la prestation.

_ Les salariés sont renseignés nominativement dans l'Active Directory, le SIGB et le logiciel de planning.

La finalité est de leur créer un compte nominatif pour chacun de ces outils.

➤ La déclaration des prestataires extérieurs :

J'ai également dû signifier chacun de mes prestataires informatiques et désigner ceux qui peuvent potentiellement avoir un accès à certaines de nos données :

_ Le fournisseur du SIGB ainsi que son sous-traitant pour l'hébergement du logiciel dans lequel est renseigné tous les lecteurs inscrits ainsi que tout le personnel. Le sous-traitant effectue également une copie du serveur afin de nous mettre à disposition une redondance en cas de panne du premier

_ Google pour lequel nous utilisons leur formulaire Google Forms qui enregistre toutes les suggestions d'achats qui sont nominatives. Nous utilisons également l'outil Google Analytics pour les statistiques de fréquentations du site Internet

_ Le fournisseur RFID, qui a un accès aux automates de prêt sur lesquels les lecteurs se connectent avec leur compte nominatif.

_ Le fournisseur des proxys Ucopia, lesquels enregistrent les logs Internet réalisés sur les VLAN publics. Il réalise des sauvegardes de ces fichiers.

_ Le fournisseur des pare-feux, dans lesquels il y a des comptes nominatifs pour les agents ayant un accès VPN. Ils enregistrent également les logs professionnels. De plus, Il réalise des sauvegardes de ces fichiers.

_ La mairie d'Epinal qui a un accès physique à mon NAS ainsi qu'à une des sauvegardes des fichiers cités ci-dessus. C'est également la mairie qui héberge nos boîtes emails.

➤ Les données récoltées :

_ Les noms et prénoms car toutes les inscriptions à la bibliothèque, ainsi qu'aux activités, sont nominatives.

_ L'adresse d'habitation afin de justifier du tarif préférentiel destiné aux habitants de la C.A.E

_ Leur statut socio-professionnel pour profiter d'autres réductions voir de la gratuité.

_ Le numéro de téléphone afin de pouvoir les recontacter plus rapidement s'il venait à y avoir un souci (un document très en retard, une annulation de l'activité à laquelle ils sont inscrit)

_ L'adresse mail pour recevoir nos actualités et des alertes liées à leur compte lecteur (document très en retard, réservation disponible par exemple).

- _ Les logs Internet afin de répondre aux obligations légales
- _ Un numéro d'identifiant propre au réseau de bibliothèques.

➤ Les durées de conservations

_ Les comptes utilisateurs sont conservés le temps de leur abonnement + une année glissante une fois l'abonnement non renouvelée. Cette année glissante sert à ne pas tout recommencer si, par exemple, la personne a simplement oublié de se réabonner à temps. A l'issue de ce délai, seul la fiche du SIGB est supprimée.

_ Les fichiers d'inscriptions aux évènements sont conservés jusqu'à l'établissement des statistiques de fréquentations de l'année concernée.

_ Les formulaires de suggestions sont conservés jusqu'à ce qu'elles soient traitées par les référents achats des bibliothèques.

_ Tous les logs Internet sont conservés durant une année glissante afin de répondre à certaines obligations légales. Une fois l'année écoulée, ils sont supprimés automatiquement par les systèmes.

- Il ressort quelques défaillances dans nos traitements que le DPO nous demande de corriger :

- Supprimer également les formulaires papier correspondantes aux abonnements non renouvelés
- Je remplace le formulaire Google Forms par un formulaire que j'ai créé à partir du module dédié du SIGB

Pour ajouter ce formulaire, j'ouvre le menu contenu. Je clique ensuite sur « ajouter du contenu ». Je clique ensuite sur le type de contenu « Webform ». Je renseigne tous les champs.

Webform est un module permettant de collecter des données et de les soumettre à une application ou un système.

A Weform Node allows webforms to be fully integrated into a website as nodes. ▶ Voir la vidéo

Créer Webform

Titre *

Introduction

Body (Modifier le résumé)

- Je remplace Google Analytics par la création d'un compte sur la plateforme Matomo Analytics, préconisé par la CNIL
Pour intégrer ce compte au site Internet, je suis allé dans le menu configuration du site Internet. De là j'ai ouvert le module dédié que j'ai demandé au prestataire d'intégré au préalable. J'ai renseigné l'URL de mon compte Matomo.

PARAMÈTRES GÉNÉRAUX

Matomo site ID *

10

The user account number is unique to the websites domain. Click the **Settings** link in your Matomo account, then the **Websites** tab and enter the appropriate site ID into this field.

Matomo HTTP URL *

https://matomo.bmi.fr/

The URL to your Matomo base directory. Example: "http://www.example.com/matomo/".

Matomo HTTPS URL

https://matomo.bmi.fr/

The URL to your Matomo base directory with SSL certificate installed. Required if you track a SSL enabled website. Example: "https://www.example.com/matomo/".

Portée du suivi

ENREGISTRER LA CONFIGURATION

- Les fichiers contenant les personnes ayant participées aux animations ne peuvent plus être conservés une fois l'atelier passé.
Pour les statistiques, j'ai créé un document partagé dans lequel est simplement noté le nombre de participants de manière anonymisé.
- Je mets aux normes la gestion des cookies :

- Pour cela, j'ouvre le menu « configurations » et j'ouvre le module « EU cookies compliance »
- Le choix des cookies par les internautes est maintenant de type opt-in.

Opt-in signifie que le choix d'acceptation n'est plus sélectionné par défaut. C'est à l'internaute de cliquer sur le bouton d'acceptation

- Les cookies sont segmentés
- Un texte explicite la finalité de leur utilisation

The screenshot shows the Joomla administrator interface. At the top, there's a blue header bar with various tabs like 'Gérer', 'Raccourcis', and 'Configuration'. The 'Configuration' tab is highlighted with a red box. Below the header, there's a section titled 'CONSENT FOR PROCESSING OF PERSONAL INFORMATION'. It contains a paragraph about the GDPR and several radio button options for 'Consent method'. One option, 'Opt-in with categories. Let visitors choose which cookie categories they want to opt-in for (GDPR compliant.)', is selected and highlighted with a red box.

- J'effectue des ateliers de sensibilisation au personnel
 - Ça les concerne directement en tant que professionnel manipulant des données personnelles mais aussi en tant que citoyen européen, concerné par cette mesure de protection.
 - Je rappelle ce qu'est une donnée personnelle :

_ Je présente des exemples de données qui permettent d'authentifier directement (nom, prénom) et indirectement (numéro d'abonné, numéro de téléphone) une personne.

_ Cette partie leur permet d'identifier les données qu'ils manipulent au quotidien.

- Je défini ce qu'est un traitement

_ Les traitements de données sont tous types d'opérations effectués sur des informations.

_ Je précise qu'un traitement n'est pas nécessairement informatique

_ Je présente les bases légales de traitement autorisées par la RGPD.

- _ L'intérêt vital de la personne
- _ L'intérêt public
- _ La nécessité contractuelle

- _ Le respect d'obligations légales
 - _ Le consentement non-ambigu de la personne
 - _ L'intérêt légitime du responsable de traitement
- _ Je les fais ainsi réfléchir sur leurs pratiques au quotidien, lorsqu'ils inscrivent une personne, effectuent une recherche sur le compte d'un lecteur ou lorsqu'ils inscrivent des personnes à un évènement. On réfléchit également ensemble sur la légitimité de ces pratiques.

➤ Je présente les droits des personnes vis à vis de leurs données :

- _ Je défini les différents droits :
 - _ Le droit d'accès : connaitre quelles données une entreprise à de nous
 - _ Le droit d'opposition : s'opposer à l'utilisation de nos données
 - _ Le droit à la portabilité : possibilité de récupérer ses données dans un format de fichier permettant l'interopérabilité
 - _ Le droit de rectification : possibilité de faire modifier des données
 - _ Le droit d'effacement : possibilité de demander que toutes ses données soient supprimées des bases de l'entreprise
 - _ Le droit à la limitation : possibilité de demander à l'entreprise de ne plus utiliser ses données durant un laps de temps

_ Nous réfléchissons encore une fois sur nos pratiques :

- _ Sommes-nous en mesure de faire valoir ces droits à nos abonnés ?
- _ Comment leur permettre ?

_ Nous discutons de leurs pratiques en tant que citoyen :

- _ Lorsqu'ils acceptent des conditions générales sans les lire
- _ Lorsqu'ils acceptent les cookies sans consulter les descriptifs
- _ Lorsqu'ils remplissent les formulaires sans se demander quelles données ils sont en train de fournir et pour quels usages

Avec la bonne volonté de tous les employés, nous avons réussi à passer le cap dans les temps impartis.

Toutefois, la loi RGPD n'est qu'un exemple d'un monde en constante évolution, que ça soit les outils, les pratiques ou la législation qui les accompagne.

Il est donc tout aussi importants que les utilisateurs du SI maintiennent leur niveau de compétences, afin de s'adapter aux nouvelles pratiques.

Je me suis donc constitué tout un panel documentaire afin de régulièrement monter en compétences.

Veille et formations

- En tant que fonctionnaire territorial, j'ai le droit à de la formation continu. Celle-ci est en très grande partie dispensée par le **CNFPT (Centre National de la Fonction Publique Territoriale)**. Elle propose, entre autres, tout une gamme de formations sur des concepts clés de la gestion d'un SI

STAGES	OFFRE DE FORMATION CNFPT	STAGES	OFFRE DE FORMATION CNFPT
SPECIALITE: INFORMATIQUE ET SYSTÈMES D'INFORMATION / Sous-spécialité: Architecture, développement et administration des systèmes d'information	L'ORGANISATION DE L'ASSISTANCE AUX UTILISATEURS DES SYSTÈMES D'INFORMATION		
LA VIRTUALISATION DES SYSTÈMES D'INFORMATION : ARCHITECTURE, PROJET ET SÉCURITÉ			
Duree: 1 jour à distance + 2 jours présentels	PUBLIC	Duree: 1 jour à distance + 2 jours présentels	PUBLIC
Niveau: Approfondissement	Responsables de la production et du support, cheffes et chefs de projet informatique.	Niveau: Fondamentaux du métier	Directeurs et directrices des systèmes d'information, responsables informatiques, responsables production et support.
Code stage: SXHOP		Code stage: SXHOP	
TOULOUSE Code IEL: 07SXHOP015 20-21/02/23 Salle de réunion 04 67 81 77 33 DCCITANIE 87 Plataforme en ligne ouverte du 08/02 au 24/02/23	OBJECTIFS Identifier et décrire les enjeux, les solutions et les méthodologies pour la mise en œuvre de la virtualisation des systèmes d'information.	MONTEPELLIER Code IEL: 07SXHOP013 4-5/12/2023 Salle de réunion 04 67 51 77 33 DCCITANIE 87 Plataforme en ligne ouverte du 20/11 au 31/12/23	OBJECTIFS Mettre en place une politique d'assistance aux utilisateurs des outils informatiques au sein de la collectivité.
	CONTENU - définitions de la virtualisation de serveur et de stockage, - concepts et composants de l'architecture technique, - les gains potentiels, - revue des principales solutions du marché (VMWare, MicroSoft, XEN, CITRIX...) et leurs caractéristiques, - l'administration et la sécurité liée à la virtualisation.		CONTENU - les enjeux d'un accompagnement des utilisateurs, - le panorama des principaux logiciels du marché en relation avec ITIL V3, - la gestion des acteurs et de leurs rôles, - le cycle de vie d'un ticket, - les rapports et statistiques (utilisation, exploitation des données recueillies...), - la présentation de l'application service d'assistance aux utilisateurs dans l'outil GLPI.
	MÉTHODES PÉDAGOGIQUES - apports théoriques et cas pratiques, - cette formation fait l'objet d'un temps à distance composé d'un module de e-formation et d'une e-communauté de stage, tous deux accessibles depuis la plateforme numérique d'apprentissage du CNFPT.		MÉTHODES PÉDAGOGIQUES - apports théoriques et études de cas pratiques, - cette formation fait l'objet d'un temps à distance composé d'un module de e-formation et d'une e-communauté de stage, tous deux accessibles depuis la plateforme numérique d'apprentissage du CNFPT.
	PRÉ-REQUIS Connaître les bases des systèmes, réseaux et bases de données. Ce stage appartient à un ou plusieurs itinéraires ou cycles : - AICRT Chargé ou chargée des réseaux et télécommunications		PRÉ-REQUIS Connaissance des systèmes informatiques. Ce stage appartient à un ou plusieurs itinéraires ou cycles : - AICHT Chargé ou chargée des réseaux et télécommunications - ATRPT Responsable production et support des Systèmes d'Information
358			359

- Je me forme également à titre personnel sur à l'aide de MOOC
 - **MOOC (Massive Open Online Course) est un type de cours, en ligne et ouvert à un très grand nombre de participants simultanément.**
 - Avantages :

- Les modules sont consultables gratuitement
- Le mode de fonctionnement s'adapte au rythme de chacun
- L'avancé est sauvegardée
- Met en relation les participants afin qu'ils s'entraident

- Inconvénients :

- _ Il n'y a que très peu de suivi de la part de professeur
- _ Les parcours « formations » sont payants
- _ Les attestations de fin de cours n'a pas le même statut qu'un diplôme de l'éducation nationale
- _ J'utilise ses deux plateformes qui proposent toutes les deux un grand choix de formations informatiques.

_ <https://www.fun-mooc.fr/fr/>

_ <https://openclassrooms.com/fr/>

- Pour cela, je me suis constitué une webographie afin de mettre en place une veille documentaire adaptée :

Evolution de la législation :

<https://www.legifrance.gouv.fr> : c'est le site officiel du gouvernement pour la diffusion des textes de lois et leurs mises en application.

Sécurité informatique :

<https://www.cnil.fr> : créé avec la loi informatique et liberté, c'est l'organisme de référence sur les traitements des données, ainsi que la loi RGPD.

<https://www.ssi.gouv.fr> : agence nationale de sécurité des systèmes d'informations propose régulièrement des alertes concernant des failles de sécurité des systèmes ainsi que la mise à disposition de documents sur les bonnes pratiques à adopter.

<https://www.cybermalveillance.gouv.fr> : c'est un complément à l'ANSSI, qui propose des rapports sur les pièges de l'Internet, des documents rappelant les bonnes pratiques à adopter pour s'en protéger, des kits de communications que j'ai très largement réutilisé lors de mes ateliers de sensibilisation par exemple. Enfin, il est

possible d'y déclarer un acte de cyber malveillance à laquelle on serait victime et de se faire accompagner.

Fonctionnement des systèmes :

<https://support.microsoft.com> : Support officiel de Microsoft. J'y retrouve tous les tutoriels pour toutes les manipulations concernant les différents OS Windows PC et serveurs. J'y retrouve également des aides dans la résolution de certains problèmes (lorsque la référence est indiquée dans le message d'erreur notamment),

<https://www.stormshield.com> : Site officiel de la marque de mes pare-feux. J'y retrouve toute la documentation technique sur les machines ainsi que leurs logiciels.

https://www.zabbix.com/documentation/1.8/fr/manual/about/overview_of_zabbix : Site officiel du logiciel de monitoring que j'exploite. J'y retrouve toute la documentation le concernant

<https://glpi-project.org/fr/glpi-documentation/> : La même chose que Zabbix pour mon logiciel de gestion du patrimoine

- J'ai également la chance de travailler dans un réseau de bibliothèque avec des moyens conséquents. J'ai donc la possibilité de faire acheter et de me constituer une importante bibliographie qui me permet une monter en compétence.

Je m'appuie notamment sur la collection de l'éditeur ENI qui propose de nombreux livres sur les sujets des systèmes et réseaux

The screenshot shows a web browser displaying the ENI website (<https://www.editions-eni.fr>). The URL in the address bar is <https://www.editions-eni.fr/systeme-et-reseau/reseau/notions-fondamentales>. The page title is "Livres et vidéos / Système et réseau / Réseau / Notions fondamentales". On the left, there is a sidebar with a red border containing a navigation menu for various IT topics such as Poste de travail, Windows, Linux, Client léger, Serveur, Réseau, and others. The main content area displays two book entries under the heading "Notions fondamentales". The first book is "Réseaux Informatiques" (Coffret 2 livres) by José DORDOGNE, published on 09/08/2023, with a price of 56,99 €. The second book is "Réseaux informatiques" (Notions fondamentales) by François GRELIER, published on 31/05/2023, with a price of 39,99 €. Both books have an "Ajouter au panier" button below them. The top right corner of the page has a "ENI Blog" button.

En conclusion, je présente donc dans cette activité tous mes acquis dans le domaine de la sécurité informatique :

- _ Je prends part à la protection des données personnelles.
- _ J'interviens dans la préservation de l'identité numérique du service.
- _ Je sécurise les équipements et les usages des utilisateurs.
- _ Je garantie de la disponibilité, de l'intégrité et de la confidentialité aux données.
- _ J'assure la cybersécurité du SI

De plus, ma veille documentaire démontre un peu plus ma capacité à organiser mon développement professionnel.

Conclusion

Au moment de conclure ce livret, je ne cache pas mon soulagement.

En effet, c'est exercice c'est révélé plus fastidieux que ce que je m'étais imaginé.

Tout d'abord, du fait de ma vie personnelle. Je suis salarié à temps complet et père de deux enfants en bas-âge. Il m'était parfois compliqué de dégager suffisamment de temps pour progresser régulièrement. Je me suis retrouvé à devoir mettre plusieurs fois l'écriture de côté, durant plusieurs semaines parfois. Or s'y remettre et retrouver le fil conducteur n'a pas toujours été évident.

L'écriture en elle-même m'a également mis en difficulté. L'organisation des idées dans un plan logique n'est pas représentative de ma manière de réfléchir sur le terrain. Au quotidien, les notions de technique, d'administration et de sécurité s'entremêlent nécessairement. Les dissocier tout en démontrant leurs liens m'a demandé beaucoup d'essais avant d'obtenir un texte qui me convenait.

La dernière difficulté a été que j'ai quitté ce poste depuis plus d'un an et demi maintenant. Les souvenirs étaient encore assez frais. Cependant, je n'ai plus aucun accès au SI, ni aux tutoriels que j'ai écrits à l'époque. J'ai donc dû effectuer des recherches documentaires afin d'illustrer mes propos et pouvoir retranscrire précisément certaines manipulations.

Toutefois, je suis persuadé que ce travail me sera profitable ces prochaines années.

Premièrement, le référentiel du BTS m'a aidé à pointer mes acquis mais également ma marge de progression. Mes recherches documentaires m'ont également aidé à mettre à jour ma veille documentaire.

Deuxièmement, la rédaction m'a obligé à remettre de l'ordre dans mes idées. J'ai pris conscience de certains mécanismes pour lesquels je n'étais pas en mesure d'expliquer à quel rouage j'intervenais.

Dernièrement, cette aventure m'apporte une certaine satisfaction personnelle. Voir qu'à bientôt quarante ans, je suis encore en mesure de fournir un travail intellectuel. Que je suis également encore capable de progresser.

Cette dernière notion est très importante pour moi car je ne veux pas me contenter de mon poste actuellement.

En premier lieu, je souhaite encore progresser dans les catégories de la fonctions publiques. Je suis actuellement catégorie C mais j'espère réussir à passer B voire B+ rapidement. Aussi, ce diplôme m'offrirait une certaine légitimité qu'il me manque à l'égard de certains jurys. De plus, ce livret va me permettre d'améliorer ma présentation orale avec des idées maintenant bien ordonnées.

En deuxième lieu, je ne compte pas m'arrêter à ce BTS, si je venais à l'obtenir. En effet, j'aimerais prétendre à une licence professionnelle dans le domaine de la cybersécurité. J'ai le projet de faire du service qui m'emploie actuellement un service de référence en matière de sécurité informatique pour les plus petites collectivités du département. Ce cursus, m'apporterait de la légitimité auprès du conseil départemental qui est le décideur.

En dernier lieu, j'ai également la chance de travailler pour une très grosse collectivité, qui propose régulièrement des évolutions de postes grâce aux mouvements du personnel. Ce BTS serait un point de départ pour prétendre à un poste plus important que le mien actuellement.

Pour terminer je souhaiterais remercier toutes les personnes qui m'ont permis de prétendre à cette aventure ou qui m'ont accompagné :

- _ Mon chef de service de l'époque, qui m'a octroyé toute sa confiance et qui m'a apporté toutes ses connaissances. Sans ça, je n'aurais pas progressé aussi rapidement, ni eu le passif nécessaire pour rédiger ce livret.
- _ Mon coach d'écriture, qui m'a guidé tout au long, afin de produire un document de qualité. Je le remercie également pour sa patience malgré mes périodes d'inactivités et de doutes.
- _ Ma famille et mes amis qui m'ont soutenus et épaulés à leur manière pour me relancer lorsque je pensais avoir lâché complètement.

Déclaration sur l'honneur

Information sur les risques encourus en cas de fraude

Les services académiques se réservent la possibilité de vérifier l'exactitude de vos déclarations.

En cas de fausses déclarations, l'obtention du diplôme vous sera refusée, et l'administration sera tenue de déposer plainte contre vous.

La loi punit quiconque se rend coupable de fausses déclarations :

"Constitue un faux toute altération frauduleuse de la vérité, de nature à causer un préjudice et accomplie par quelque moyen que ce soit, dans un écrit ou tout autre support d'expression de la pensée qui a pour objet ou qui peut avoir pour effet d'établir la preuve d'un droit ou d'un fait ayant des conséquences juridiques. Le faux et l'usage de faux sont punis de trois ans d'emprisonnement et de 45.000 euros d'amende." (Code pénal, art. 441-1)

"Le fait de se faire délivrer indûment par une administration publique ou par un organisme chargé d'une mission de service public, par quelque moyen frauduleux que ce soit, un document destiné à constater un droit, une identité ou une qualité ou à accorder une autorisation, est puni de deux ans d'emprisonnement et de 30.000 euros d'amende." (Code pénal art. 441-6).

Le plagiat, qui consiste à intégrer dans son travail (copie, dossier...) l'intégralité ou des extraits d'une autre œuvre dont on n'est pas l'auteur, sans mention de la source, est une contrefaçon constitutive d'une fraude, en applications des articles L335-2 et L335-3 du code de la propriété intellectuelle ;

- la substitution d'identité lors du déroulement des épreuves ;
- tout faux et usage de faux d'un document délivré par l'administration (falsification de relevé de notes ou de diplôme, falsification de pièce d'identité...).
- corruption ou tentative de corruption d'un agent de la fonction publique en vue d'obtenir des documents confidentiels. »

Cette liste n'est pas exhaustive.

Deux types de sanction peuvent vous être appliqués

1. Les sanctions administratives

Un candidat suspecté de fraude présentera sa défense lors d'une audition devant une émanation du jury ou par écrit, afin de respecter le principe de la procédure contradictoire. L'éventail des sanctions est variable selon la gravité des faits reprochés et s'étend de l'annulation de l'examen, jusqu'à une interdiction de se présenter à tout examen et concours de l'enseignement technique durant une période maximale de deux ans.

2. Les sanctions pénales

Les fraudes commises dans les examens et les concours publics constituent un délit et sont réprimées par le Code pénal.

Exemples de sanctions pénales possibles :

- la substitution d'identité lors du déroulement des épreuves peut entraîner des sanctions pénales : peine d'emprisonnement et amende pouvant aller jusqu'à 45 000 euros selon les cas.
- l'usurpation d'identité dans un document administratif ou dans un document authentique est punie de 6 mois d'emprisonnement et de 7500 euros d'amende.
- Enfin, tout faux et usage de faux d'un document délivré par l'administration sont punis de 5 ans d'emprisonnement et de 75 000 euros d'amende.

Pour plus d'information, veuillez consulter :

- le Code pénal et notamment les articles 313-1, 313-3, 441-1, 433-19, 441-2
- l'arrêté du 19 mai 1950 relatif aux fraudes aux examens et aux concours de l'enseignement technique.

Je déclare sur l'honneur :

- × Avoir pris connaissance des informations relatives aux fraudes en VAE ;
- × Attester de l'exactitude de toutes les informations figurant dans le présent livret ;
- × Autoriser la communication de mes résultats en termes de validation au Dispositif académique de validation des acquis (DAVA) pour bénéficier d'un conseil post-Jury.

Fait à Crouy, le 31 / 08 / 2023

Nom, prénom : TURCK Julien



RUBRIQUE 7 : Réservé à l'organisme certificateur (ne pas remplir)Dossier reçu le 19/09/2022Dossier complet le 19/09/2022N° d'identifiant 2231495Code du diplôme /Niveau de certification visé, le cas échéant 5Décision de recevabilité : favorable défavorableDate de décision de la recevabilité 21/10/2022Date limite de validité de la recevabilité (le cas échéant) 21/10/2025



Ministère de l'Education nationale
Direction générale de l'enseignement scolaire
VAE- Dossier de validation - Livret 2 - Edition 2018