# Ne pas diffuser

**Ce document doit encore faire l'objet d'une décision du Conseil communal le 26 mars 2020**

**RAPPORT N° 35/2019**
**AU CONSEIL COMMUNAL**

# Renouvellement 2020 de l'infrastructure centrale (serveurs et stockage) de l'informatique de l'administration communale de la Ville de Vevey

**La commission chargée d'étudier le préavis N°35/2019**

# Renouvellement 2020 de l'infrastructure centrale (serveurs et stockage) de l'informatique de l'administration communale de la Ville de Vevey

**s'est réunie le mercredi 11 décembre 2019 de 19h30 à 21h45 à la salle N°6 de l'Hôtel de Ville de Vevey,**

**puis lors d'une seconde séance suite au complément du préavis le 13.02.2020 de 19h à 21h25 (voir présences page 6)**

Conseillers communaux :

- M. Moïn Danaï UDC
- M. Karim El Khalifa VER
- M. Vincent Imhof PLR
- M. Karim Jerbia PS
- M. Martino Rizzello PDC
- M. Clément Tolusso DA
- M. Pascal Molliat (président-rapporteur) VL

Municipalité :

- M. Michel Agnant

Présent pour les services de la ville :

- M. Robert Schneider Chef de service DSI

## Informations préliminaires

Quelques jours avant que la commission ne siège, un commissaire a transmis à la DSI et aux autres commissaires une série de questions relatives au préavis (en annexe I).
Par courriel, M. Schneider a informé la commission de l'impossibilité de répondre à ces questions avant la séance, mais qu'il réunirait un maximum d'informations pour répondre à celles concernant le préavis.

## Introduction

M. Agnant introduit le préavis en soulignant que le matériel en utilisé a atteint sa limite d'âge. L'évolution technologique galopante et la hausse rapide des besoins font qu'une mise à jour est devenue nécessaire.
La préavis 35/2019 demande donc un budget permettant de passer à la dernière technologie, soit une capacité de stockage accrue et une maintenance simplifiée.

M. Schneider indique que le remplacement matériel des serveurs et du stockage se fait régulièrement environ tous les 5 ans. La dernière mise à jour matérielle s'est faite en 2015 (la seconde baie de serveur a en outre été remplacée en 2018). A l'époque, le stockage SSD (disque dur non mécanique) n'avait pas été adopté pour des questions de coût. Actuellement cette technologie est nécessaire, car elle est devenue omniprésente.
En cas de panne, le temps de reprise est actuellement d'environ 3h. Cela serait plus rapide et plus simple à gérer avec le nouveau matériel.

M. Schneider présente l'historique de l'infrastructure centrale informatique de la ville de 1999 à 2019 (en annexe II).

## Questions des commissaires

- Combien de sites physiques de sauvegarde y a-t-il ?

Il y a actuellement deux sites physiques en ville, distants de 400m. Le projet du préavis maintient les deux sites et en crée un nouveau pour servir de « témoin » de synchronisation aux deux autres.

- Est-ce qu'une stratégie de migration de l'ancien vers le nouveau système est établie ?

L'année 2020 est déjà bien remplie pour le DSI avec l'implémentation du central téléphonique. Grâce à l'accompagnement externe prévu, l'implémentation du nouveau matériel pourrait se faire en parallèle de l'utilisation de l'ancien sans problème.

- Pourquoi remplacer après 4 ans et non 5 ans comme prévu et amorti (20% plus tôt)?

Cela a été proposé, car il n'y aura plus d'espace de stockage à court/moyen terme, notamment à cause de la migration vers le nouveau système de courriel Exchange en plus de l'utilisation courante. On espère cette fois-ci ne pas rater un virage technologique comme le passage au SSD en 2015.
Information obtenue par courriel après la commission : l'ajout de 15To de mémoire sur chacune des deux baies pour régler le problème actuel d'espace coûterait environ 35'000 CHF.

- Le contrat de maintenant signé en 2015 se termine fin 2020, y a-t-il un coût de résiliation ?

Non un arrêt de maintenance ne coûte rien, mais on paie les 5 ans.

- Combien coûte la 5$^{e}$ année de maintenance, sachant qu'en principe les 2-3 premières années sont incluses d'office ?

Difficile à dire, car le contrat était négocié sur 5 ans en bloc. M. Schneider propose de fournir la réponse une fois qu'il aura pu chercher. En revanche, une synergie pourrait être trouvée si la même entreprise est sélectionnée pour le projet proposé que pour le contrat de maintenance en cours. Mais sans garantie à cause de la loi sur les marchés publics.
La prochaine demande d'offre sera faite avec 3 ans de maintenance et la 4$^{e}$ et 5$^{e}$ année en option.

- En page 4 du rapport, pouvez-vous détailler la ligne avec 269'000 CHF représentant près de ¾ du montant total demandé ?

Le préavis est basé sur des appels d'offres budgétaires, il s'agit donc d'une enveloppe globale.

- Il est difficile de s'exprimer sur la question sans un minimum de détails, n'est-il pas possible d'avoir plus d'explications ?

Il y a des contraintes liées aux marchés publics. La limite pour rester dans des appels d'offres sur invitation est de 250'000 CHF HT, soit environ 270'000 CHF TTC, d'où le montant proposé pour le préavis. Le DSI est un peu en retard sur les appels d'offres concernant ce projet et il est difficile de donner des détails sans soumissions précises.

+++ Suite à cette réponse, les commissaires manifestent leur incompréhension sur le manque d'anticipation et le côté précipité du préavis générant un flou global sur le projet et les chiffres proposés. +++

- Le chiffre de 269'000 CHF proposé est-il plutôt large ou plutôt serré ?

C'est difficile à dire, on est plutôt dans le haut de la fourchette, mais encore une fois il s'agissait d'un appel d'offres budgétaire donc assez global. Il y a peu d'acteurs sur le marché.

- La ligne à 50'000 CHF correspond-elle à des machines ou à du software ?

Des machines physiques.

- Est-ce qu'il serait possible d'obtenir plus de détails concernant les chiffres ? Peut-être à une date ultérieure ?

Cela n'aurait pas de sens, tout sera accessible après les appels d'offres, une fois le crédit validé.

- Si M. Schneider venait à être absent est-ce que le système serait gérable ?

Oui, car il y a trois personnes qui gèrent l'informatique et qu'il y a beaucoup d'appuis externes.

- Les SSD ne s'usent-ils pas plus rapidement que les disques mécaniques ?

Non, le problème existait au début de cette technologie, mais n'est plus significatif maintenant.

- Est-ce qu'on pourrait externaliser partiellement le hardware ?

Il y aurait un problème de vitesse de transferts (volume total des données environ 40To) et il faudrait trouver un fournisseur.

- Quel serait le prix pour avoir une ligne au débit suffisant pour externaliser ?

Pour une ligne 10 gigas, Swisscom demande 60'000 CHF / an.

- Comment se passent les backups (sauvegardes) ?

On sauvegarde les fichiers 2 fois/jours et un backup complet une fois /semaine de manière incrémentale répartie sur la semaine. Le backup complet prendrait actuellement environ 7h.

- Il y a bien deux baies de sauvegardes actuellement ?

Oui, une récente (2018) et une ancienne (2015) qui est celle qu'il faut changer à court/moyen terme

- Est-ce qu'une externalisation complète de l'infrastructure a été envisagée ?

Non.

- Suite à la commission sur le renouvellement des licences informatiques et du système de courriel de février 2019, un commissaire annonce avoir transmis un courriel d'Infomaniak qui annonçait (en réponse à la question du commissaire) être capable de fournir un service complet d'externalisation (sur territoire suisse) des serveurs et de l'hébergement des courriels pour une commune. Il a transmis ce courriel à l'époque à Mme Leimgruber, M. Rivier et M. Halter. Cette information a-t-elle été transmise à M. Schneider ?

Oui le courriel avait été transmis mais est resté sans suite.

- Vu l'extrait du rapport de préavis 03/2019 de février 2019 ci-dessous, ne semble-t-il pas incohérent de faire exactement l'inverse 10 mois plus tard en proposant de tout renouveler ? A contrario, est-ce que le fait de devoir renouveler l'infrastructure maintenant n'ouvre pas, justement, la porte à l'étude d'une solution externalisée ?

***Extrait du rapport de préavis 03/2019 de février 2019***
*Une solution d'externalisation des boîtes mail a-t-elle été étudiée ?*

> *Non, car l'infrastructure physique utilisée à Vevey est déjà amortie et il serait dommage de tout jeter pour aller vers une autre solution actuellement.*

Aucune solution d'externalisation n'a été étudiée. Cela mettrait en jeu notamment la sécurité de l'information.

Un commissaire commente que les employés communaux utilisent (louent) actuellement des logiciels propriétaires américains (Microsoft, Office…) qui sont donc non sécurisés par essence. Ce n'est pas parce que le programme est hébergé physiquement sur place qu'il est inaccessible, loin de là.

- Les courriels sont gérés intégralement à l'interne actuellement ?

Oui, sur nos serveurs.

- Pourquoi dépasse-t-on de 80'000 CHF le plan des investissements ?

Car le plan des investissements était chiffré sur la base de la technologie précédente et ne prévoyait pas tout ce qui serait nécessaire actuellement.

- Une récente commission s'est penchée sur le réseau téléphonique avec un crédit de 15'000 CHF dévolu au réseau, est-ce qu'on repaie le réseau avec ce préavis ?

Non il ne s'agit pas du même réseau. Le crédit pour le réseau concerné par ce préavis est une somme d'appoint pour les petites mises à jour.

- Quid de la stratégie de sécurité concernant les mots de passe au sein de l'administration ?

Il n'y a actuellement aucune stratégie, car nous sommes en phase de changement de Lotus vers Exchange. Une fois la migration terminée, il sera possible de développer cela.

- M. Danaï a envoyé de multiples questions à M. Schneider quelques jours avant la commission, bien que certaines aient trouvé une réponse suite aux questions des commissaires, serait-il possible d'avoir une réponse à tout ou partie des autres questions concernant le préavis ?

Non, ce sont des questions pointues dont une partie ne concerne pas directement le préavis et qui nécessiteraient trop de temps pour notre petit service. Il y a actuellement d'autres choses prioritaires.

Suite à cela, les commissaires n'ayant plus de question, M. Schneider et M. Agnant sont remerciés pour leur présence et leurs réponses, ils quittent la salle.

## Discussion finale 1ère séance

Les commissaires s'entendent rapidement sur l'aspect « flou » des chiffres avancés ainsi que sur le projet lui-même.

L'absence totale d'alternatives et de réponses aux questions les concernant malgré les interventions lors des commissions précédentes ainsi que les différentes questions posées lors de cette commission pose problème.

L'urgence utilisée comme argument pour avancer le renouvellement de l'infrastructure informatique d'une année via un projet non abouti ne convainc pas. Cette urgence serait plutôt de nature à encourager une intervention ponctuelle et nettement moins onéreuse afin de gagner une année pour étudier réellement les alternatives et proposer une solution tangible.

A l'issu de cette séance les commissaires refusent les conclusions du préavis en assortissant cette sentence du vœu suivant :
**«** La commission émet le vœu que la DSI étudie plusieurs alternatives pour l'externalisation complète ou partielle de l'infrastructure informatique centrale de la Commune de Vevey. »

En apprenant le résultat du vote ainsi que le vœu, la Municipalité décide de reporter la discussion sur le préavis au CC suivant et organise une seconde séance de commission pour tenter de répondre au vœu des commissaires.

**La commission chargée d'étudier le préavis N°35/2019**

# Renouvellement 2020 de l'infrastructure centrale (serveurs et stockage) de l'informatique de l'administration communale de la Ville de Vevey

**S'est réunie suite au complément du préavis lors d'une seconde séance le 13.02.2020 de 19h à 21h25 à la salle N°6 de l'Hôtel de Ville de Vevey**

Conseillers communaux :
- M. Moïn Danaï UDC
- M. Karim El Khalifa VER
- M. Vincent Imhof PLR
- M. Karim Jerbia PS
- M. Martino Rizzello PDC
- M. Pascal Molliat (président-rapporteur) VL

Municipalité :
- Mme Elina Leimgruber
- M. Michel Agnant
- M. Etienne Rivier

Présent pour les services de la ville :
- M. Robert Schneider Chef de service DSI

Expert externe
- M. C. Delattre H+S Communication

## Informations préliminaires

Afin d'appuyer le DSI pour répondre au vœu de la commission, la municipalité a mandaté l'entreprise d'ingénieur conseil H+S Communication.

Quelques jours avant la seconde réunion de la commission, les commissaires reçoivent une présentation PowerPoint complémentaire au préavis qui traite de la question de l'externalisation (en annexe).

## Introduction

M. Agnant introduit cette séance en rappelant la mission du DSI qui est de fournir les outils informatiques appropriés aux autres services de la ville. Le DSI n'a pas pour vocation à faire de la recherche et développement. Il rappelle également que chaque changement nécessite une mise à jour des formations des utilisateurs.

M. Delattre se présente ainsi que l'entreprise pour laquelle il travaille. Il précise que H+S Communication est basée à Vevey, vend ses services d'ingénieur conseil particulièrement dans le domaine de l'informatique et des problématiques d'externalisation et ne représente aucun intérêt privé.
Suite à cela deux présentations sont faites aux commissaires par M. Schneider ; l'une sur les enjeux du préavis et la seconde sur l'étude d'alternatives pour externaliser l'informatique communal.

## Questions des commissaires

- Qu'en est-il de l'externalisation des boîtes de messageries ?

Externaliser que les boîtes de messageries ne règlerait pas le problème des performances des serveurs. Et en l'état il s'agit d'effectuer la migration de Lotus vers Exchange qui sera une messagerie pratique et compatible.

- Les problèmes de ralentissement et de blocage viennent actuellement des sauvegardes quotidiennes des boîtes de messageries ?

Oui Lotus est très gourmand et ne permets pas l'archivage.

- Est-ce qu'externaliser les boîtes de messageries règlerait le problème ?

Cela aiderait mais il s'agit surtout d'effectuer la migration vers Exchange qui permettra l'archivage des courriels. Les courriels ne représentent que 1To de mémoire contre un peu plus de 20To pour l'ensemble du volume des dossiers communaux.

- Où seront stockées les archives de courriel ?

Sur un support non sauvegardé quotidiennement.

- Quand démarrera la migration et combien de temps devrait-elle durer ?

Cela devrait démarrer à la fin du mois de mars avec l'entreprise mandatée pour effectuer le travail. La durée sera d'environ un mois.

- Vu que nos licences exchanges le permettent, ou pourrait externaliser les messageries de manières simples et sans coûts non ?

Oui mais actuellement les serveurs sont en Irlande et aux Pays-Bas. En revanche des data center sont prévus en Suisse d'ici deux ans maximum.

- Sous Exchange, le volume des boîtes de messagerie est limité ?

Oui à 5Go par boîte hors archives, ce qui limitera la problématique des lourdeurs sauvegardes que nous avons actuellement

- On compare des choses incomparables au niveau des coûts. Si les prix d'externalisations sont complets, ceux du maintien à l'interne ne tiennent pas compte des frais annexes, des locaux, du refroidissement, de l'électricité, du personnel nécessaire, etc.

L'une des deux salles informatique héberge aussi la centrale téléphonique donc existerait malgré une externalisation. Pour le reste c'est vrai mais on estime les frais annexes à environ 10% du total (hors charges salariales) ce qui ne changerait pas le résultat : une externalisation resterait plus cher.
Et une externalisation nécessite la mise en place d'un suivi du prestataire au niveau des performances contractuelles. De l'expérience de M. Delattre, il s'agit un gros point à retenir. Des entreprises ayant passé leur structure informatique en externe ont engagé des

gens spécifiquement pour assurer le suivi du/des prestataires tant au niveau technique que légal.

On peut ajouter la problématique des marchés publics : il s'agirait de refaire un appel d'offre tous les 5 ans avec le risque de devoir refaire une migration en cas de changement de prestataire.

- Question à M. Delattre : Que pensez-vous d'externaliser l'infrastructure informatique communal ?

L'externalisation doit entrer dans une stratégie plus globale et surtout externaliser partiellement ne fait pas de sens car cela ne règle pas les problèmes soulevés.
En France, il est interdit par la loi d'externaliser des données publiques et ils envisagent un service de serveurs centralisé mis en place par l'état. Un équivalent suisse serait un serveur cantonal dédié aux Communes. Toutefois cela n'existe pas encore et faire le choix d'externaliser serait inédit et ouvrirait la porte au débat légal. Le système mis en place actuellement fonctionne et est sécurisé. Suivez la communauté des Communes et ne partez pas seul dans cette option qui est à la fois onéreuse, légalement peu claire et techniquement complexe.

- Y'a-t-il une législation en Suisse relative à l'externalisation de données publiques ?

Actuellement il ne semble pas encore mais en UE oui. On ne peut donc pas externaliser des données relatives à des citoyens européens.

Un commissaire rappel que quelle que soit la solution retenue – interne ou externe – les problèmes de sécurité des données liés à l'utilisation de logiciels propriétaires restent les mêmes.

- Quelle est la différence de coûts entre l'option de prendre chaque licence séparément et celle retenue de prendre un paquet contenant toutes les licences pour chaque utilisateur, sachant que pas tout le monde n'utilise tout ?

Il s'agit de la tendance du marché de louer des paquets de licences. La Ville ne loue pas Microsoft 360 mais bien Microsoft 365 E3 qui inclus également le système d'exploitation et d'autres licences nécessaires. L'option de les prendre séparément serait plus cher.

- M. Schneider a articulé un montant de 35'000 CHF pour remplacer la baie de 2015 à titre de mesure temporaire dans le cas où le renouvellement complet est repoussé, serait-ce la seule option ?

Oui car il faut prendre du matériel compatible avec ce qui est installé et qui permet une maintenance adéquate ainsi que le maintien des garanties. De plus cette option ne règle pas le problème des capacités actuelles limitées des serveurs.

Mme Leimgruber prend la parole en conclusion afin de rappeler le côté stratégique et pressant de la demande vis-à-vis du bon fonctionnement de l'administration communale. Elle précise que la porte est ouverte au renouvellement de la réflexion lors de la prochaine mise à jour du matériel prévue aux environ de 2025.

## Vote et vœux

**Au vote final, la commission accepte les conclusions du préavis par 4 oui, 0 non et 2 abstentions.**

**Et émet les vœux suivants à l'unanimité :**

**Vœu 1**: Dans les futurs préavis, faire une séparation claire entre les coûts d'achat des appareils et ceux de maintenance.

**Vœu 2**: La Commune doit se renseigner auprès du Canton sur les bases légales liées à l'externalisation du stockage des données informatiques et/ou des courriels.

**Vœu 3**: Le DSI doit rester attentif aux évolutions techniques et financières liées aux questions d'externalisation, particulièrement en amont du prochain renouvellement matériel.

En conclusion, nous vous prions, Monsieur le Président, Mesdames, Messieurs, de bien vouloir prendre les décisions suivantes :

**LE CONSEIL COMMUNAL DE VEVEY**

**VU** le préavis no 35/2019, du 25 novembre 2019, concernant le renouvellement 2020 de l'infrastructure centrale (serveurs et stockage) de l'informatique de l'administration communale de la Ville de Vevey

**VU** le rapport de la commission chargée d'étudier cet objet, qui a été porté à l'ordre du jour

**d é c i d e**

1. d'allouer à la Municipalité un crédit de Fr.380'000.-- pour financer la mise à niveau de l'infrastructure informatique de l'administration communale ;

2. de financer cette dépense par la trésorerie courante, par prélèvement sur le compte « Dépenses d'investissements » ;

3. d'amortir cette dépense par un amortissement annuel de Fr.76'000.-- pendant 5 ans ;

Le rapporteur,

P. Molliat

Pascal Molliat

# Questions en amont de la commission traitant du préavis n°35/2019 du conseil communal de Vevey

Certaines des questions ci-dessous touchant à des sujets sensibles de la DSI, il est envisageable de signer une NDA (accord de confidentialité) ou de ne pas faire mention de certains éléments de réponse dans le rapport pour garantir le secret de fonction. Ces questions indiqueront « *NDA possible* ».

## Sécurité

1. La sécurité est une problématique importante au vu de la criticité de l'informatique pour le bon fonctionnement de tout organisme en dépendant. **La DSI y est-elle attentive ? Agit-elle de manière proactive, en implémentant par exemple les derniers correctifs de sécurité et « industry best practices » dans des délais adéquats ?**

2. Les ransomwares[1] sont une menace réelle n'épargnant personne. Des multi-nationales comme Maersk en ont fait les frais et même frôlé la catastrophe[2]. Si les grands sont touchés, les petits aussi peuvent l'être. **Quelles mesures sont actuellement en vigueur pour (1) rendre difficiles de telles attaques et (2) minimiser l'impact en cas d'attaque ? S'il y en a, ont-elles été mises à l'épreuve en scénarios de test, et si non, pourquoi ? Quelles seront les mesures futures si elles devaient changer avec la nouvelle infrastructure IT ?** Notez que l'on parle ici de « rendre difficile » et « minimiser » car la sécurité parfaite n'existe pas. *NDA possible*

3. La sécurité peut se faire en défense ou en attaque. Dans le cadre d'une administration communale, et plus généralement un consommateur de technologie, seule la première variante fait sens. Il s'agit des mesures passives et actives ayant pour but (sans être exhaustif) de (1) analyser le trafic Web pour détecter des anomalies, (2) appliquer le principe des « moindres privilèges » lors de la définition des droits d'accès et (3) assurer des copies de données en suffisance et correctement stockées pour permettre un retour en arrière. Comme mesures, on citera entre autres les VLANs[3], IDS/IPS[4], et ACLs[5]. **Quelles mesures passives et actives sont actuellement en vigueur ? Ont-elles été testées en simulation ? Vont-elles changer avec la nouvelle infrastructure IT, et si oui comment ?** *NDA possible*

4. De nombreuses failles matérielles ont touché les processeurs Intel et AMD. Celles-ci n'étant corrigeables qu'avec une refonte du matériel (réalisable par le constructeur uniquement), il faut appliquer des mitigations logicielles pour palier à ces brèches critiques. On citera entre autres Spectre, Meltdown et ZombieLoad 2. **Est-ce que la DSI a choisi des serveurs dont les**

1 Logiciel malveillant verrouillant irréversiblement un système et demandant une rançon en échange de la libération, généralement inutile et ne servant qu'à enrichir les attaquants
2 https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
3 Segmentation d'un réseau Ethernet physique en plusieurs réseaux Ethernet virtuels
4 Inspecteur/analyseur de paquets ou « firewall »
5 Access Control List, définition des droits d'accès dans un système informatique

**processeurs implémentent ces correctifs ? Si non, les systèmes d'exploitations prévus ont-ils toutes les mitigations installées ? Si non, pourquoi et quand cela sera-t-il fait ?** Une liste des serveurs choisis, avec mention détaillée des processeurs (modèle, stepping number, etc.), ainsi qu'un liste des versions de systèmes d'exploitations envisagés sont également souhaitées.

5. La sécurité comprend aussi l'accès physique et virtuel aux composants de l'infrastructure IT. **Quelles mesures sont actuellement en vigueur pour n'autoriser que les personnes habilitées à (1) se rendre dans des locaux techniques, (2) se connecteur aux serveurs avec privilèges administrateur et (3) sécuriser les accès à distance aux serveurs (ex. SSH, RDP) ?** *NDA possible*

6. Un appareil sécuritaire non vérifié équivaut à ne rien avoir du tout. **Afin de déterminer si la sécurité actuelle est suffisante, un audit de sécurité a-t-il été mené récemment ? Si non, des commissaires pourraient-ils avoir un accès accompagné pour mener leurs propres observations ?** A l'issue de ces visites, il serait possible de demander d'implémenter cette thématique dans le projet (et donc son budget) car il est indispensable d'avoir preuves formelles d'une sécurité en ordre. *NDA possible*

7. La cryptographie est un outil crucial pour garantir certaines propriétés désirables, comme la confidentialité de données « au repos » (stockage), en transit (ex. TLS) ou échangées (ex. GPG). **Quels sont les protocoles, logiciels et algorithmes actuellement utilisés pour ces trois cas pratiques ? Qu'est-il prévu avec le nouvelle infrastructure ? Conformément au « principe de Kerckhoffs »[6], est-ce que tous les éléments cryptographique sont ouverts ?**

8. Pour assurer le bon fonctionnement des systèmes internes de communications d'une organisation, il est important d'inciter ses utilisateurs à ne pas employer de moyens externes (par exemple avec des mesures organisationnelles et technologiques). **Quelles mesures la DSI implémente-t-elle pour éviter que les collaborateurs de l'administration communale utilisent des services externes (ex. WhatsApp, Telegram) ?**

## Fiabilité

1. Il est fait mention de SPOF (Single Point Of Failure) pour les baies de stockage. Sachant que la fiabilité d'un système est égale à celle du maillon le plus faible, il faut dessiner l'architecture informatique de sorte à ce que tous les éléments soient hautement disponibles (« high availability ») ou du moins conformes aux attentes. **Quelle est l'architecture actuelle et dans quelle mesure a-t-elle été mise à l'épreuve ? Qu'en est-il avec la nouvelle infrastructure IT ?** Afin de déterminer le degré de redondance prévu, un plan architectural des services (aux niveaux logiques et physiques) est souhaité. *NDA possible*

6 Principe établi par August Kerckhoffs, cryptographe du 19e, selon lequel la sécurité d'un élément ne doit pas résider sur le secret de son architecture mais uniquement sur la robustesse des clefs secrètes. Ce concept est unanimement approuvé par les cryptographes modernes, argumentant que la « sécurité par l'obscurité » n'apporte aucun bénéfice et même des désavantages.

2. Les backups[7] se font selon un cahier de charges définissant quel degré de résilience est souhaité (ex. nombre de backups par tranche horaire, nombre de backups précédents gardés, copies hors-site). **Quelles sont les présentes et futures politiques de backup et DR (« disaster recovery ») ? Ont-elles été testées ? Si oui, quel en fut le résultat ? Si non, pourquoi et quand est-il prévu de le faire ?** Il est crucial d'avoir des backups fiables et testées car l'absence de validation équivaut à un backup à l'aveugle qui n'est par définition pas fiable. *NDA possible*

3. La profondeur d'un backup correspond au nombre de backups précédents qu'un système garde à un instant T, ainsi qu'au nombre de ces backups qui seraient éventuellement stockés en copie sur un système hors-site et en lecture seule. **Combien de quoi contiennent les backups et à quelle profondeur ? Existe-t-il des backups hors-site ? Si non, pourquoi et quand est-il prévu de le faire ?**

4. Les solutions de stockage de données sont nombreuses, chacune avec ses avantages et désavantages suivant les cas d'utilisation que l'on peut rencontrer. On trouve par exemple des solutions à base d'un seul serveur ou d'autres utilisant un « cluster »[8], ou celles qui emploient des cartes contrôleur de disques plutôt que seulement des logiciels pour gérer le matériel. Sachant que :

   - le RAID[9] souffre du « write hole »[10], qu'il soit implémenté en matériel (avec carte contrôleur disque) ou logiciel,
   - l'utilisation de RAID matériel implique qu'une panne de contrôleur nécessite le remplacement par une carte du même modèle (afin de pouvoir rouvrir le volume RAID tel qu'encodé par la précédente carte) et que cette disponibilité est généralement onéreuse et difficile à assurer plus le temps passe,
   - le RAID n'offre ni protection contre la corruption silencieuse de données (ex. bit rot[11]) ni atomicité[12] des transactions en écriture,

   **la DSI a-t-elle choisi des solutions de stockage implémentant les dernières protections contre les problèmes mentionnés ci-dessus ? La DSI a-t-elle étudié l'usage de solutions**

7 Sauvegardes de données, généralement faites sur des serveurs de données dédiés à cette tâche

8 Ensemble d'unités logiques regroupées sous une même unité parente, ici des serveurs fonctionnant ensemble avec un quorum

9 Redundant Array of Inexpensive Disks, technologie permettant de lier plusieurs disques en une unité logique pour palier à certains problèmes de performances et/ou de fiabilité

10 Bug inhérent au RAID qui résulte en une corruption silencieuse des données en cas de panne système ou interruption d'écriture (opérations non-atomiques)

11 Bit rotation, changement incontrôlable de certains bits sur le support de données dû à des événements physiques (ex. rayons cosmiques, dégradation du médium au fil du temps)

12 Propriété garantissant qu'une transaction (généralement de données) s'effectue soit en totalité ou pas du tout, ne laissant ainsi pas un système avec ses composants dans des états contradictoires

**(entièrement logicielles) comme ZFS[13] ou Ceph[14] qui représentent la dernière itération du stockage de données numériques ?**

## Open source

1. Les logiciels libres présentent de nombreux avantages. On citera notamment la transparence vis-à-vis du code (pas de boîte noire, possibilité d'audit par n'importe qui (ex. OpenSSL[15])), la présence d'une communauté globale d'utilisateurs et développeurs plutôt qu'une seule entreprise gérant le tout, ainsi que l'opportunité d'investir l'argent dans autre chose que des licences annuelles et onéreuses. Il y a par exemple les systèmes d'exploitation à base Linux. **La DSI a-t-elle exploré de telles options ? Si oui, lesquelles, et si non, pourquoi ?**

## Planification

1. **Quelle est la durée de vie estimée de la future infrastructure IT ? Quels sont les plans de migration pour cette transition et celle à venir lors du prochain renouvellement ? Les compatibilités entre les différentes systèmes (présents et futurs) ont-elles été prises en compte lors du choix de technologies ou cela a-t-il été déchargé en travaux artificiels de migration ?**

## Divers

1. Il est d'usage d'utiliser de la compression sur les systèmes de stockage de données pour gagner de l'espace en échange de cycles de calcul processeur. Par exemple, ZFS permet d'utiliser différents algorithmes comme LZ4 pour atteindre des ratios intéressants (de l'ordre de 1.5x, selon le type de contenu). **Est-ce que le système prévu emploie de telles mesures ? Si oui, lesquelles, et si non, pourquoi ?**

2. Les solutions de type « cloud », autrement dit de l'hébergement chez un fournisseur externe, permettent d'éliminer (en partie ou en totalité) l'acquisition de certains éléments physiques. Les cas les plus fréquents concernent le stockage de données, les bases de données, ainsi que les serveurs de virtualisation. **La DSI a-t-elle étudié de telles options ? Si oui, lesquelles, et si non, pourquoi ?** Sachant que de tels fournisseurs ont un accès intégral aux ressources louées et que certains états peuvent exercer une surveillance à leur insu suivant l'emplacement géographique de leurs serveurs, on chiffre généralement le contenu avant qu'il soit traité par ces entités externes pour préserver sa confidentialité. De plus, l'usage de services externe rend la DSI dépendante d'un lien réseau ainsi que d'une disponibilité supposément infaillible (ou du moins très haute, selon les SLA[16]) entre elle et ces fournisseurs, sous peine d'être privée de son IT. **Cela a-t-il également été pris en considération dans l'affirmative ?**

---

13 Zettabyte File System, suite logicielle initialement développée par Oracle mais actuellement logiciel libre, garantissant entre autres ce que le RAID ne peut avoir (atomicité, intégrité, snapshots, chiffrement)

14 Stockage de données par cluster, logiciel disponible commercialement et en open-source, notamment employé par le CERN avec plus de 200 petabytes sans perte de données

15 Suite logicielle permettant d'établir des communications sécurisées

16 Service-Level Agreement, accord garantissant la disponibilité d'un certain service (chiffré en pourcentage du temps annuel) fourni par une entité pour une autre

3. Le facteur humain est souvent en cause d'intrusions, même dans les systèmes les plus « sûrs » (ex. Stuxnet). **La DSI a-t-elle mené ou prévoit-elle des cours de sensibilisation à la sécurité informatique pour les collaborateurs de l'administration communale afin d'enseigner les réflexes à avoir face à des cas communs d'ingénierie sociale ? Si non, pourquoi et quand prévoit-elle de le faire ?**

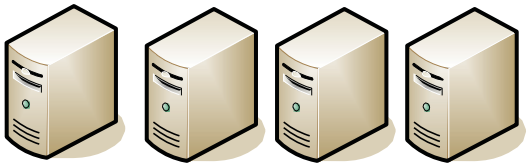
Vevey, le 9 décembre 2019

Moïn Danai

# Evolution de l'informatique « centrale » à Vevey

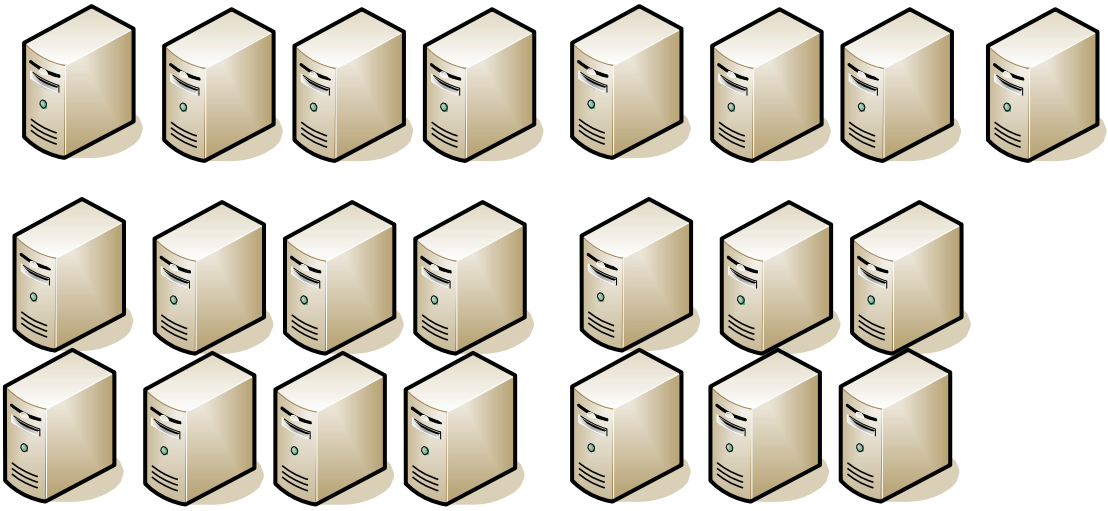
1989 : 1 mini-ordinateur Data General« central »

1999 : 4, puis 5 serveurs PC physiques

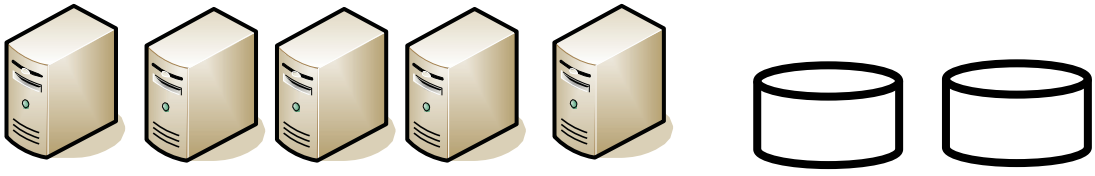


- serveur de fichiers
- serveur base de données Oracle
- serveur de messagerie
- serveur d'impression
- serveur d'applications (Jourap, salaires. etc.)

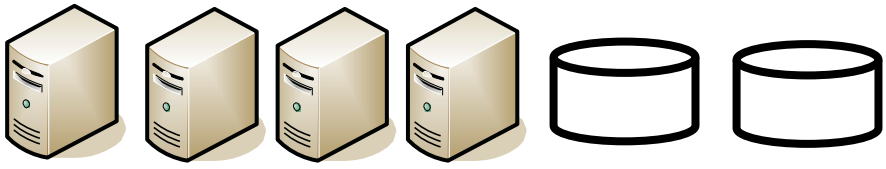
2005 : 15 serveurs physiques et même 22 en 2008, si on compte les PC remplissant une fonction de serveur



2011 : 5 serveurs physiques, mais ~ 30 serveurs virtuels

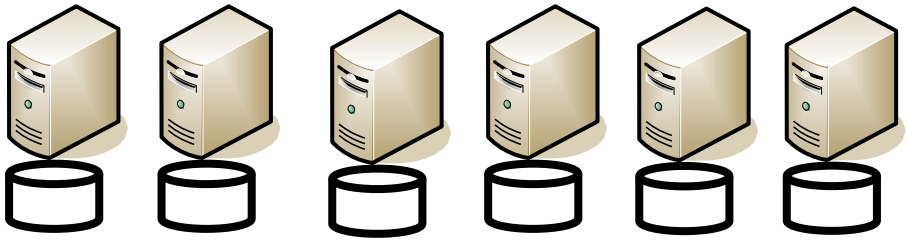


2015 : 4 serveurs physiques, mais ~ 40 serveurs virtuels et 2 baies disques



Réponses :
- virtualisation
- baies de stockage

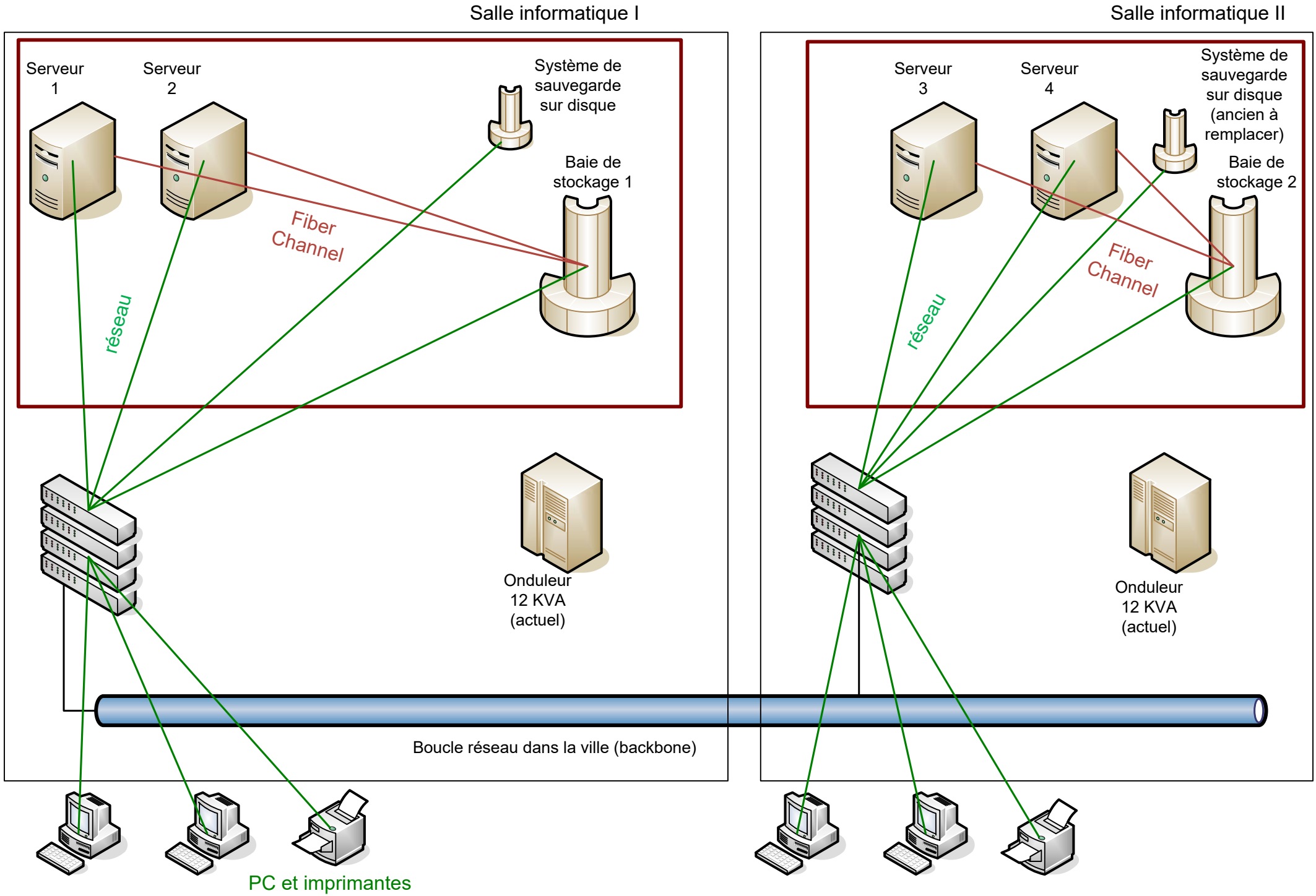
2020 : 6 serveurs physiques avec disques intégrés, mais ~ 70 serveurs virtuels



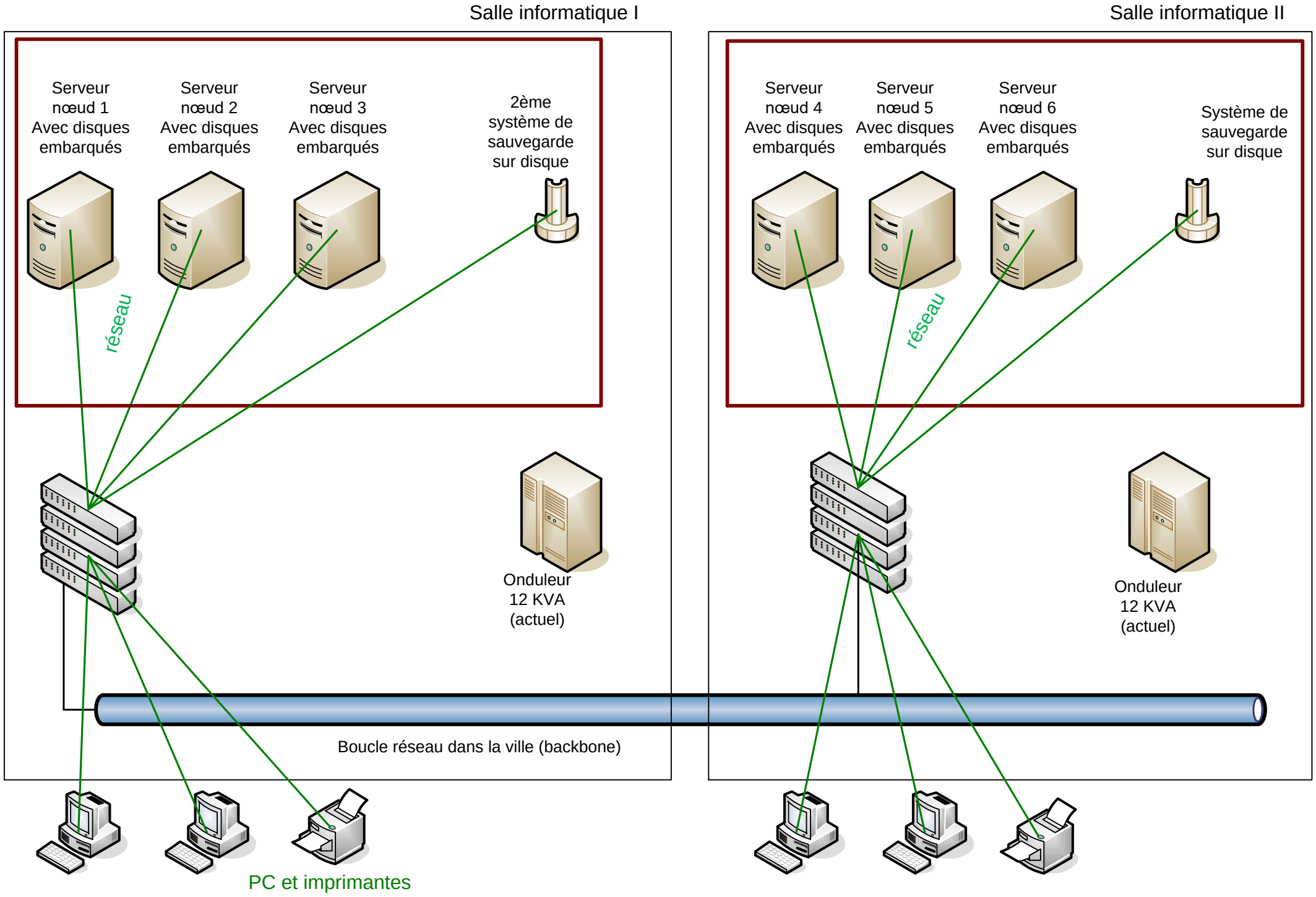
- virtualisation
- hyperconvergence
- distribution des données

Augmentation des besoins en serveurs et en volume de stockage des données : serveurs dédiés pour central téléphonique, pour base de données, accès à Internet, solution de gestion des PC, centre d'impression, webcam, impression, serveurs de fichiers, etc.

# Infrastructure informatique actuelle (fin 2019) de l'administration communale



# Infrastructure informatique de l'administration communale : projet 2020



DIRECTION DES SYSTEMES D'INFORMATION -DSI

# Etude complémentaire externalisation

**10.02.2020**

# Index

- **Situation infrastructure de stockage informatique**
- **Types de cloud / d'externalisation**
  - Location de serveurs virtuels (IaaS)
  - Hébergement d'applications (SaaS)
- **Les + et les – d'un hébergement cloud**
- **Complément d'étude et coûts**
- **Situation des autres communes et retours**
- **Conclusions suite au complément d'étude**
- **Recommandations et stratégie de la DSI**

# Situation infrastructure de stockage info

- **Les baies de stockage informatiques exploitées à Vevey depuis fin 2015 présentent les problèmes suivants :**
  - L'espace disque va arriver à saturation
  - Les performances des baies de stockage et des disques mécaniques qu'elles contiennent sont limitées et créent des ralentissements importants, voire des blocages, lors de sollicitations particulières (par exemple dans les cas récurrents des sauvegardes de la messagerie se terminant en journée)
- **L'ajout de disques sur les baies actuelles coûterait dans les 35'000.- CHF, l'investissement serait perdu au remplacement de l'infrastructure et ne réglerait pas les problèmes de performances**
- **Un remplacement (accompagné d'une nouvelle architecture) est donc nécessaire dans un délai rapide pour que l'exploitation informatique continue dans de bonnes conditions!**

# Types de cloud

| Modèle interne | Hébergement externalisé | Infrastructure As A Service | Software As A Service |
|---|---|---|---|
| Code applicatif | Code applicatif | Code applicatif | Code applicatif |
| Logiciels de base * | Logiciels de base | Logiciels de base | Logiciels de base |
| Système exploitation º | Système exploitation | Système exploitation | Système exploitation |
| Serveurs virtuels | Serveur virtuels | Serveurs virtuels | Serveurs virtuels |
| Serveur physique | Serveur physique | Serveur physique | Serveur physique |
| Réseau interne | Réseau privé loué | Réseau privé loué | Réseau privé loué |
| Salle machine | Salle machine | Salle machine | Salle machine |

exemple : Gelore gestion réservations

*Géré externe*

*Géré en interne*

* : base de données, serveur web, etc.
º : Windows ou Linux

# Les + du cloud

- **Evolutivité : possibilité d'ajouter rapidement des prestations / unités de services**
  *- une nouvelle machine virtuelle peut être opérationnelle en l'espace de qqs heures*
  *- la capacité de stockage peut être adaptée selon les besoins*
- **La gestion technique peut être assurée par un partenaire externe, on s'affranchit alors de certaines activités et problématiques techniques (en option payante)**
- **Disponibilité 24x7 (en option payante)**
- **Sécurité au travers des infrastructures plus robustes mis en place par le fournisseur (en option payante pour certains services)**
- **Un lissage des coûts, et seul le service effectif utilisé est facturé**

# Les - du cloud (pour Vevey)

- **Problématiques techniques**
  *(migration lourde avec une durée de projet importante; temps d'accès aux applications à garantir)*
- **Les coûts**
  *(projet, service, lignes de communication, disponibilité / redondance, amortissement nécessaire des investissements effectués récemment)*
- **Risque de perte de maîtrise, risque de dépendance**
  *(plus de contrôle ni de choix de la solution de virtualisation par exemple)*
- **Sécurité**
  *(encryption, risque d'intrusion)*
- **Les aspects juridiques**
  *(conformité loi sur la protection des données ; élaboration / négociation des contrats de service)*
- **Rendrait plus difficile la collaboration régionale**
  *(les infrastructures des communes peuvent se voir dans le VLAN «communes» du Réseau Cantonal Vaudois (RCV))*

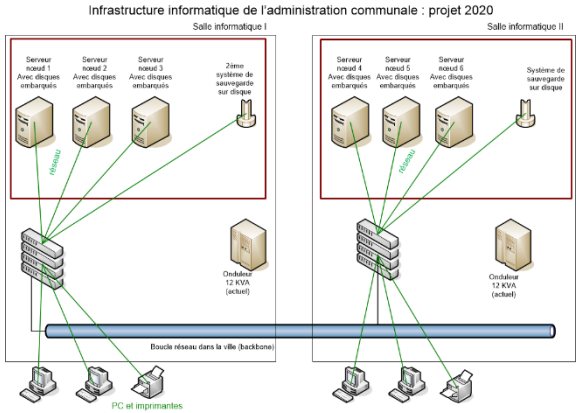
# Maîtrise des risques sur le cloud

- **Niveau de sécurité**
- **Niveau de service**
- **Récupération des données en cas de fin contrat**
- **Pénalités en cas de problème**
- **Contractualisation précise nécessaire**

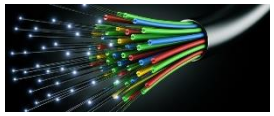
- ***Augmentation du travail administratif si on veut maîtriser les risques***
- ***La DSI n'a pas d'expérience à ce jour dans ce domaine***

# Complément d'étude externalisation : variantes

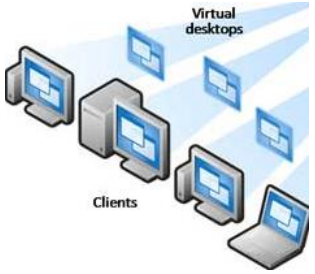
## 3 variantes possibles :




- **Hébergement interne**



- **1: Cloud + réseau 10 Gbps**




- **2: Cloud + Terminal Server / Citrix**

**La DSI n'a pas étudié la variante 2 basée sur du Terminal Server / Citrix qui demanderait encore un important travail supplémentaire pour mettre en place des serveurs applicatifs et paramétrer tous les logiciels pour les faire exécuter sur ces machines ! Un changement complet de l'environnement poste de travail serait à prévoir.**

# Coûts Externalisation infrastructure Serveur – Stockage – Variante 1

## Estimation des coûts sur 5 ans sur la base de retour d'offres budgétaires

| | | Infrastructure | | Backup | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | Description serveur | Prix annuel TTC | Prix sur 5 ans TTC | Backup sur 5 ans | Option de continuité "next business day" 5 ans | Coûts 5 ans sans lignes | Ligne redond. 10 Gbits/s 5 ans (prix opérateur) | Coûts 5 ans avec lignes | |
| **Prestataire 1** | 4 CPUs, 12 Go de RAM, 300 Go disque | 93'535 | 467'674 | ? | ? | 467'674 | 345'932 | 813'606 | offre "nue" sans sauvegardes, ni redondance permettant une reprise d'activité ! |
| **Prestataire 1 avec redondance** | 4 CPUs, 12 Go de RAM, 300 Go disque | 93'535 | 467'674 | ? | 482'674 | 950'349 | 345'932 | 1'296'281 | manque la sauvegarde, réplication manuelle des serveurs sur Datacenters |
| **Prestataire 2** | Sur base globale (3,4 CPUs, 14.28 Go de RAM, 314 Go disque) | 96'633 | 483'164 | 322'075 | ? | 822'902 | 345'932 | 1'168'834 | manque la redondance permettant une reprise d'activité ! |
| **Prestataire 3** | 4 CPUs, 16 Go de RAM, 300 Go disque | 151'986 | 759'931 | 61'928 | 522'830 | 1'347'273 | 345'932 | 1'693'206 | mais avec nos systèmes de sauvegarde hébergés dans leurs Datacenters ! |
| **Prestataire 4** | Sur base globale (2.2 CPUs, 6.85 Go de RAM, 428 Go disque) | 267'990 | 1'339'950 | backup limité inclus | sans | 1'339'950 | 345'932 | 1'685'882 | manque la redondance permettant une reprise d'activité ! |
| **Prestataire 4 avec redondance** | Sur base globale (2.2 CPUs, 6.85 Go de RAM, 428 Go disque) | 405'167 | 2'025'837 | backup limité inclus | avec | 2'025'837 | 345'932 | 2'371'769 | offre assez complète |
| **Coûts achat et installation locaux Ville de Vevey** | | | | | | 380'000 | 0 | 380'000 | |

DIRECTION DES SYSTEMES D'INFORMATION - DSI

# Coûts Externalisation infrastructure Serveur – Stockage – Variante 1

## Estimation des coûts sur 5 ans sur la base de retour d'offres budgétaires

| | Infrastructure | Backup | | | | |
|---|---|---|---|---|---|---|
| | Prix sur 5 ans TTC | Backup sur 5 ans | Option de continuité "next business day" 5 ans | Coûts 5 ans sans lignes | Ligne redond. 10 Gbits/s 5 ans (prix opérateur) | Coûts 5 ans avec lignes |
| **Prestataire 1** | 467'674 | ? | ? | **467'674** | **345'932** | **813'606** |
| **Prestataire 1 avec redondance** | 467'674 | ? | 482'674 | **950'349** | **345'932** | **1'296'281** |
| **Prestataire 2** | 483'164 | 322'075 | ? | **822'902** | **345'932** | **1'168'834** |
| **Prestataire 3** | 759'931 | 61'928 | 522'830 | **1'347'273** | **345'932** | **1'693'206** |
| **Prestataire 4** | 1'339'950 | backup limité inclus | sans | **1'339'950** | **345'932** | **1'685'882** |
| **Prestataire 4 avec redondance** | 2'025'837 | backup limité inclus | avec | **2'025'837** | **345'932** | **2'371'769** |
| **Coûts achat et installation locaux Ville de Vevey** | | | | **380'000** | **0** | **380'000** |

offre "nue" sans sauvegardes, ni redondance permettant une reprise d'activité !

manque la sauvegarde, réplication manuelle des serveurs sur Datacenters

manque la redondance permettant une reprise d'activité !

mais avec nos systèmes de sauvegarde hébergés dans leurs Datacenters !

manque la redondance permettant une reprise d'activité !

offre assez complète

# Coûts par variante

## Coûts sur 5 ans : estimation de Nyon qui a fait le même travail fin 2019

VILLE DE NYON
SERVICE INFORMATIQUE ET POPULATION

### Coûts par variante

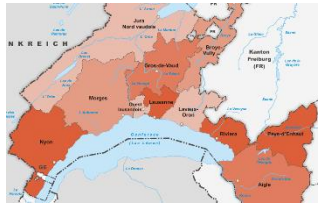
| Scenario 1 | Scenario 2 |
|---|---|
| • Ligne très haut débit 3'000-5'000 chf/mois<br>• Computing 15'000-20'000 chf/mois<br>• DRP a définir | • Ligne haut débit 1500 chf /mois<br>• Computing 15'000-20'000 chf /mois<br>• Affichage déporté 100'000 chf (minimum)<br>• DRP à définir |

### Coûts sur 5 ans :

| Solution | Achat | Cloud (prix amazon) | Réseau et Citrix |
|---|---|---|---|
| Interne (avec DR) | 350'300.- | 0 | 0 |
| 1: Cloud + 10Gbps | 0 | 900'000.- à 1'200'000.- | 180'000 à 300'000.- |
| 2: Cloud + Citrix | 0 | 900'000.- à 1'200'000.- | 190'000<br>(dont 100'000 Citrix) |

***Note; DRP = Infrastructure de recouvrement en cas de désastre – redondance de l'infrastructure***

# Solutions des autres villes



**11 Communes avec deux sites d'exploitation informatique :**

- **Morges, Pully, Epalinges, Lausanne, Prilly, Vevey, Montreux, Aigle, Payerne, Yverdon, Montreux**

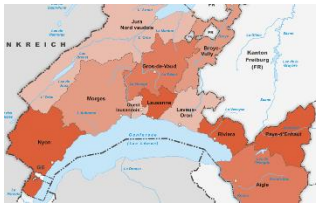
**4 Communes avec un seul site d'exploitation informatique :**

- **La Tour-de-Peilz, Crissier, Bussigny, Nyon**

**Commune avec hébergement externalisé / cloud :**

- **AVRiC : aucune réponse reçue dans ce sens**

# Pourquoi héberger en interne ?



**Consolidation des retours d'un sondage auprès des communes vaudoises de l'AVRiC :**

- **Les prix sont bien plus bas pour la solution interne**
- **Passer à un hébergement externe demanderait d'augmenter la vitesse et de sécuriser les connexions vers l'extérieur, ce qui entraînerait des coûts considérables**
- **Protection des données, nécessité de crypter les données sensibles si hébergées en externe**
- **Ne pas être trop dépendant des prestataires**
- **Maîtriser ses données**

# Conclusions de l'étude

- **Les offres budgétaires en main de la DSI pour une infrastructure interne sont très concurrentielles, aussi s'agit-il en l'état des solution les plus économiques vis-à-vis de la puissance de traitement mise a disposition. Les offres pour une infrastructure externe avec la redondance nécessaire coûteraient plus de 1.5 millions sur 5 ans, soit 5x plus cher.**
- **La nouvelle architecture hyperconvergée (serveurs & stockage) prévue simplifiera la gestion et diminuera les temps de reprise en cas de problèmes et un équivalent hébergé se révèle hors de prix.**
- **Cette solution (passage à une architecture hyperconvergée) est également la moins impactante sur le confort des utilisateurs et sur les équipes IT de la DSI.**

# Recommandations suite à l'étude

- **La décision la plus logique, la plus réaliste et la plus économique est de continuer sur une infrastructure physique hébergée dans les locaux informatiques de Vevey…**
- **Tout en gardant la possibilité à terme (horizon 5 ans) d'une future migration dans le cloud ouvert, si les tarifs baissaient considérablement jusqu'à devenir compétitifs et que les contraintes techniques d'accès et les aspects en lien avec la sécurité des données étaient réglés.**

# Stratégie de la DSI

- ***Maintenir la gestion des serveurs en interne à court – moyen terme (horizon 5 ans)***
- ***Procéder à l'investissement rapidement en 2020 pour faire évoluer l'architecture de la plateforme serveurs/stockage obsolète et sous-dimensionnée***
- ***Privilégier dans la mesure du possible les solutions web pour les nouvelles applications***

  *– pour le télétravail et l'indépendance de l'OS*

  *Note : les développeurs d'applications privilégient la mise à disposition en mode SaaS*
- ***Rester attentif aux évolutions futures***

  *– éventuel cloud public, etc.*

  *– se reposer la question avant chaque investissement majeur*