Consolidation des moyens informatiques

Christophe Cornu

CONSERVATOIRE NATIONAL DES ARTS ET METIERS

Centre régional associé de Belfort

———

Mémoire présenté en vue d'obtenir le diplôme d'ingénieur C.N.A.M. spécialité Informatique, Réseaux, Systèmes et Multimédia

par

M. Christophe CORNU

———

Consolidation des moyens informatiques

Soutenu le 08 décembre 2015

———

JURY

Président : M. Fouad BADRAN

Membres : M. Alain-Jérôme FOUGERES, M. Philippe DESCAMPS, M. Olivier LAMOTTE

Remerciements

Je tiens à remercier mes différents directeurs, Mme Myriam Gravelle et M. Didier Chauvin ainsi que M. Martial Ratié président de l'OGEC Saint Joseph St Paul qui ont tout mis en œuvre afin de me permettre d'effectuer ce stage de fin d'études dans les meilleures conditions.

Un grand merci également à M. Claude Hurth qui m'a accompagné tout au long de ces mois de travail.

Et bien entendu une mention particulière à Louise et Laetitia qui m'ont souvent supporté… et encouragé.

Abréviations

ACE : *Access Control Entry*

ACL : *Access Control List*

AD : *Active Directory*.

BYOD : *Bring Your Own Device ("apportez vos appareils personnels" dans l'entreprise et travaillez avec…)*

DFSN : *Distributed Files System Namespaces*

DFSR : *Distributed Files System Replication*.

DMZ : *DeMilitarized Zone*.

FSMO : *Flexible Single Master Operation*

GPO : *Group Policy Objects*

OGEC : Organisme Gestionnaire de l'Enseignement Catholique

OU : *Organization Unit*

PDC : *Principal Domain Controller*.

SID : *Security IDentifier*

TGT : *Ticket Grant Ticket*

UPN : *User Principal Name*.

Glossaire

ACL/ACE : Les ACL sont des listes d'ACE qui permettent de définir les droits d'accès sur des ressources.

Active Directory : implémentation d'annuaire LDAP Microsoft

DMZ : un sous-réseau isolé par un pare-feu. Ce sous-réseau contient des machines se situant entre un réseau interne (LAN - postes clients) et un réseau externe (typiquement, Internet).

Forêt AD : structure hiérarchique englobant une ou plusieurs arborescences de domaines.

FSMO : Rôles attribués à certains serveurs DC afin que seuls ces serveurs puissent modifier certains aspects de l'AD.

GPO : Les GPOs sont des objects Active Directory qui contiennent les paramétrages à appliquer à des OUs contenant des utilisateurs et/ou des machines.

OU : Conteneurs permettant de former une hiérarchie reflétant l'organisation physique ou logique de l'entreprise.

SID : Un identifiant de sécurité est une valeur unique utilisée pour identifier une entité de sécurité comme un utilisateur, un ordinateur.

TGT : Ticket d'authentification présenté par le client au serveur pour accéder à la ressource hébergée.

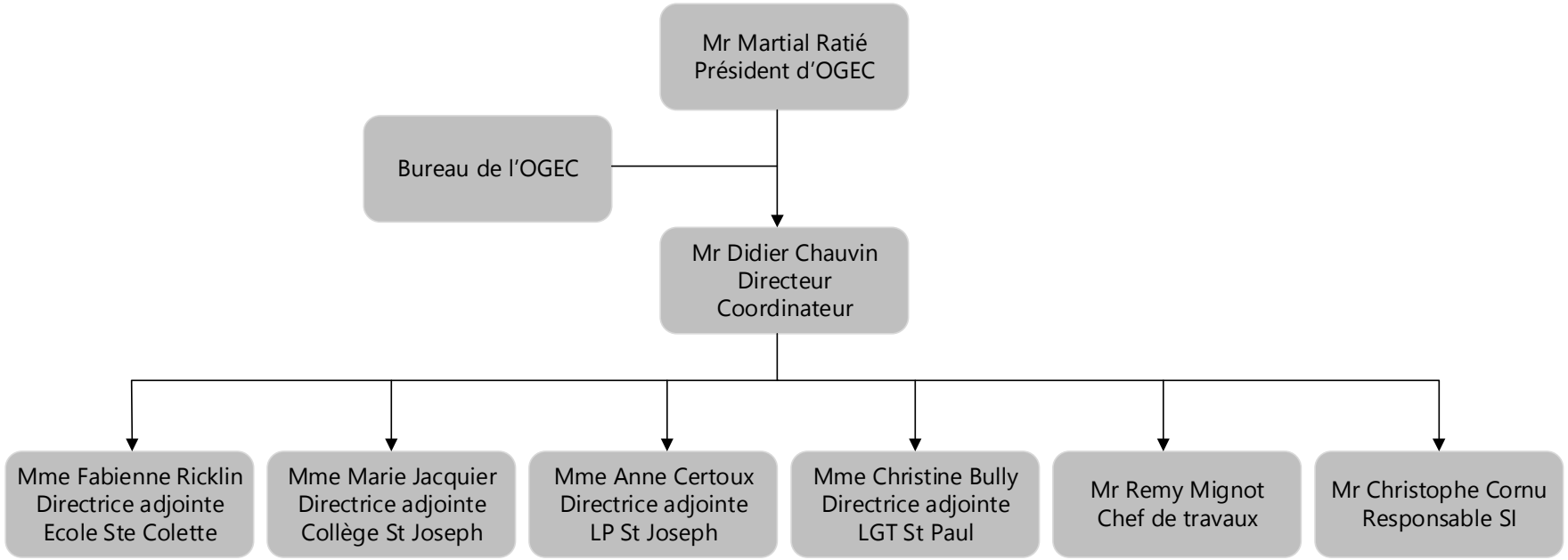
Table des matières

1 Présentation du projet

1.1 Présentation de l'entreprise et contexte du projet

L'Organisme Gestionnaire de l'Enseignement Catholique Saint Joseph Saint Paul est implanté sur deux sites au cœur de la ville de Besançon depuis de nombreuses années et regroupe des établissements scolaires d'enseignement privé. Il accueille aujourd'hui plus de 1200 élèves de la maternelle au Brevet de Technicien Supérieur.

C'est à la suite de l'audit informatique commandé par le conseil d'administration de l'OGEC et réalisé par la société ESDI de Belfort en mars 2014 que la volonté de regrouper nos moyens informatiques s'est affirmée. En effet, plus que jamais dans une période de profonds changements et avec des effectifs en constante progression depuis plusieurs années, il semble judicieux de se projeter dans l'avenir en se dotant des moyens et des fonctionnements adéquats afin de faire face aux défis futurs : téléphonie IP, déploiement du Wifi, prise en charge du BYOD, mise en place d'une messagerie, refonte de nos sites webs …



Organigramme de l'OGEC St Joseph St Paul

1.2 Périmètre du projet

Le groupe scolaire est distribué sur deux sites géographiques distants et nécessite à l'heure actuelle la gestion de trois SI distincts. Après une **étude de l'architecture existante**, il est demandé d'établir une **proposition d'architecture SI cible**, afin de mutualiser les ressources informatiques existantes et d'optimiser les opérations d'échange de données et de gestion au travers de la **réalisation de l'interconnexion des sites** du groupe.

Ce lien permettra d'effectuer la **fusion des différentes entités de gestion Active Directory** au sein d'un LAN étendu.

Il faudra faciliter l'utilisation des logiciels de gestion des élèves et plus particulièrement de la partie comptabilité en consolidant l'architecture logicielle concernée sur un seul et même site en réalisant la **migration vers la suite logicielle Charlemagne**.

On s'appuiera également sur ce lien pour mettre en place un système de **sauvegarde des données stratégiques** de l'ensemble du groupe sur chaque site géographique.

Les enjeux se situent tant au niveau des utilisateurs (environnement commun, partage facilité des données, …) que du service informatique (gestion centralisé d'un SI unique, gains en terme d'efficience et de maintenance…).

1.3 Encadrement du projet

M. Claude Hurth Responsable Systèmes, Réseaux et Télécoms au sein de la société ESDI de Belfort assurera le suivi de l'évolution du projet au travers d'une réunion mensuelle avec M. Christophe Cornu. Au cours de ces réunions, les propositions de M. Cornu seront évaluées et validées par M. Hurth.

2 Etude de l'architecture existante

Le rapport d'audit réalisé par la société ESDI en février 2014 avait pour objectif de réaliser une cartographie ainsi qu'une analyse des constituants du Système Informatique du groupe scolaire.

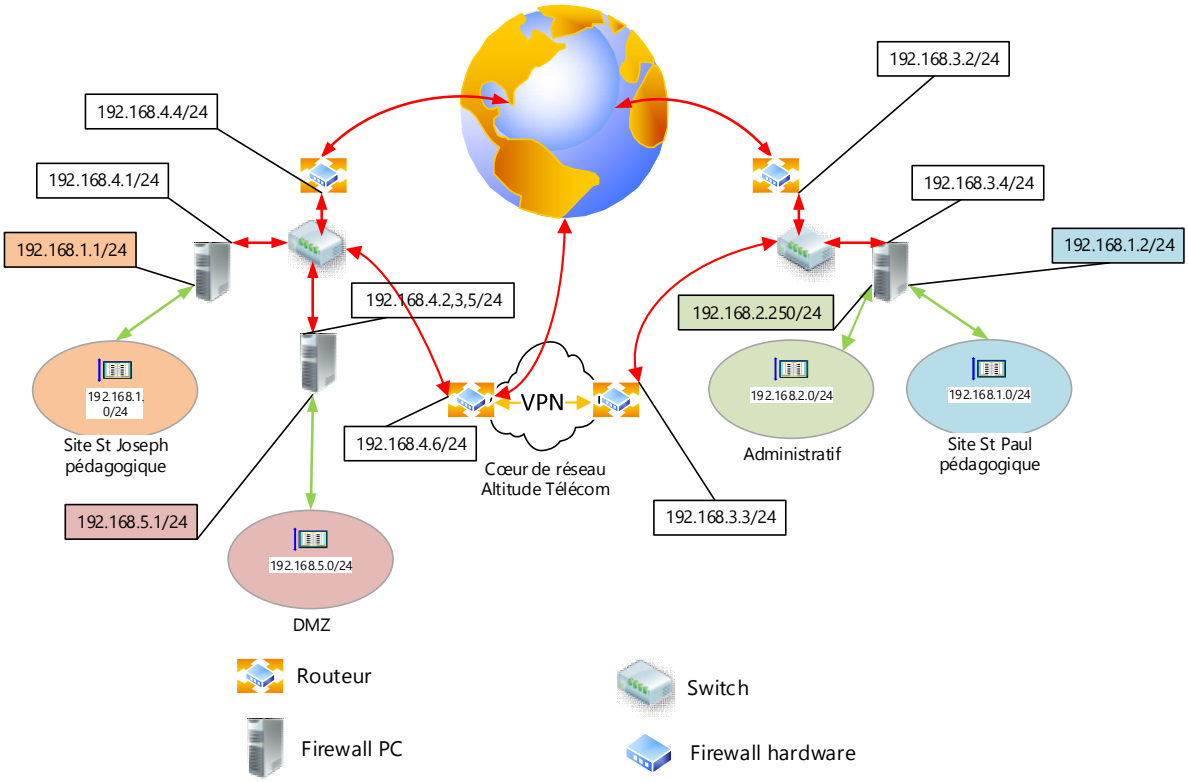


Figure 1 : plan d'urbanisation actuel

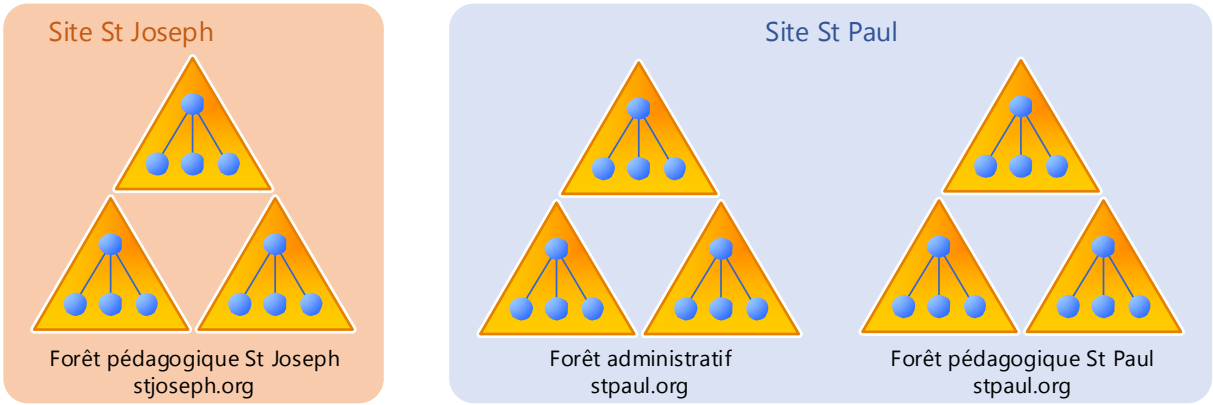


Figure 2 : architecture AD actuelle

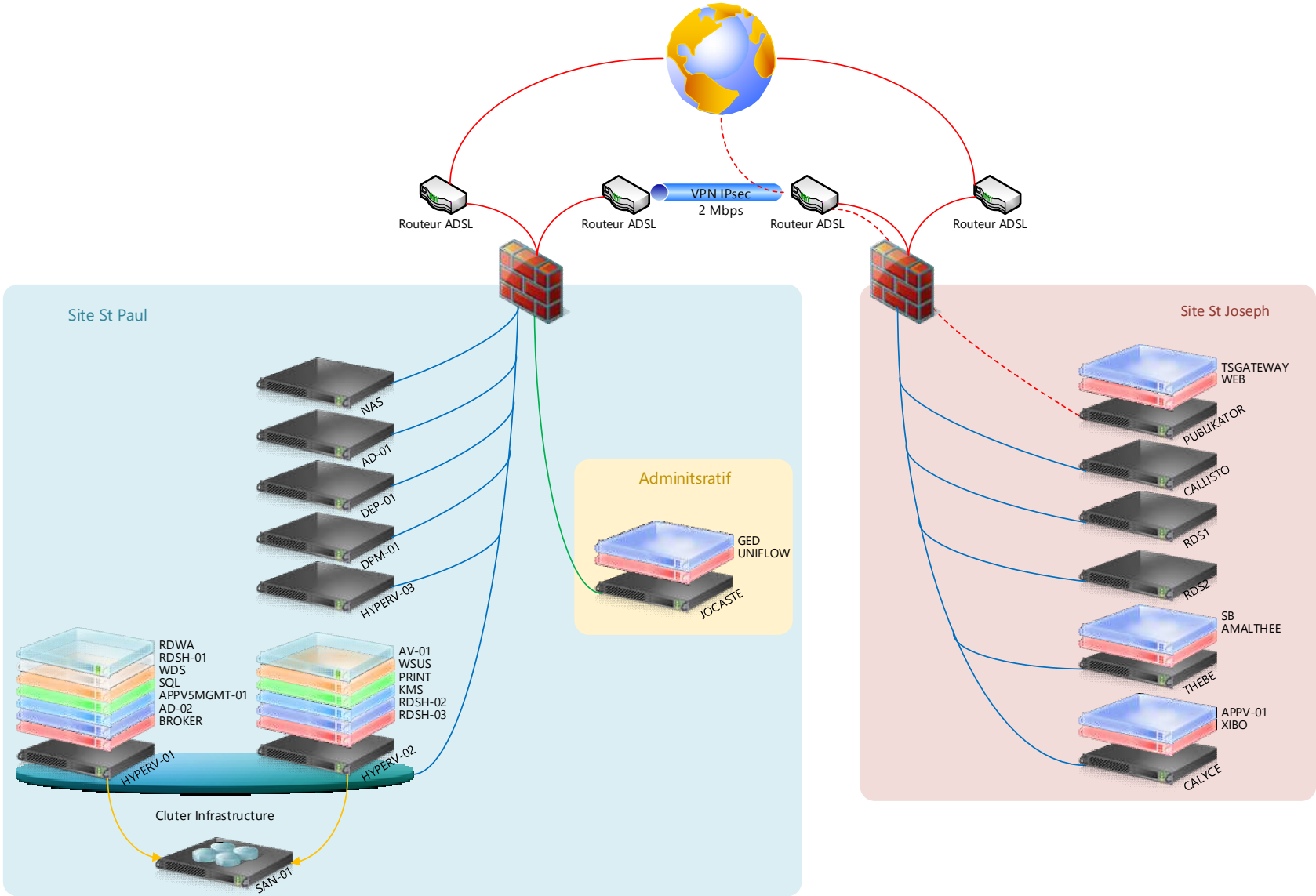


Figure 3 : architecture serveur existante

Les conclusions de cette étude ont permis à l'OGEC d'établir une stratégie à court et moyen terme dans un contexte de profonde restructuration de ses locaux.

Les grandes orientations ainsi dégagées définissent le cadre de ce projet informatique explicité dans le chapitre *1.2 Périmètre du projet*.

3 Proposition d'architecture SI cible

3.1 Lien inter-sites

Par un temps envisagé, l'interconnexion directe entre nos sites n'est plus à privilégier compte tenu du caractère aléatoire et des délais d'obtention des autorisations nécessaires auprès de la copropriété et des autorités compétentes (travaux de voirie entre autres). De même une liaison hertzienne ne permet pas de répondre au niveau de service exigé.

Figure 4 : gaines techniques et distribution des domaines de responsabilité

On fera donc appel à un opérateur télécom. Ce dernier devra de plus être propriétaire de l'infrastructure sous-jacente afin d'éviter un maximum d'intermédiaires et d'optimiser in fine les temps d'interventions selon les exigences exprimées par le conseil d'administration de l'OGEC. Il restera à évaluer la bande passante nécessaire qui découlera des choix techniques retenus pour l'architecture du SI cible.

On intégrera à la réflexion une éventuelle connexion à l'Internet en lieu et place de chacun des liens existants sur chaque site ainsi que les projets à courts termes comme la téléphonie IP.

3.2 Architecture Active Directory cible

Le SI actuel est éclaté sur 2 sites géographiques distants représentant 3 entités de gestion différentes. Il comprend 3 forêts AD sans relation d'approbation inter-forêts.

Il est proposé de réduire le nombre de forêts, et donc le nombre d'entités de gestion, tout en tenant compte des contraintes de sécurité et notamment de la demande d'isolation des services administratifs. La frontière de sécurité AD est par design délimitée par la forêt AD elle-même. En effet au sein d'une forêt tous les domaines de la forêt sont liés entre eux par des relations d'approbation transitives bidirectionnelle. Ces liens permettent à tout utilisateur d'ouvrir une session dans n'importe quel domaine de la forêt et d'accéder de même à toute ressource si les autorisations d'accès le lui permettent. De plus, la compromission d'un compte ayant des droits à l'échelle de la forêt (un compte d'administrateur d'entreprise par exemple), impacte la sécurité de la forêt dans son intégralité.

Pour toutes ces raisons, les services administratifs seront confinés au sein d'une forêt dédiée. On souhaite cependant que certains utilisateurs des services administratifs puissent ouvrir des sessions sur n'importe quel site du groupe (chef de travaux, secrétaires…). L'architecture AD suivante permet de répondre à ces problématiques :

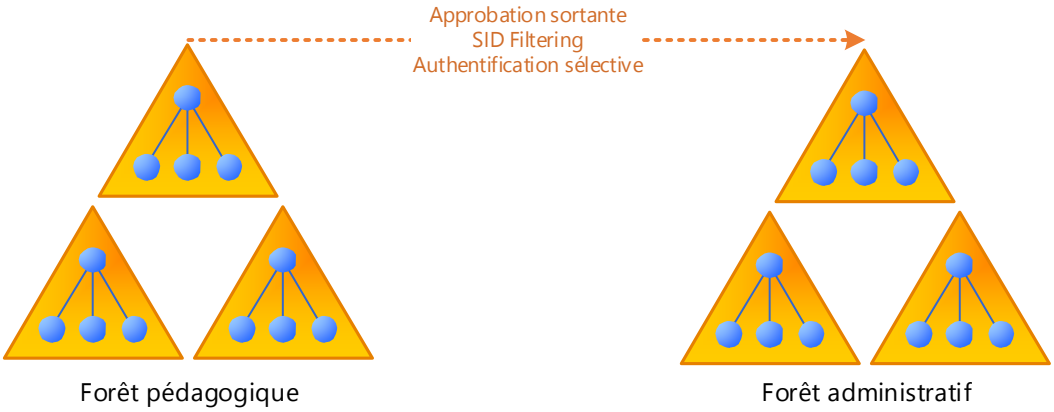


Figure 5 : Architecture AD cible

On procèdera à une fusion de l'AD du domaine racine de la forêt stjoseph.org pédagogique avec l'AD du domaine racine de la forêt stpaul.org pédagogique existant

pour ne plus former qu'un domaine racine de forêt stpaul.org pédagogique. Chaque site géographique étant dès lors matérialisé par un site AD.

Grâce au routage des suffixes de noms entre forêts, l'authentification au sein d'un domaine des forêts est possible quel que soit le domaine d'appartenance de l'utilisateur si l'approbation de forêt le permet. Cela impose cependant l'utilisation de suffixes UPN uniques entre les deux forêts ce qui n'est pas le cas ici (domaine racine de la forêt pédagogique stpaul.org et domaine racine de la forêt administratif stpaul.org). Toutes les forêts ne contenant que le domaine racine, il suffit donc d'en renommer un. Le choix se porte sur le domaine racine de la forêt stpaul.org administratif du fait du nombre de machines membres réduit et de la présence d'un seul et unique DC.

On ne souhaite cependant pas qu'un personnel non administratif puisse ouvrir une session dans le domaine administratif. On ne créera donc qu'une relation d'approbation de forêt sortante vers la forêt administratif. Afin de garantir également un certain niveau de sécurité sur la forêt pédagogique, on s'appuie sur le mécanisme d'authentification sélective pour contrôler les accès du personnel administratif aux ressources de la forêt pédagogiques. Le SID Filtering permet d'effectuer un filtrage sur les SID contenus dans les TGT et les tickets de services qui transitent entre les forêts lors de l'accès aux ressources. Ainsi les SIDs différents du SID de réseau d'origine sont supprimés, empêchant certaines attaques par insert de SIDs dans les données d'autorisation d'un utilisateur.

Enfin, l'adressage IP de chaque sous réseau doit être modifié afin d'obtenir des domaines de diffusions distincts afin de permettre un routage inter-sites et de déclarer les sites AD.

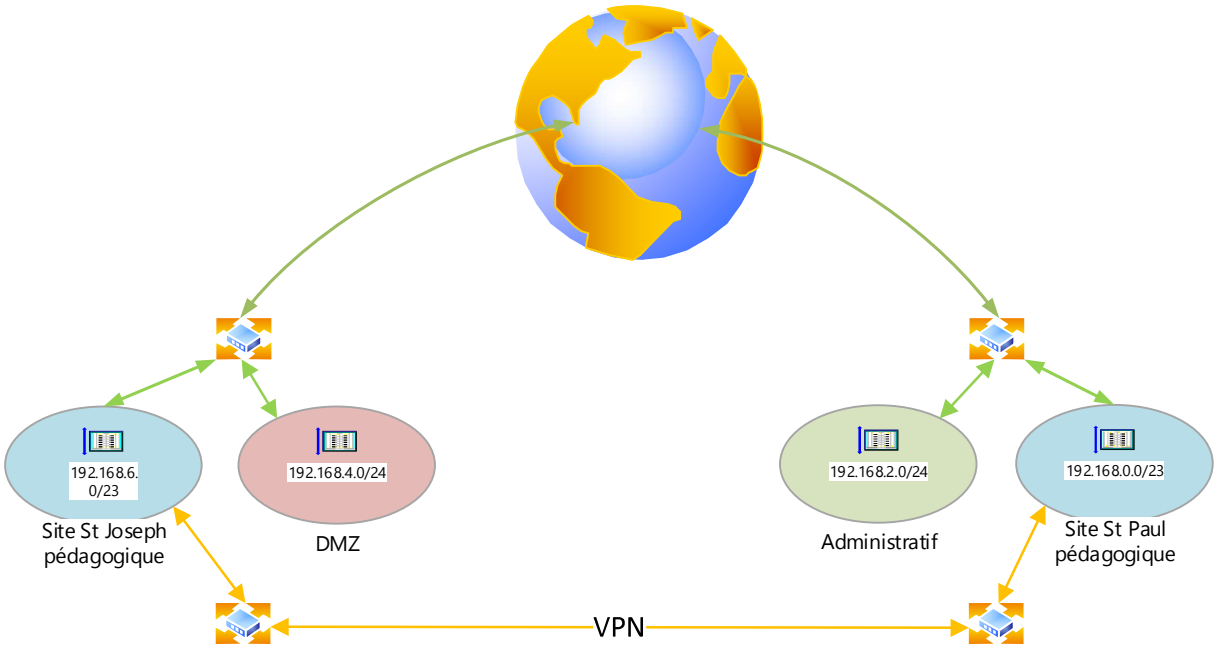


Figure 6 : Adressage IP du SI cible

3.3 Consolidation de la gestion administrative

3.3.1 Suite Aplon et compta Sage Ligne 500

La partie compatibilité entre autres est totalement obsolète et n'évolue plus depuis de nombreuses années (pas d'intégration automatique des mouvements bancaires, pas d'accès multi-utilisateurs à certains modules...). La société éditrice propose cependant une toute nouvelle mouture de ces logiciels dès la rentrée 2015 avec des produits en début de vie et encore en phase de maturation. Dans cette perspective, les logiciels Aplon sont abandonnés et le conseil d'administration de l'OGEC choisit une autre suite logicielle.

3.3.2 Suite Charlemagne

Cette suite logicielle seule concurrente à Aplon sur le marché répond en tous points aux demandes et attentes que l'on est en droit d'espérer d'un tel environnement de travail. Forte de plusieurs années d'expérience, la société STATIM est à même de répondre à nos besoins et s'adapte parfaitement à notre environnement.

Toutes les données nécessaires au fonctionnement de Charlemagne sont conservées sur un unique site et sont accédées à distance en mode RemoteApp via un lien VPN. Tous les calculs informatiques sont effectués sur une machine qui ne retransmet que des « images » aux postes clients distants ce qui rend le procédé d'exploitation très léger et parfaitement adapté à notre architecture cible. Ce mode de fonctionnement nécessite des licences d'accès par machine accédant au service distant. Un pack office est quant à lui nécessaire pour les éditions.

Ce fonctionnement facilite également la sauvegarde des données puisque toutes les données sont consolidées sur un même site.

3.4 Sauvegarde déportée

On définira les données dites stratégiques pour l'entreprise afin d'établir la volumétrie brute de ces sauvegardes spécifiques.

On peut poursuivre l'utilisation du système actuel en accord avec le rapport d'audit ESDI et placer quotidiennement une sauvegarde spécifique sur un autre site du groupe. On prévoira un espace disque suffisant pour cette sauvegarde ce qui se traduira par l'achat éventuel d'espace disque supplémentaire.

Cette solution ne répond cependant pas à toutes les exigences de sécurité et de récupération de données en cas de sinistre grave. On s'oriente donc également vers une solution de stockage en ligne. Le choix étant pléthorique, il faudra rester vigilant sur certains points comme la durée de rétention des données, le respect des normes et certifications (ISO 27001 et eTRUST), la redondance des stockages proposée par l'opérateur, les services associés, le SLA…

3.5 Planning du projet

Le projet débute et se termine selon les dates du stage de fin d'étude de M. Christophe Cornu, à savoir du 1er février 2015 au 30 septembre 2015.

Le planning prévisionnel suivant est établit :

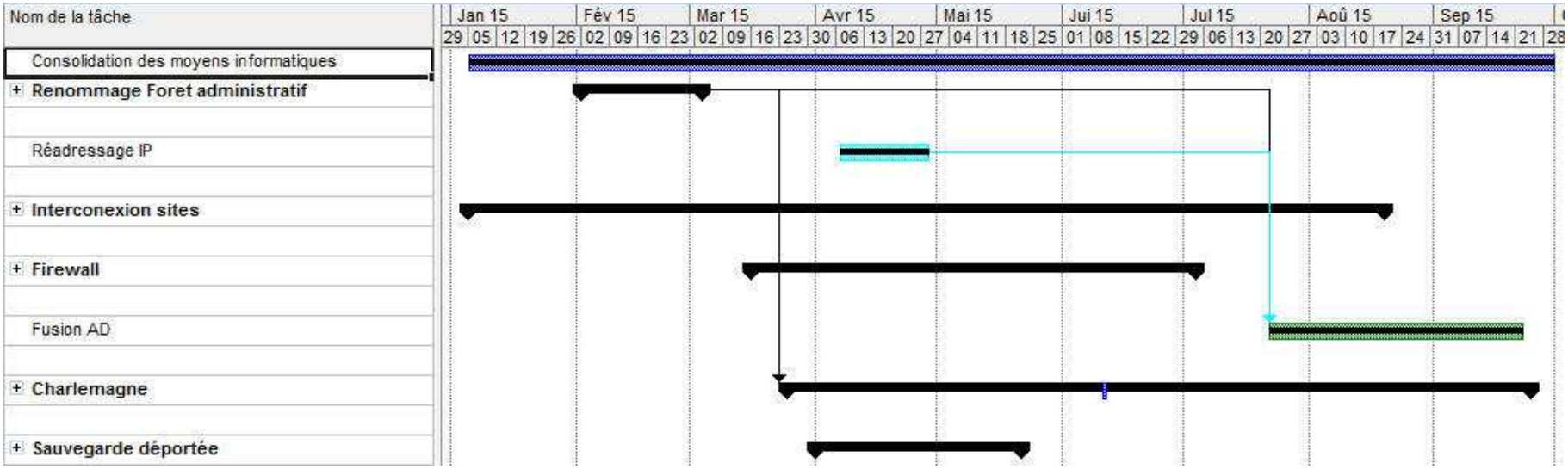


Figure 7 : planning prévisionnel du projet « Consolidations des moyens informatiques »

4 Réalisation de l'interconnexion des sites

Dans le cadre du projet de consolidation des moyens informatiques du groupe OGEC St Joseph St Paul, la construction d'un LAN étendu est à réaliser afin d'interconnecter les deux sites de la structure.

Les tarifs d'accès direct au réseau lumière étant prohibitifs (http://syml.fr/?page_id=4), on s'adressera donc à un prestataire de service internet en privilégiant une interconnexion type VPN MPLS. Ce standard en termes d'interconnexions est en effet largement maîtrisé et proposé par la quasi-totalité des acteurs du secteur. Cette technologie contrairement à un VPN IPSec ne s'appuie pas sur l'Internet pour réaliser les interconnexions, mais sur un réseau dédié, étanche, maîtrisé et sécurisé.

Quelle que soit la solution retenue, le choix du débit est important car il influe directement sur le coût des liaisons. Il ne faut pas surévaluer le débit par rapport aux besoins, afin d'éviter de payer un surcoût inutile. Il ne faut pas non plus le sous-évaluer, car les utilisateurs et les applications exigent des temps de réponse corrects. La conception d'un réseau inter-sites résulte donc d'un compromis coûts/performances.

Afin de correctement dimensionner le lien, il faudra identifier les flux et les besoins applicatifs, et estimer la volumétrie. On s'intéressera également au temps de latence, à la QOS, à la GTR… A partir de ces données et hypothèses on va pouvoir évaluer le débit nécessaire.

On inclut dans l'étude une éventuelle ouverture à l'Internet en tenant compte qu'actuellement les abonnements inhérents à ces services sont pris en charge par la région Franche-Comté dans le cadre du projet ELAIR III qui a pour finalité d'offrir une connexion Internet haut débit à tous les lycées Franc-comtois.

Cette restructuration du SI nous conduit à interconnecter nos sites distants de façon à mettre en commun un maximum de ressources informatiques au sein d'un LAN étendu. Il en découle donc une exposition accrue de nos systèmes aux attaques informatiques

internes et externes, aux virus en tous genres... Ainsi toute vulnérabilité exploitée devient d'autant plus nuisible. Nous intégrons donc également la sécurisation de nos réseaux dans l'interconnexion de nos sites distants en faisant évoluer nos firewalls afin de prendre en charge ces nouvelles menaces.

4.1 Planning

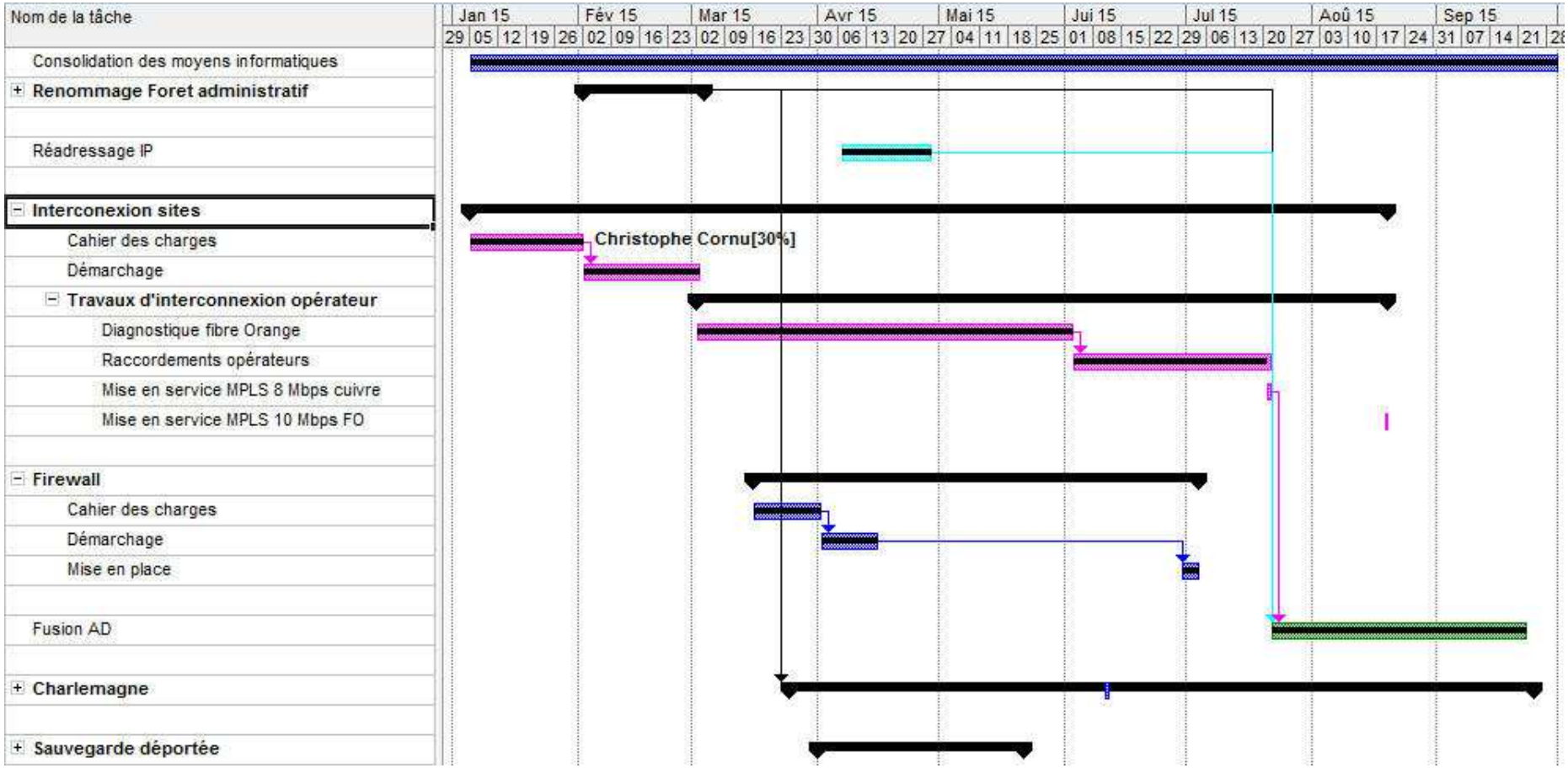


Figure 8 : planning de la phase interconnexion et sécurisation des sites

4.2 Débit IP

Les différentes offres commerciales sont aujourd'hui caractérisées par leur « débit IP » niveau 3 et non plus par leur débit de niveau 1 ou 2 en référence à la couche correspondante du niveau OSI et fonction de la technologie sous-jacente de la connexion. On parle de débit IP de 5, 8 ,10 Mbps voire bien plus encore.

Sachant qu'un paquet IP peut faire au plus 65 536 o auquel on retire 20 o d'entête IP et 32 o d'entête TCP, la charge utile est réduite à 65 484 o.

On peut donc calculer le ratio suivant 65 484o /65 356 o = 99,92% qui correspond au pourcentage de charge utile d'un paquet IP. Si on l'applique à un débit IP de 10 Mbps, on obtient 9,992 Mbps de débit IP « charge utile ». Il en résulte que l'on peut raisonner directement sur les débits IP au vu du résultat précédant (le cas d'un paquet UDP étant encore plus parlant du fait de la taille de l'entête encore plus réduite).

4.3 Caractérisation des flux et estimation des débits nécessaires

Il s'agit dans cette section d'identifier tous les flux susceptibles de transiter par le lien VPN.

4.3.1 Définition d'un site Active Directory

Dans Active Directory, un site est un ensemble d'ordinateurs correctement connectés par un réseau haut débit, tel qu'un réseau local (LAN). Tous les ordinateurs au sein du même site se trouvent généralement dans le même bâtiment ou sur le même réseau. Les sites et les sous-réseaux IP sont représentés dans Active Directory par des objets de sites et de sous-réseaux et correspondent donc à la structure physique du réseau tandis que les domaines correspondent à la structure logique ou administrative de l'organisation. Un site peut être connecté à d'autres sites via un lien VPN par exemple.

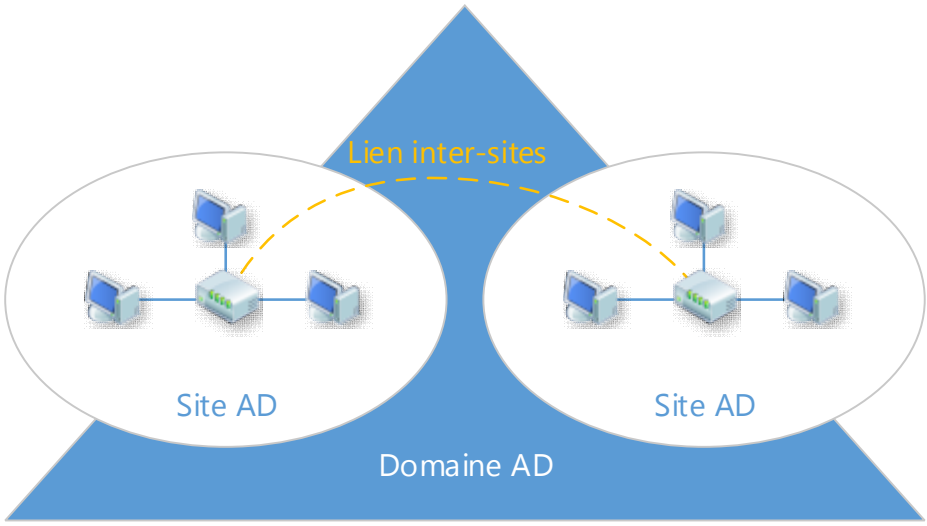


Figure 9 : sites et domaines Active Directory

L'architecture AD retenue défini 2 sites AD interconnectés par un lien VPN, le site St Joseph et le site St Paul.

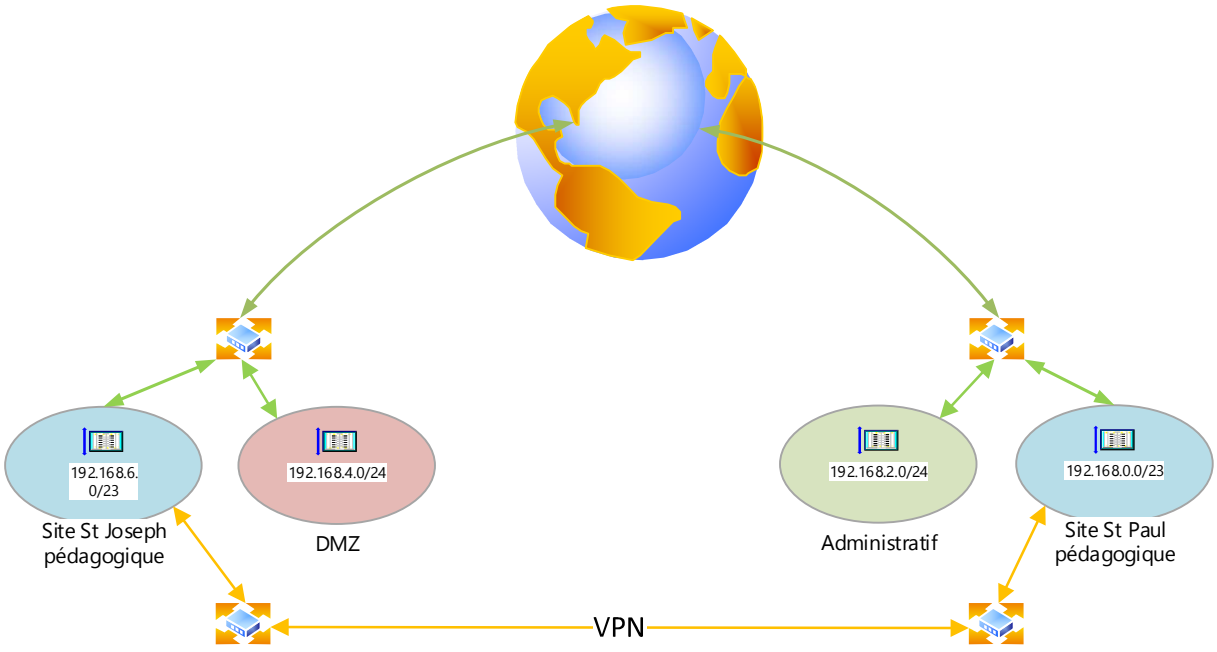


Figure 10 : Architecture réseau du SI cible

4.3.2 Flux lié à la réplication AD

Le modèle multi maîtres sur lequel repose AD permet d'apporter des modifications à l'annuaire AD à partir de n'importe quel contrôleur de domaine. L'annuaire est maintenu cohérent grâce à la réplication des changements opérés entre les contrôleurs de domaine. Au sein d'un LAN, le volume engendré par ce système est sans effet sur la bande passante. Lorsqu'il s'agit de réplications qui empruntent une liaison inter-sites, il convient de contrôler le trafic. Si l'on considère que les modifications apportées à l'AD peuvent attendre la prochaine réplication (par défaut toutes les 180 minutes sur un site AD) pour mettre en cohérence tous les DC du domaine, on peut utiliser le planificateur lié à la connexion inter-sites déclarée dans l'AD et ainsi faire en sorte que le lien VPN ne soit pas utilisé par la réplication lors des heures de bureau où le trafic est soutenu.

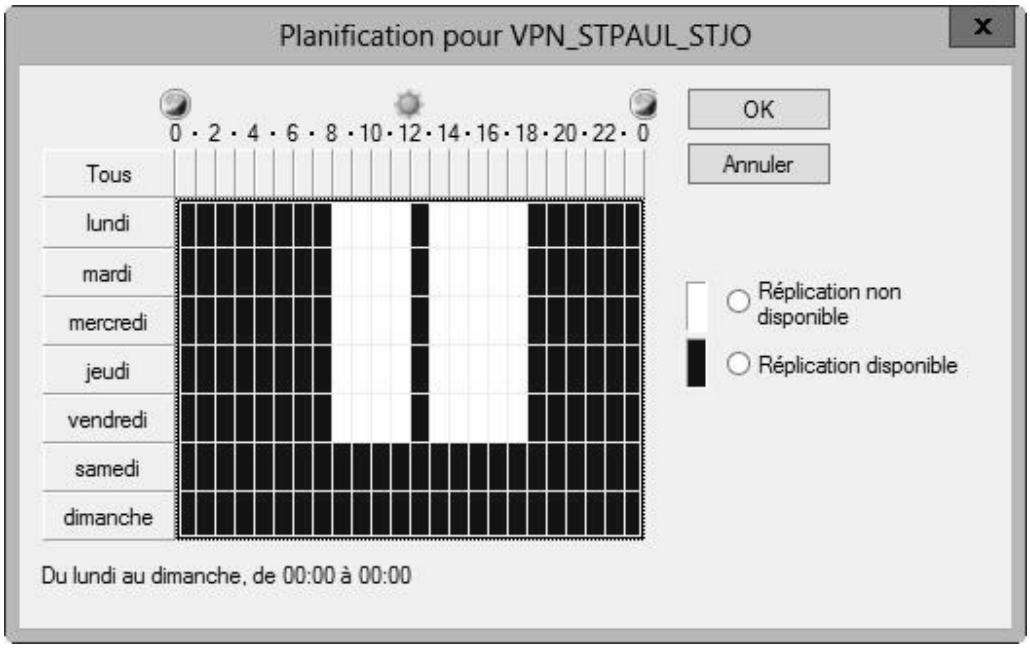


Figure 11 : Planification de la réplication AD inter-sites

Il est également possible de désigner des serveurs « têtes de pont » sur chaque site, afin d'orienter les réplications inter-sites vers des machines connues et non choisies au hasard par le moteur de réplication.

Le protocole employé par le système de réplication inter-sites est de type RPC/IP synchrone faible vitesse point à point. Ce protocole utilise une compression de données avec un ratio de 10 à 15%, ce qui permet de baisser sensiblement la consommation de bande passante inter-sites.

On peut cependant estimer le trafic lié à une réplication sans changement apporté à l'AD à environ 17 Ko en effectuant une capture réseau avec l'outil Wireshark lors d'une réplication forcée.

Display

Display filter: ip.addr == 192.168.1.250
Ignored packets: 0 (0,000%)

Traffic	Captured	Displayed	Displayed %	Marked	Marked %
Packets	92311	28	0,030%	0	0,000%
Between first and last packet	15,493 sec	4,332 sec			
Avg. packets/sec	5958,056	6,463			
Avg. packet size	125,584 bytes	627,714 bytes			
Bytes	11592766	17576	0,152%	0	0.000%
Avg. bytes/sec	748235,314	4057,192			
Avg. MBit/sec	5,986	0,032			

Figure 12 : capture de trame réplication AD forcée.

Les comptes d'utilisateurs et d'ordinateurs sont les objets AD les plus fréquemment créés. Un pic est observé en début d'année scolaire ou les comptes élèves sont créés, soit environ 1200 objets. De la même façon que nous avons estimé le flux de réplication AD de base, on estime la quantité de données échangée après création d'un compte d'utilisateur. On mesure un volume de 38 Ko par utilisateur créé, soit environ 45 Mo pour 1200 utilisateurs.

D'une manière générale, les changements apportés à l'AD sont peu fréquents hors période de rentrée scolaire où les comptes élèves sont créés et les mots de passe des utilisateurs pédagogiques sont initialisés. Ces données ne devraient donc pas beaucoup

évoluer dans le temps même après migration de la forêt stjoseph.org dans la forêt stpaul.org.

Si l'on considère que ce flux est en plus compressé, il apparaît que le trafic de réplication est peu important. Dans tous les cas, même avec un débit faible de l'ordre de quelques Mbps, la réplication inter-sites fonctionnera correctement tant que la latence du lien emprunté reste réduite. Cela mettra juste un peu plus de temps !

4.3.3 Flux lié à l'authentification AD

Les flux d'authentification ne concernent que les utilisateurs administratifs qui se connectent sur une machine du site St Joseph, soit au maximum une dizaine de personnes puisque l'authentification des utilisateurs lambda s'effectue auprès du contrôleur de domaine le plus proche, soit un de ceux présents sur chaque site AD.

On réalise une capture de trames pour évaluer le trafic lié à l'authentification.

Environ 40 kb sont échangés entre la machine utilisateur et le serveur AD du site lors de la phase d'authentification. Même si les échanges sont un peu plus complexes dans une configuration inter-sites avec approbation de confiance, on peut affirmer que la quantité de données reste faible. Pour 10 utilisateurs se connectant au même moment, on arrive à environ 500 Kb de données échangées.

4.3.4 Flux lié aux profils itinérants

Un profil utilisateur définit des environnements de bureau personnalisés, qui intègrent des paramètres d'affichage individuels, des connexions à des réseaux et à des imprimantes, ainsi que d'autres paramètres spécifiques. Il est dit itinérant s'il est rendu disponible sur un serveur de partage de fichiers et téléchargé ou synchronisé chaque fois qu'un utilisateur ouvre une session sur un ordinateur du réseau. Une fois rapatrié sur la machine, le profil est traité par le processus Winlogon. Les modifications apportées au profil utilisateur itinérant sont mises à jour sur le serveur à la fermeture de

session et permettent ainsi de conserver un environnement de travail unique quelle que soit la machine sur laquelle l'utilisateur se connecte.

Lors de la connexion, les profils itinérants des personnels administratifs sont téléchargés ou synchronisés au travers du lien inter-sites. La taille d'un profil est comprise entre 10 et 20 Mo.

Sur un réseau Ethernet connecté à 1 Gbps, le temps de téléchargement d'un profil de 10 Mo est de l'ordre de la seconde (cf. annexe 1 : calcul du temps de téléchargement d'un profil itinérant).

On considère donc qu'il est acceptable que le rapatriement du profil lors de la première connexion au travers du VPN puisse prendre jusqu'à 10 secondes.

On peut donc écrire pour un temps de téléchargement souhaité de 10 secondes :

Taille du profil (10 Mo) / Temps de téléchargement du profil itinérant (10 s)= vitesse de téléchargement Mio/s soit 10 Mo/10 s=1 Mio/s.

En raisonnant sur des débits IP, on obtient un débit physique nécessaire de 8 Mbps pour un temps de téléchargement équivalent.

Un débit de 3 à 4 Mbps porte ce temps de téléchargement à environ 30 secondes.

4.3.5 Flux lié au Catalogue Global

Le catalogue global regroupe les données descriptives de chaque domaine d'une forêt AD. Notre forêt stpaul.org n'est constituée que du domaine racine, cependant, le CG est tout de même consulté lors de la phase d'authentification des utilisateurs dont les UPN sont différents du domaine (nos utilisateurs administratif par exemple). On ne peut donc totalement le désactiver.

Puisque les données du domaine sont déjà répliquées par le mécanisme de réplication AD habituel, le CG ne consomme aucune ressource supplémentaire. On déclare donc tous les contrôleurs de domaine en tant que CG, augmentant de fait la disponibilité de ce dernier.

4.3.6 Flux lié aux changements de mot de passe et réplication urgente

Dans un fonctionnement normal, le changement de mot de passe initié par un utilisateur au moment de sa première connexion par exemple, implique de contacter le DC possédant le FSMO PDC du domaine stpaul.org situé sur le site St Paul. Ce mot de passe est ensuite transmis aux différents DC par les mécanismes de réplication AD.

Un autre cas de figure est à prendre en compte, celui de la vérification du mot de passe. Imaginons un utilisateur se connectant auprès de son DC local avec un mot de passe différent de celui connu par ce DC (le DC local n'a pas encore été répliqué avec le PDC et n'a pas encore connaissance du nouveau mot de passe). Le DC contacte le PDC pour vérification du mot de passe. Le PCD déclenchera une réplication urgente du mot de passe vers le DC demandeur qui peut alors réaliser l'authentification avec le mot de passe à jour.

Il est possible de modifier ce comportement et de faire en sorte que les changements de mot de passe soient gérés par les DC locaux plutôt que de contacter le PDC et d'utiliser le lien inter-sites. Les mots de passes sont alors répliqués par l'intermédiaire des mécanismes habituels.

Sur le site St Joseph on pourra activer le paramètre *Configuration ordinateur/Modèles d'administration/Système/Net Logon/Contacter le contrôleur de domaine principal lors de l'échec de l'ouverture de session* dans une GPO de site.

Quelques dizaines de Ko de données sont alors échangés, ce qui reste négligeable sauf en période de rentrée où les changements de mot de passe sont massifs.

4.3.7 Flux DFSR

Le protocole Distributed Files System Replication (DFSR) permet de synchroniser un système de fichier entre plusieurs cibles NTFS au sein d'une même forêt AD (mais pas de forêts différentes, même avec une relation de confiance établie entre elles).

DFSR utilise l'algorithme de compression différentiel Remote Differential Compression (RDC) sur les blocs au niveau fichier, non au niveau bloc de disque. Pour chaque bloc d'un fichier, le système de compression calcule une signature, à savoir un petit nombre d'octets représentant de façon unique le bloc. L'ensemble des signatures est transféré du serveur au client. Le client compare les signatures du serveur à ses propres signatures. Le client demande alors au serveur de n'envoyer que les données correspondant aux différentiels de signatures économisant ainsi la bande passante.

Les réplications sont planifiées et la bande passante utilisable est paramétrable, ce qui permet de contrôler efficacement l'utilisation du lien inter-sites.

Nous utilisons DFRS pour maintenir à jour nos espaces de noms \\stpaul.org\Deployment\Packages et \\stpaul.org\Deployments\Contents qui correspondent respectivement aux packages applicatifs distribués par GPO et aux bulles AppV applicatives. Ces contenus ne sont pas appelés à être drastiquement modifiés au quotidien. De plus un nouveau membre de réplication peut être amorcé par copie de fichiers avant la réplication initiale, réduisant de façon spectaculaire la quantité de données répliquées. On limitera la bande passante allouée à la réplication à 1 Mbps.

4.3.8 Flux RemoteApp

Le principe technologique du protocole RDP (communication graphique compressée limitée au rafraîchissement d'écran dans un sens, et évènements clavier/souris, impression, flux de lecteurs réseaux dans l'autre) induit une faible consommation de bande passante sur un réseau à faible latence.

À minima, lorsque l'utilisateur ne manipule pas le clavier ou la souris et que rien ne bouge à l'écran (lecture d'une vidéo par exemple), seules quelques trames de contrôle de connexion transitent sur le réseau afin de vérifier que le poste est toujours connecté au serveur. Il y a à cet instant une consommation de bande passante quasi nulle.

À maxima, lorsque l'utilisateur rafraîchit l'intégralité de la surface de l'écran, par exemple lorsqu'il va basculer d'une application à une autre, la consommation de bande passante est de l'ordre de 120 à 128 Kbps. En moyenne, c'est à dire en utilisation courante d'un utilisateur actif, on constate que la bande passante consommée oscille entre 64 et 80 Kbps.

On obtient donc une consommation de bande passante oscillant soit entre quasi 0 Kbps et 128 Kbps, avec une moyenne normalisée oscillant entre 0 et 80 Kbps par poste connecté.

Il convient alors d'intégrer deux dimensions supplémentaires : la simultanéité et la réalité de l'entreprise. Considérons la dizaine d'utilisateurs qui travailleront en mode client léger. Le protocole ne consommant que l'équivalent de la somme des rafraîchissements de l'ensemble des écrans des utilisateurs, combien d'écrans complets cela peut-il représenter à l'instant t, car à l'instant t+1, si les utilisateurs ne poursuivent pas leurs actions, la consommation retendra vers 0. On constate généralement que l'on peut diviser le nombre d'utilisateurs par 2 pour avoir la réponse, et multiplier par 64 Kbps par utilisateur pour obtenir un ordre de grandeur de la bande passante utilisée (ou nécessaire).

Dans la réalité de l'entreprise, un salarié ne passe pas tout son temps à manipuler son ordinateur (sauf quelques activités ou postes spécifiques) : il téléphone, manipule du papier, participe à des réunions, etc. Cela reste donc difficile à évaluer, mais l'on peut considérer que l'ordre de grandeur obtenu convient à une population de 50% supérieure. Nous arrivons donc au calcul suivant pour 10 à 15 utilisateurs:

(10/2)*64=320 kbps soit 0,31 Mbps

Les écrans dont la conception matérielle imposent une position fixe aux pixels, comme les écrans plats modernes, peuvent subir d'importantes déformations de crénelage qui se manifestent par des traits dentelés lorsqu'on affiche des petits éléments à forts

contrastes comme du texte. ClearType utilise une technique d'anticrénelage au niveau du sous pixel afin de réduire fortement les défauts perceptibles (les artefacts), lors de l'affichage des manuscrits, et fait apparaître des caractères plus lisses et plus lisibles.

Bien que l'activation du lissage des polices amène un confort visuel supplémentaire aux utilisateurs, il faut bien garder à l'esprit que cela induit également une augmentation de la consommation de bande passante de l'ordre de 4 à 10 fois. Si l'activation du support des polices ClearType permettant de rendre à l'écran un texte aussi claire et précis que sur un document imprimé est effective, la bande passante nécessaire est multipliée par 4 voire 10, soit au maximum 3,1 Mbps.

En ce qui concerne l'impression, on peut utiliser TS Easy Print. C'est un système d'impression sans pilote qui permet de simplifier la redirection des imprimantes clientes.

Dans les faits, TS Easy Print agit comme un proxy pour toutes les demandes d'impression et les réoriente vers la machine cliente, sans pour autant installer un quelconque pilote sur le serveur RDS.

Aucun prérequis n'est nécessaire sur les serveurs RDS en version 2012, seul est nécessaire côté client le RDC 6.1 minimum, ainsi que le Framework 3.0 SP1 (natif avec Windows 7 et Windows Server 2008 R2).

On prévoit cependant une bande passante réservée plus conséquente afin de prendre en charge le flux d'impression, soit 2 Mbps au total.

4.3.9 Flux lié aux transferts de données

Chaque utilisateur possède un dossier personnel qui le suit sur les machines sur lesquelles il se connecte quel que soit le site. Il faut donc prévoir l'ouverture de fichiers au travers du VPN. Certaines sections telles les classes de Sciences de l'Ingénieur ou encore de BTS Conception Pour l'Ingénieur sont amenées à utiliser des logiciels de CAO produisant des fichiers de plusieurs dizaines de Mo ou plus couramment des fichiers de présentation, des fichiers audio ... On conçoit aisément qu'il n'est pas envisageable

d'attendre plusieurs minutes l'ouverture ou l'enregistrement d'un fichier. Le débit du VPN doit donc être suffisamment élevé pour réduire ce temps d'attente à des valeurs acceptables de l'ordre des 20 à 30 secondes pour un fichier de 10 Mo.

Compte tenu des calculs effectués au chapitre en *4.3.4 Flux lié aux profils itinérants*, un débit de 3 à 4 Mbps est nécessaire.

4.3.10 Flux lié aux sauvegardes des données stratégiques

Les sauvegardes concernent les données stratégiques du groupe, à savoir les données liées à la comptabilité, et à la gestion des élèves, ce qui représente un volume d'environ 1 Go. Ces données doivent permettre de reconstruire la solution initiale avec les données les plus à jour.

Le volume concerné peut être répliqué via DFSR de façon à ce que chaque site dispose d'une copie synchronisée de ces données. Sur chaque site, une sauvegarde incrémentielle est effectuée quotidiennement.

L'utilisation de DFSR présente de nombreux avantages, dont la planification et la maîtrise de la bande passante mise à disposition pour réaliser la synchronisation. Cependant DFSR n'est utilisable qu'au sein d'une même forêt. On utilise donc Robocopy pour copier les données stratégiques vers un partage au sein du domaine stpaul.org sur le site St Paul, puis DFSR synchronisera ce contenu avec un partenaire situé sur le site St Joseph.

4.3.11 Flux WSUS

Les systèmes d'exploitation des stations et des serveurs sont mis à jour automatiquement par le service Windows Server Update Services. WSUS rapatrie les mises à jour depuis les sites Microsoft afin de les distribuer hors ligne aux machines du réseau selon une planification établie. Ce service peut être déployé différemment afin de faciliter la gestion des mises à jour (choix des mises à jour, assignation à tel type de

système d'exploitation…). Ainsi un serveur WSUS amont peut transmettre ses mises à jour et/ou tout le paramétrage qui s'y rattache à un serveur WSUS en aval en mode réplica. Ce dernier effectue la tâche de distribution des mises à jour en fonction des informations reçues du serveur amont. On peut également envisager le cas où le serveur aval est amené à télécharger les mises à jour retenues par le serveur amont à partir de Microsoft Update. On allège ainsi le lien inter-sites en s'appuyant sur la connexion haut débit Internet locale pour les téléchargements tout en conservant une gestion centralisée qui limite les échanges entre serveurs à des transferts de méta données décrivant les mises à jour à télécharger.

Les échanges peuvent donc être limités aux métadonnées décrivant les mises à jour.

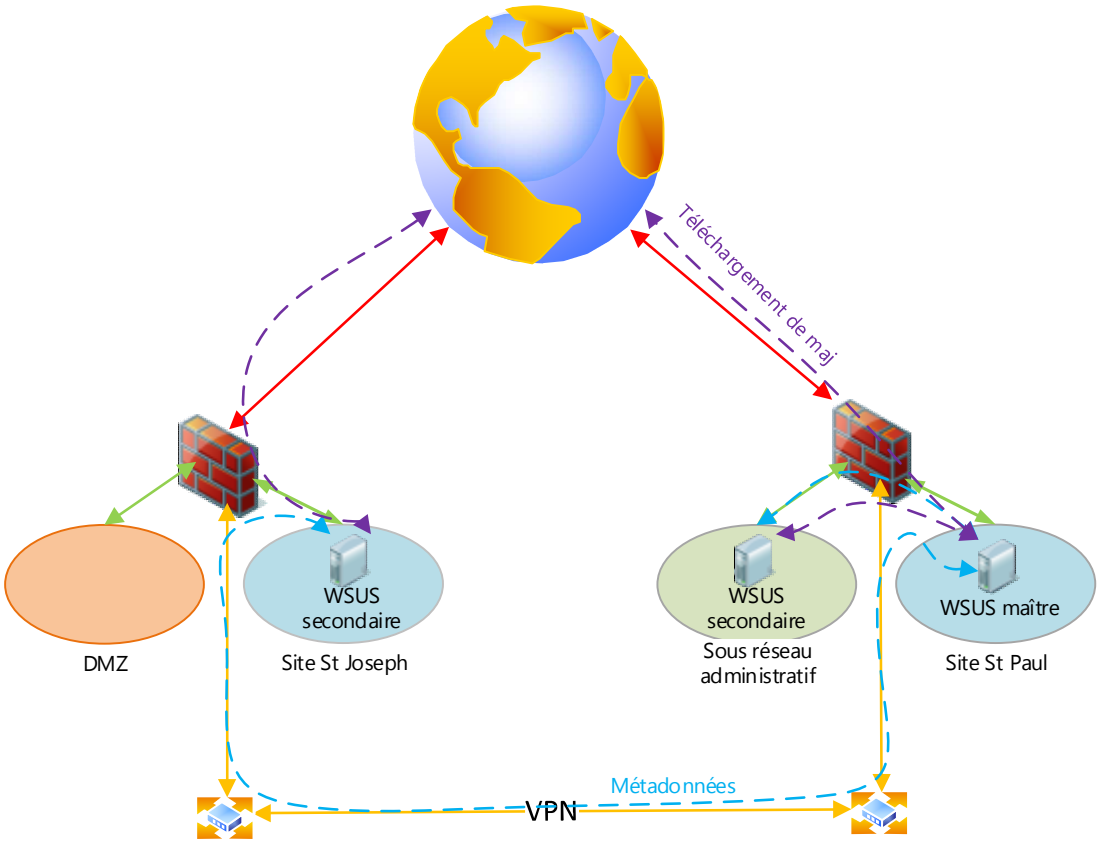


Figure 13 : architecture du système de mise à jour WSUS

Ce modèle en place entre notre serveur wsus réseau pédagogique et notre serveur Jocaste réseau administratif nous permet de réaliser une capture de trame et d'évaluer à environ 500 Ko le volume de ces métadonnées.

Display filter: ip.addr == 192.168.2.17
Ignored packets: 0 (0,000%)

Traffic	Captured	Displayed	Displayed %	Marked	Marked %
Packets	43839	192	0,438%	0	0,000%
Between first and last packet	36,463 sec	0,240 sec			
Avg. packets/sec	1202,293	798,593			
Avg. packet size	131,010 bytes	2338,370 bytes			
Bytes	5743334	448967	7,817%	0	0.000%
Avg. bytes/sec	157512,024	1867404,812			
Avg. MBit/sec	1,260	14,939			

Figure 14 : capture de trames échange WSUS

4.3.12 Flux lié à la voix sur IP

Ce flux n'est pas intégré dans le présent projet mais reste cependant une donnée à prendre en compte puisque la restructuration de la téléphonie fait partie du projet de restructuration global du groupe scolaire est doit être engagée au dernier trimestre 2015. On suppose que la compression G729 est utilisée pour la VOIP, ce qui nous amène à une consommation d'environ 28 Kbps par canal. On prévoit une dizaine de communications simultanées en période de pointe soit 280 Kbps supplémentaires qui doivent être supportés sur le lien VPN. On s'attachera à ce que la QOS appliquée sur le lien inter-sites intègre la voix et réserve en priorité le débit suffisant.

4.3.13 Récapitulatif

Tableau 1 : récapitulatif des flux transitant sur le lien inter-sites

Flux	Description du flux	Périodicité	Utilisateurs	Débit estimé/mesuré
Réplication AD	Réplication liées au modèle multi maitres d'Active Directory	Par défaut de 180 minutes. Plages paramétrable. Hors heures ouvrées	NA	Quantité de données échangées de l'ordre de 300 à 400 kb par réplication. Latence faible ~ 40 ms (données Microsoft)
Authentification AD		Heures ouvrées.	Personnel administratif site St Joseph	1 à 3 Mbps, comprend le téléchargement du profil itinérant.
Catalogue Global	Données qui décrivent les domaines d'une forêt AD	NA	NA	Nul
Changement mot de passe et réplication urgente		Heures ouvrées Pic en début d'année	Professeurs et élèves principalement	Quelques centaines de Kb par utilisateur. Latence faible ~

		scolaire		40 ms (données Microsoft)
DFSR	Synchronisation des cibles DFS en réplication	Hors heures ouvrées		1Mbps
RemoteApp	Application RDS	Heures ouvrées	Personnel administratif site St Joseph	1 à 2 Mbps
Data		Heures ouvrées		1 à 4 Mpbs
Sauvegarde	Sauvegarde données stratégiques	Hors heures ouvrées	NA	NA, passe par DFSR
WSUS	Echange de métadonnées de mises à jour entre serveurs amont et aval	Hors heures ouvrées		Quelques centaine de Ko sont échangés
Voix	VOIP	Heures ouvrées	NA	280 Kbps

Heures ouvrées : 7h00-21h00, NA : Non Applicable

On constate donc qu'un débit d'au moins 4 Mbps est nécessaire, un débit de 10 Mbps serait correct pour « encaisser » les pics de trafics identifiés.

4.4 Caractéristiques de la connexion

La solution attendue est de niveau de service OSI 3, plus précisément de routeur à routeur.

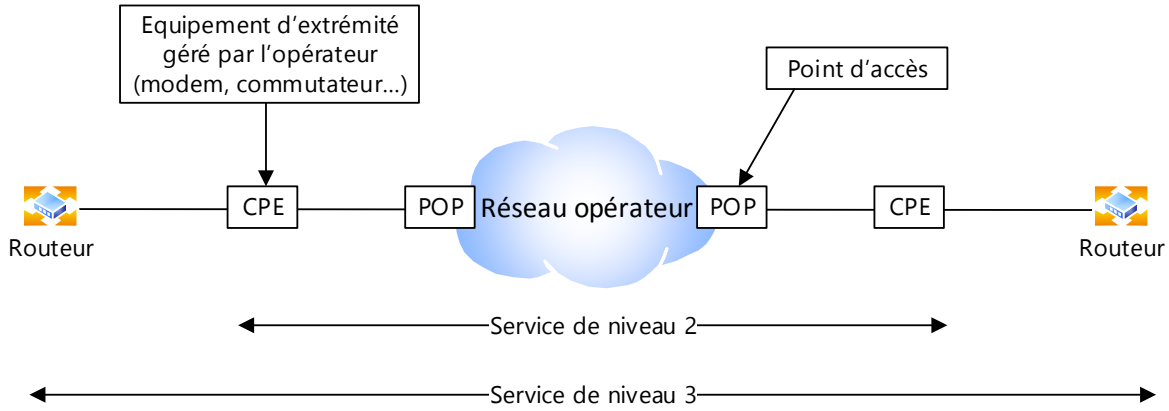


Figure 15 : schéma fonctionnel et limites de responsabilité opérateur

Le tableau suivant regroupe les caractéristiques techniques attendues de la liaison VPN :

Tableau 2 : récapitulatif des caractéristiques attendues du lien inter-sites

Critères	Engagement opérateur correspondant	Commentaires
VPN Lan to Lan symétrique niveau OSI 3	L'opérateur fournit la solution correspondante.	Pas de solution IPsec (débit et latence non garanti si l'opérateur s'appuie sur l'Internet). MPLS préféré.
Taux de disponibilité	Garantie que le réseau opérateur est disponible 99,9 % du temps.	Valeur courante chez les opérateurs.
Bande passante	L'opérateur garantit que le client disposera du débit demandé entre les deux sites pendant 100 % du	Doit être suffisamment élevée pour supporter les pics. Au moins 4 Mbps débit IP,

	temps.	10 Mbps idéalement.
Temps de transit	L'opérateur garantit le temps mis par un paquet pour aller d'un site à l'autre.	La latence est primordiale pour le bon fonctionnement notamment de la réplication AD < 40 ms, et sessions RDS.
Sécurité des flux	L'opérateur garanti la sécurité des données transmises par le biais du VPN.	Technologie MPLS
Service Level Agreement (SLA)	L'opérateur s'engage à respecter ses engagements, sous peine de pénalités.	Le SLA comprend aussi bien le respect des débits annoncés que la reprise d'activité en cas de sinistre (généralement de 4 heures)
Evolutivité du lien	L'opérateur peut faire évoluer les débits du lien.	Dans l'éventualité de la mise en place de VOIP ou d'autres services

Le tableau suivant regroupe les services associés à la liaison VPN :

Tableau 3 : services associés au VPN

Service attendu	Service proposé	Commentaires
Supervision et reporting	L'opérateur met à disposition du client des statistiques sur le VPN, fournissant de même les preuves que ses engagements sont respectés.	Besoin d'avoir une vision de l'état de réseau, d'établir des statistiques
QOS	L'opérateur fournit un moyen de caractériser les flux voix et data (cf. *Tableau 4 : QOS data lien inter-sites*).	Besoin de garantir une bande passante pour certains flux.
Accès VPN utilisateur nomade	Connexion sécurisée au réseau d'entreprise pour utilisateur nomade.	Management du SI à distance

Tableau 4 : QOS data lien inter-sites

Classe de service	Nom du flux	Adresse Source	Port Source	Adresse Destination	Port Destination	commentaires
D1 /40%						
	tse		3389		3389	TCP
D2 / 50%						
		192.168.6.31	any	192.168.2.17	any	TCP et UDP
		192.168.6.31	any	192.168.1.21	any	TCP et UDP
		192.168.6.31	any	192.168.1.250	any	TCP et UDP
		192.168.6.34	any	192.168.1.44	any	TCP
		192.168.6.7	any	192.168.1.21	any	TCP
		192.168.6.5	any	192.168.1.247	any	TCP
		192.168.6.5	any	192.168.1.118	any	TCP
D3 / 10%						
	Tout le reste		any		any	

Lors de la phase d'étude commerciale, on demandera à ce que soient bien précisés les éléments suivants :

- Délais de mise en œuvre (garantis ou pas)
- Coûts par site de mise en service
- Coûts de fonctionnement par site

4.5 Choix des opérateurs

Selon les exigences du conseil d'administration de l'OGEC, nous ne retenons que les opérateurs propriétaires de leur infrastructure physique et interlocuteurs direct afin de limiter les intermédiaires, soit ORANGE ENTREPRISE et BOUYGUES TELECOM.

Un cahier des charges est envoyé à ces deux prestataires afin de leur permettre d'établir une proposition commerciale et technique.

Compte tenu des tarifs d'accès à l'Internet s'ils sont intégrés à la solution, ces options ne sont retenues pour aucun des opérateurs.

Tableau 5 : tarifs accès Internet

Opérateur	Solution de connexion	Nombre d'utilisateurs	Prix HT / mois
ORANGE ENTREPRISE	10 Mbps IP cœur de réseau	Entre 100 et 150 utilisateurs simultanés par site	100 € HT /mois /site
BOUYGUES	10 Mbps IP cœur de réseau	Entre 100 et 150 utilisateurs simultanés par site	450 € HT / mois

Nous décidons donc de conserver nos liens ADSL actuels et d'éventuellement les faire évoluer indépendamment de notre solution d'interconnexion. Les choix suivants en découlent donc.

4.6 Sécurisation des flux

Les nouveaux risques introduits par l'éclatement du modèle de protection périmétrique et du contrôle de tous les terminaux par l'entreprise (terminaux non maîtrisés connectés au réseau, nouveaux canaux de propagation des menaces, données externalisées dans le Cloud sans protection avancée,...), doivent pouvoir être pris en compte. Il reste cependant très difficile de gérer toutes ces demandes en constante évolution et de garantir un haut niveau de sécurité d'un bout à l'autre du réseau. Nous devons pour cela nous appuyer sur du matériel performant, intégrant les dernières technologies en matière de protection réseau.

Nous nous attachons ici aux systèmes Egress/Ingress placés aux frontières du SI, ceux permettant l'ouverture sur l'Internet et l'interconnexion des différents sous-réseaux hors

routeurs VPN opérateurs dont nous n'avons pas la gestion. La sécurité « interne » du SI reste assurée par les mécanismes déjà en vigueurs (antivirus, contrôles d'accès aux services par ALC, authentification des utilisateurs…).

4.6.1 Architecture existante

Les systèmes actuellement en place afin de sécuriser notre SI s'appuient sur des machines multi-homed type PC sous Linux Debian dont le noyau est compilé pour prendre en charge les fonctionnalités de routage, de Firewall (IPtables/NetFilter) et de Proxy cache (Squid) avec filtrage d'URL SquidGuard.

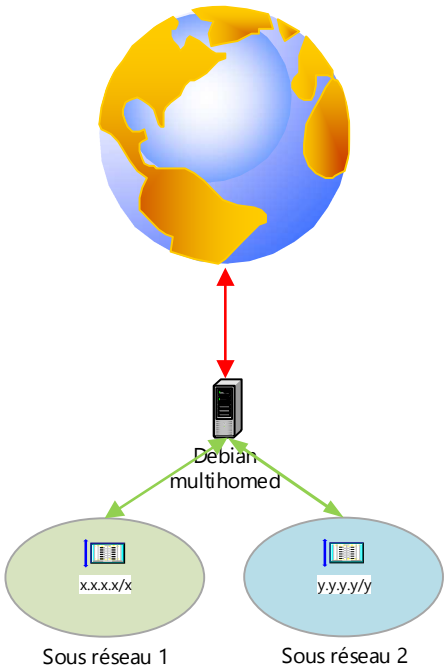


Figure 16 : modèle d'architecture firewall actuel

Ce modèle à l'évidence obsolète ne propose qu'une protection limitée et ne satisfait plus aux exigences en matière de sécurité réseau puisque les contrôles de flux s'arrêtent au niveau 4 du modèle OSI.

4.6.2 Architecture cible

Nous prenons en comptes les évolutions en matière de sécurité réseau mises en face des nouvelles menaces identifiées. Ainsi nous attendons du système cible qu'il intègre un firewall flexible et efficace, un système de détection d'intrusion IDS (Intrusion Detection System) et de prévention IPS (Intrusion Protection System), de l'analyse et du filtrage de flux applicatif, du filtrage d'URL, de la détection de virus et de spam, et du reporting en plus des fonctionnalités attendues d'un routeur/firewall telles que le routage statique, la gestion de la QOS, la gestion des VLAN, … Bref un balayage de toutes les couches OSI.

Les interactions entre sous-réseaux vont considérablement augmenter, notamment entre le sous-réseau administratif et le sous réseau pédagogique (tous sites confondus). Le traitement des flux doit donc être suffisamment rapide pour ne pas pénaliser les échanges inter réseaux. Ce dernier point nous oriente vers un matériel dédié.

En effet un firewall hardware dispose d'un système optimisé pour les tâches qu'il a à effectuer et ses ressources matérielles lui sont pleinement allouées pour les réaliser. Il en résulte également un coût de maintenance minime ainsi qu'une réduction considérable de la surface d'attaque du système puisque seul le nécessaire est installé et mis à jour, ce qui n'est pas forcément le cas de la solution type PC sous Debian. L'exploitation d'un firewall hardware est grandement facilitée de par sa gestion via interface web (ou console) et ne nécessite pas de connaissances systèmes avancées contrairement à un firewall type PC. Remonter un système Debian suite à une défaillance n'est pas aussi simple et rapide que cela, malgré les scripts, sauvegardes et connaissances adéquates. Avec du hardware et une sauvegarde des paramétrages, l'affaire est rapidement sous contrôle pour peu que l'on ait sous la main du matériel de rechange et donc d'avoir souscrit un contrat de maintenance.

En d'autres termes le hardware nous propose souplesse, puissance, robustesse ainsi que plusieurs fonctionnalités essentielles aujourd'hui absentes de nos solutions en production.

4.6.3 Réseaux WIFI

Nous souhaitons dans un avenir proche offrir aux étudiants et professeurs la possibilité de se connecter à l'internet à partir de leurs appareils mobiles type tablettes et smartphones personnels.

Ce réseau sera déployé au sein d'un VLAN dont une interface du firewall fait partie et qui agit en tant que passerelle internet. Nous souhaitons bénéficier ainsi d'un réseau isolé et d'un portail captif qui s'appuiera sur l'AD stpaul.org afin d'identifier les utilisateurs. Le firewall doit inclure un service DHCP indépendant et ne le proposer qu'aux membres du VLAN.

4.6.4 Sécurité intrinsèque du MPLS

Le MPLS garanti de par sa technologie l'étanchéité du trafic entre les clients du réseau opérateur dédié. Le système de labels permet de marquer les paquets IP et de les différencier, créant ainsi le VPN.

On choisit tout de même de placer le routeur opérateur derrière le firewall. On pourra ainsi avoir la possibilité d'isoler les sites au besoin, de contrôler les flux, d'appliquer notre police de sécurité…

4.6.5 Firewall hardware, UTM ou NGFW ?

Le firewall recherché doit intégrer un certain nombre de technologies et garantir un niveau de performances adéquat.

Il existe deux grands types de Firewall statefull, les Firewall UTM (Unified Threat Management, gestion unifiée des menaces) et les NGFW (Next Generation FireWall). Si

l'on se réfère à la littérature mise en ligne par les constructeurs, l'on remarque tout simplement qu'un Firewall UTM intègre un Firewall NGFW auquel on ajoute des fonctionnalités supplémentaires de filtrage d'URL, d'antispam… La différence est cependant plus subtile.

Un firewall utilise un modèle de sécurité positif, soit le blocage par défaut. Partant de là, on autorise des trafics identifiés comme sûres, le reste est bloqué. Aujourd'hui une application peut passer par n'importe quel port soit parce qu'elle se base sur une attribution de ports dynamique (RPC et RPCmapper), ou encore parce que les utilisateurs peuvent paramétrer leur application pour utiliser un port non standard (SSH)… Les Firewall NGFW intègrent ces nouvelles données technologiques et pratiquent une analyse du flux beaucoup plus dynamique et poussée sur toutes les couches OSI que le traditionnel port/protocole/application sur lequel sont basés de nombreux Firewalls (dont fait partie notre système actuel). La décision de laisser passer tel ou tel flux se base sur de multiples méthodes d'analyse qui, combinées permettent d'apporter une réponse immédiate aux nouvelles attaques, même celles de type 0-day.

Un Firewall UTM ne se base que sur un Firewall de niveau OSI 4 et un système IPS (Intrusion Prevention System). Il est à noter que le moteur de détection d'intrusion est en principe mis à jour automatiquement par le constructeur afin de bénéficier des dernières règles en matière de détection d'attaques ce qui vient un peu compenser la faiblesse de conception du Firewall UTM par rapport au Firewall FWNG.

Ces éléments sont à prendre en compte, puisqu'à l'évidence le paramétrage et l'efficacité du Firewall vont dépendre de la technologie employée. Il en découle également qu'un Firewall FWNG ne remplira pas d'emblée les tâches de filtrage d'URL par exemple et nécessitera soit la souscription à des options supplémentaires soit à la mise en œuvre de matériels supplémentaires.

D'une façon générale, la solution Firewall NGFW est plus onéreuse que la solution UTM plus traditionnelle. Tout est question de compromis entre les besoins exprimés et le budget à disposition.

Nous nous appuyons sur les propositions de nos fournisseurs historiques pour réduire notre champ d'investigation à deux constructeurs : StormShield et WatchGuard.

4.6.6 Architectures proposées

4.6.6.1 Traitement centralisé des flux sur un site unique

Notre projet est bel et bien de consolider et de faciliter la gestion du SI en regroupant et mutualisant nos moyens informatiques tout en en améliorant la sécurité du réseau. Ainsi nous proposons de regrouper les interconnexions des différents sous-réseaux autour d'un nœud par lequel transiteront tous les flux permettant ainsi une analyse centralisée des différents trafics.

Dans le schéma présenté ci-dessous, le nœud d'interconnexion est matérialisé par un firewall/routeur. Cet appareil devra regrouper toutes les fonctionnalités liées à la sécurisation des flux.

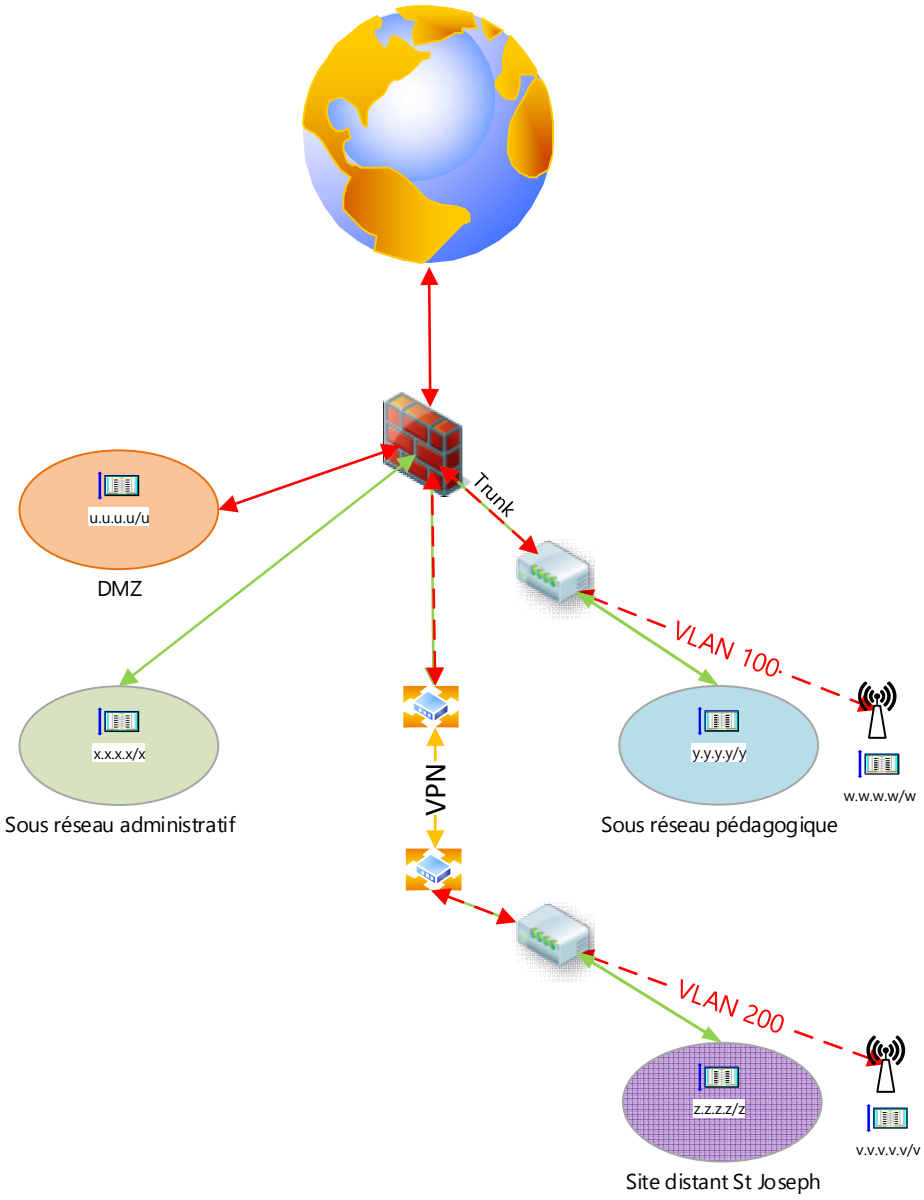


Figure 17 : Architecture cible centralisée

Dans l'étude réalisée lors de l'appel d'offre pour la mise en place du lien VPN, nous avons pu définir le volume et la nature des flux qui transiteront entre nos sites distants, une bande passante de 4 Mbps s'est avérée être un minimum avec des consommations à la hausse dans les années à venir.

Les statistiques des flux internet de nos sites sont les suivantes :

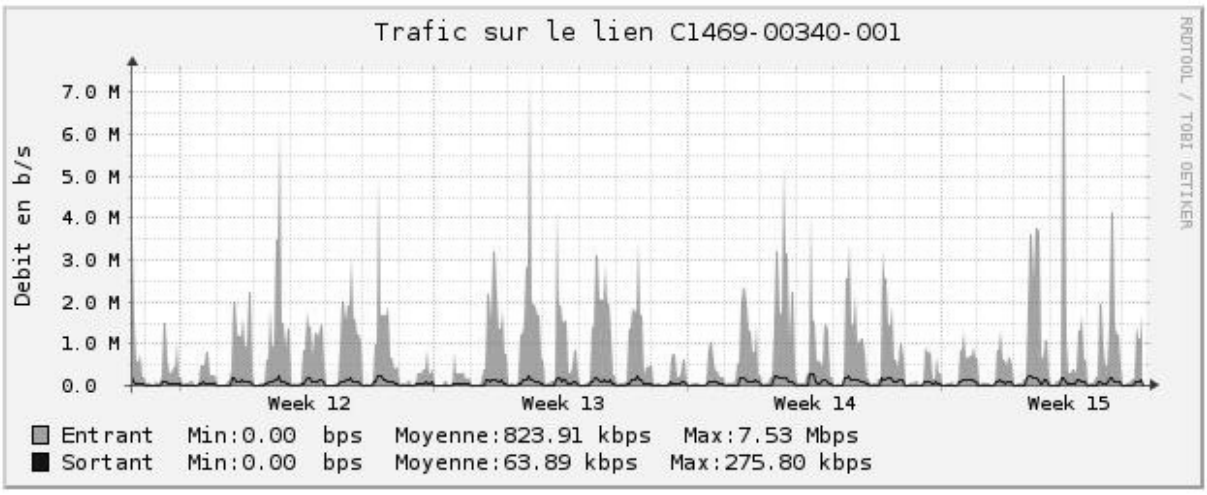


Figure 18 : Statistiques mensuelles lien ADSL 18 Mbps max site St Joseph

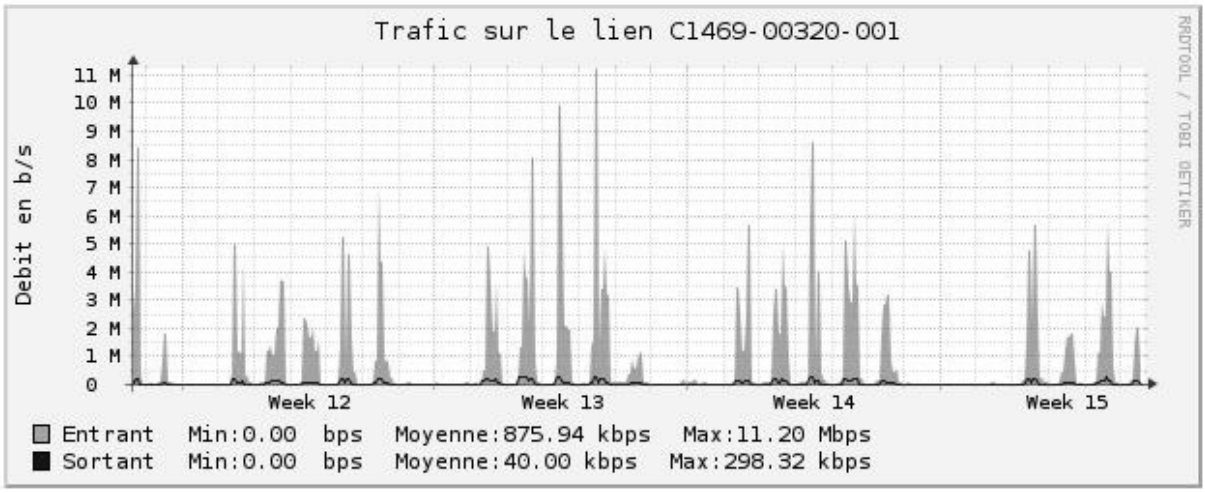


Figure 19 : Statistiques mensuelles lien ADSL 18 Mbps max site St Paul

Tableau 6 : récapitulatif des statistiques mensuelles ADSL

	Moyenne débit entrants	Moyenne débit sortants	Max débit entrant	Max débit sortant
Site St Joseph	823,91 kbps	63,89 kbps	7,53 Mbps	275,80 kbps
Site St Paul	875,94 kbps	40 kbps	11,20 Mbps	298,32 kbps
Somme	**1,7 Mbps**	**103,86 kbps**	**18,73 Mbps**	**574,12 kbps**

Un lien ADSL 18 Mbps max unique (mesuré en débit descendant à 15,35 Mbps et 16,47 Mbps pour respectivement le site St Paul et le site St Joseph lors de l'audit ESDI) pourrait donc supporter tout le volume engendré par la navigation Internet de nos sites tout en notant une baisse sensible de la qualité de réponse des services web dans leur ensemble. Il reste cependant possible d'agréger un lien WAN supplémentaire au besoin et de répartir la charge entre ces deux passerelles Internet.

Ces données nous permettent donc d'envisager une architecture réseau dans laquelle le lien VPN joue un rôle prépondérant puisqu'il permet d'ouvrir le site St Joseph à l'Internet par le biais du lien ADSL 18 Mbps max du site St Paul. Le débit sur le site St Joseph restera cependant plafonné à 1 ou 2 Mpbs débit IP selon la QOS mise en place.

Le firewall doit être à même de disposer de suffisamment de ressources matérielles pour traiter l'ensemble des flux.

4.6.6.2 Traitement des flux répartis sur chaque site distant

Dans ce modèle, on retrouve un routeur/firewall sur chaque site selon l'architecture ci-dessous :

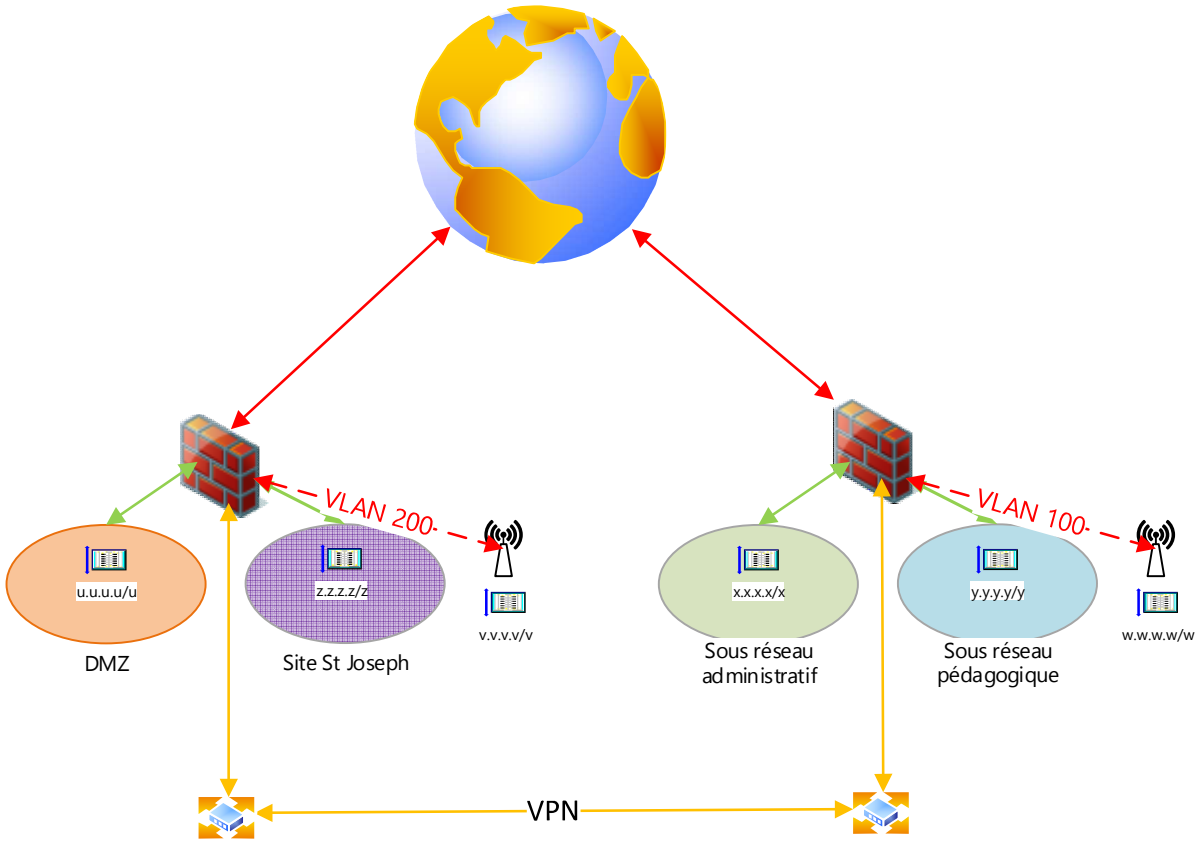


Figure 20 : architecture cible

Dans cette architecture, chaque site conserve son lien ADSL 18 Mbps max, un firewall sur site est garant de la sécurité réseau.

Les exigences en termes de ressources matérielles sont moins importantes que dans la solution centralisée.

4.6.6.3Comparaison des deux solutions

Chaque architecture présente des avantages et des inconvénients qu'il s'agit de bien identifier afin de faire le choix le plus adéquat.

Tableau 7 : comparaison des deux solutions

Architecture centralisée	Architecture répartie	Commentaire
Un seul firewall à manager	2 Firewalls à manager	Interface de gestion centralisée envisageable si gestion de plusieurs firewalls ? Coût firewall solution distribuée > solution centralisée ?
1 seul lien ADLS pour le groupe	1 lien ADSL pour chaque site	Bande passante Internet pleine et entière par site dans la solution distribuée, réorientation du flux Internet vers un site en cas de coupure et lien VPN moins sollicité.
Relai DHCP à mettre en place pour VLAN 200	DHCP VLAN géré par site	Relai DHCP en option sur le lien VPN.
DMZ à « déplacer » sur Site St Paul		Demande IP publique Altitude Telecom et maj DNS Gandi

4.6.7 Fonctionnalités et dimensionnement du/des Firewall(s)

Nous établissons deux profils de fonctionnalités définis par l'utilisation qui est actuellement faite du firewall sur chaque site. Ces profiles correspondent à l'architecture distribuée explicitée ci-dessus :

- Sur le site St Joseph, le firewall doit assurer la protection et l'accès à l'Internet entre le réseau pédagogique et l'Internet connecté à 18 Mbps max en ADSL via un routeur opérateur. Il doit également permettre l'accès à la DMZ dans laquelle est placé notre serveur web qui sera accédé aussi bien du LAN que de l'Internet via une règle de NAT 1 pour1.
- Sur le site St Paul, le besoin se situe entre les deux sous-réseaux administratif et pédagogique connectés à 1 Gbps. Le firewall doit également gérer les accès à l'Internet du site St Paul pour l'ensemble des utilisateurs via un routeur opérateur en ADSL 18 Mbps max. Le site St Paul doit également proposer des connexions VPN IPSec à des fins entre autres de dépannage à distance.

Le firewall de la solution centralisée devra fusionner les fonctionnalités décrites dans les profils du modèle distribué.

4.6.7.1Authentification des utilisateurs

Il s'agit ici d'authentifier les utilisateurs qui vont utiliser les services web à partir des machines des réseaux du groupe scolaire aussi bien pédagogique qu'administratif ou encore Wifi. Il existe de nombreuses méthodes d'authentification, cependant nous souhaitons proposer un système aussi simple et transparent que possible en nous appuyant sur l'AD. Il est à prendre en compte que l'authentification transparente des objets multiutilisateurs (plusieurs authentifications depuis une même adresse IP, typiquement nos fermes RDSH) ne peut être réalisée que par la méthode SPNEGO et n'est pas supportée par la méthode agent SSO.

4.6.7.2IPS

Le rôle de l'IPS (Intrusion Prevention System) est de stopper une attaque réseau au moment où elle est détectée en se basant sur l'analyse en temps réel du trafic réseau (comportements et signatures sont régulièrement mis à jour).

Un mode Monitor est un plus. Ce dernier permet de tester les réglages avant mise en production et fonctionne à la manière d'un IDS (Intrusion Detection System), et de détecter les faux positifs.

Il est bien évident que le Firewall doit être capable de traiter rapidement les flux qui le traversent afin de le rendre totalement transparent à tel point que les utilisateurs l'oublient. Cependant la performance a un prix, et il serait inutile de placer un firewall surdimensionné sur une interconnexion ne traitant qu'un trafic d'au plus de 20 Mbps comme sur le site St Joseph par exemple. En ce qui concerne le site St Paul, on peut aborder le problème de deux façons différentes.

La première consiste à quantifier précisément les flux en transit afin de permettre un choix précis de matériel. Cette approche reste difficile et soumise à de fortes fluctuations.

On peut adopter un autre point de vue et se dire que les différents liens peuvent nécessiter au plus un traitement de l'ordre du Gbps et baser notre choix sur ce dernier postulat. Au vu des performances affichées par les constructeurs, les modèles d'entrée de gamme permettent pour la plupart d'atteindre de telles vitesses de traitement.

4.6.7.3Filtrage d'URL

La mise en œuvre d'une base de filtrage URL suffisamment exhaustive consomme une grande zone de stockage. Les bases de filtrage URL avancées ne peuvent donc souvent pas être déployées sur les produits, d'où le stockage en cloud. On envisage une solution de base de filtrage hébergée dans le cloud.

4.6.7.4Inspection SSL

De plus en plus de trafics sont chiffrés pour accéder par exemple à des applications web de façon sécurisée en s'appuyant sur le protocole https. Ces dernières, légitimes ou non, doivent être contrôlées. On doit pouvoir également exclure certains flux sécurisé de

l'inspection SSL, notamment pour le webmail académique qui utilise un certificat auto généré et ne s'appuie pas sur l'architecture 3 tiers habituelle.

4.6.7.5Certification EAL4+

La certification EAL4+ est une norme de sécurité internationale réservée à des produits de sécurité informatique. Elle représente le plus haut niveau d'assurance qualité attribuable à un produit commercial. Cela nous garantit que le matériel a passé avec succès tous les tests de critères communs (contrôles de sécurité).

4.6.8 Synthèse des modèles de firewall retenus

Tableau 8 : comparatifs des différents modèles de firewall FWNG

Description de la fonctionnalité	Besoin	StormShield NS700	StormShield NS900	WatchGuard XTM 330	WatchGuard XTM 525
Vitesse de traitement du Firewall + IPS	De l'ordre du Gbps	2 Gbps	3 Gbps	1,4 Gbps	3 Gbps
Connexions simultanées	Donné pour 200 utilisateurs simultanés max ou 500 selon l'architecture retenue	600 000 Recommandé pour 150-200 utilisateurs	1 200 000 Recommandé pour 300-500 utilisateurs	40 000	100 000
Débit VPN IPSec AES 128/SHA1	40 Mbps	650 Mbps	800 Mbps	240 Mbps	350 Mbps

Interfaces 10/100/1000	6 interfaces indépendantes minimum	12	12	7	6
WIFI	non	non	non	non	non
VLAN 802.1Q	oui	256	512	75	200
Mode	Statique	Oui	Oui	Oui	Oui
NAT/PAT	Oui	Oui	Oui	Oui	Oui
Limitation bande passante	Oui	Oui	Oui	Oui	Oui
IPS	Oui	Oui	Oui	Oui	Oui
Inspection des flux applicatifs	Oui	Oui	Oui	Oui	Oui
Antivirus et antispam	Oui	ClamAV ou KAV	ClamAV ou KAV	Solutions propriétaires	Solutions propriétaires
Inspection SSL	Oui	Oui	Oui	Oui	Oui
Filtrage d'URL	Oui	Oui	Oui	Oui	Oui
Intégration avec Active Directory	Oui	Oui	Oui	Oui	Oui
Méthodes d'authentification SPNEGO, Kerberos, LDAP	Oui	Oui	Oui	Oui	Oui

Portail captif	Oui	Oui	Oui	Oui	Oui
VPN IPsec	5 à 10 connexions simultanées	1000	1000	55	55
Double partition RAID1	Oui	Oui	Oui	Oui	Oui
Maj régulière/automatique	Oui	Oui	Oui	Oui	Oui
Certifications EAL4+	Oui	Oui	Oui	En cours	En cours
Système d'alerte par email	Oui	Oui	Oui	Oui	Oui
Journaux et reporting	Oui	120 Go	120 Go	Oui	Oui

4.7 Synthèse des offres d'interconnexion et choix du matériel

4.7.1 Choix de l'opérateur

Plusieurs offres techniques nous ont été proposées, chacune avec des caractéristiques différentes en termes de débits, d'évolutivités…

La société BOUYGUES nous a d'abord proposé un lien VPN MPLS 8 Mbps cuivre sans évolutivité possible, ce dernier point étant lié aux contraintes physiques de la ligne. Nous avons fait évoluer cette offre sur de la fibre optique à 10 Mbps, ce débit correspondant au plus juste à nos demandes et aux offres possibles (le gap de prix entre

l'offre 5 Mbps et 10 Mbps étant minime) et cela dans la perspective d'opter pour une solution pérenne est facilement évolutive.

La société ORANGE ENTREPRISE a suivi le même cheminement.

Tableau 9 : comparatif des offres reçues et négociées avec les opérateurs

	ORANGE ENTREPRISE	BOUYGUES	Remarques
Type d'interconnexion	Fibre optique 10 Mbps	Fibre optique 10 Mbps	
Temps de déploiement	80 jours ouvrés	70 jours ouvrés	
Technologie VPN	MPLS	MPLS	
Taux de disponibilité	Garanti	99,85 % l'an	
Temps latence garanti	< 10 ms	< 30 ms	
Gigue	Réduite	< 15 ms	
GTR	4H 6/7	4H 6/7	
QOS	5 COS (3 data, 1 voix, 1 vidéo)	5 COS (3 data, 1 voix, 1 vidéo)	
Frais de mise en service	7 900 € HT	13 000 € HT	Remise à 100 %
Mensualités de la solution	1 574 € HT	1 690 € HT	

Le choix final se porte sur l'offre de la société ORANGE ENTREPRISE d'autant plus que cette dernière nous propose de mettre en place au plus vite une solution cuivre 8 Mbps temporaire compte tenu des délais de mises en service de la solution fibre optique, et ainsi de permettre au projet de consolidation de suivre normalement son cours.

4.7.2 Choix des Firewalls

Au vu des tarifs et fonctionnalités demandés, nous optons pour des firewalls StromShield en location chez l'opérateur/partenaire StormShield Orange.

La location est le choix le plus judicieux, puisqu'au terme du contrat le renouvellement de l'offre s'appuiera sur du matériel à jour et offrant les dernières technologies en matière de sécurité réseau. L'option d'achat semble plus économique, mais nous rend propriétaire d'un matériel voué à l'obsolescence à très court terme.

La demande de cotation en fonction des deux architectures proposées, ainsi que les avantages et contraintes de chaque solution, nous permettent d'arrêter notre choix sur la solution distribuée.

Tableau 10 : synthèse financière des offres firewall

Description de produit	Prix	Quantité	Total	
Achat SN-900 + pack Premium UTM Security + maintenance annuelle	11 032 € HT	1	11 032 € HT la première année, puis 402,04 € HT de maintenance/an	Solution centralisée
Location 36 mois StromShield SN-900 + pack Premium UTM Security + maintenance	371,53 € HT/mois	1	371,53 € HT/mois soit 13 375,08 € au bout des 36 mois de location	
Achat SN-700 + pack Premium UTM Security + maintenance annuelle	5 577,66 € HT	2	11 155,22 € HT la première année, puis 402,04 € HT de maintenance/an	Solution distribuée
Location 36mois StromShield SN-700 + pack Premium UTM Security + maintenance	195,76 € HT/mois	2	**376,27 € HT/mois** soit 13 545,72 € au bout des 36 mois de location	

4.8 Phases de déploiement du matériel

Le déploiement des firewalls intervient avant la mise en place du VPN Orange et doit donc venir s'intégrer à l'existant. De plus les connexions Internet de chaque site, bien que conservées feront l'objet d'un nouveau marché public mené par la région Franche-Comté. Nous souhaitons d'ailleurs à ce moment-là abandonner le VPN Altitude Télécom existant et demanderons l'attribution d'une IP publique fixe sur notre lien Internet site St Joseph en lieu et place du passage obligatoire par le cœur de réseau Altitude Télécom seule solution possible à l'époque pour obtenir une IP publique.

Le déploiement final passera donc par plusieurs étapes détaillées ci-après.

4.8.1 Urbanisation réseau actuel de l'OGEC

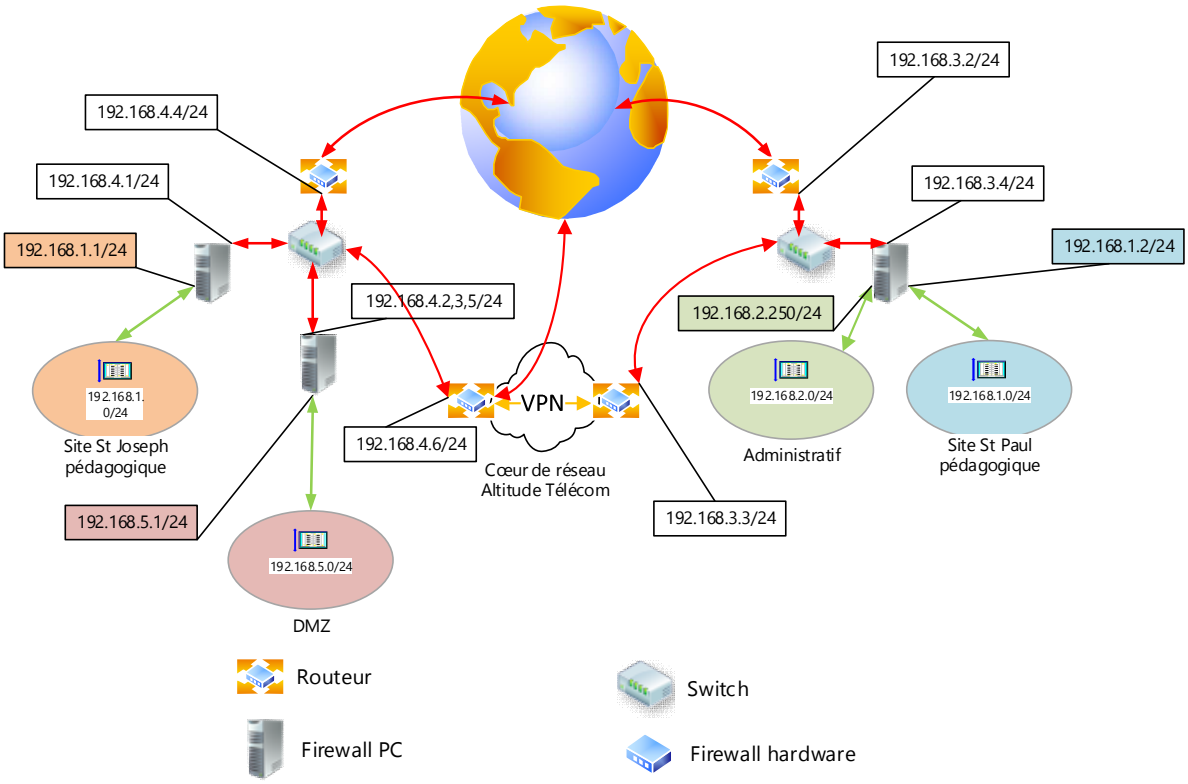


Figure 21 : urbanisation actuelle de l'OGEC

4.8.2 Urbanisation réseau intermédiaire 1 de l'OGEC

L'adressage IP des différents sites et sous réseaux est modifié afin de s'intégrer au sein du futur LAN étendu de l'OGEC.

Les firewalls sont en place et s'intègrent à l'existant en remplaçant les machines multi homed.

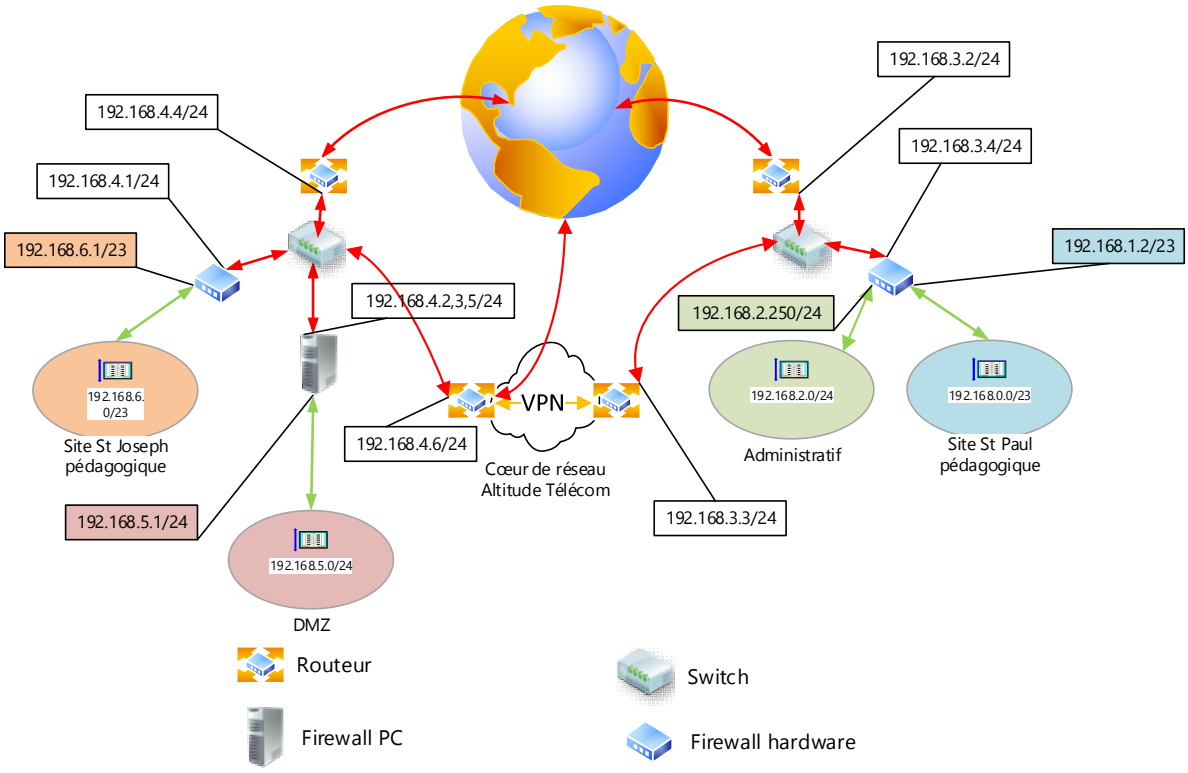


Figure 22 : urbanisation intermédiaire 1 de l'OGEC

4.8.3 Urbanisation réseau intermédiaire 2 de l'OGEC

Le VPN Orange est en place. Le VPN Altitude Télécom est abandonné sur le site St Paul mais conservé sur le site St Joseph afin d'exposer le serveur web.

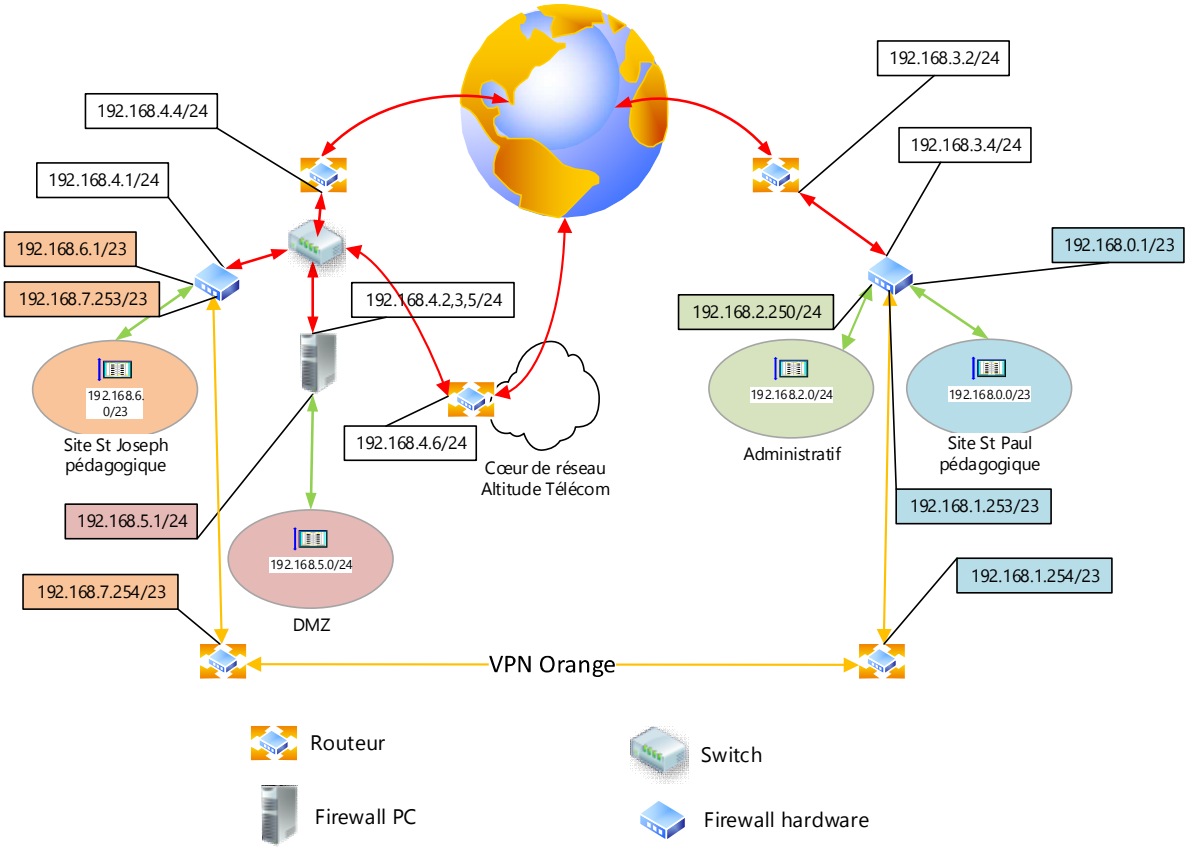


Figure 23 : urbanisation intermédiaire 2 de l'OGEC

4.8.4 Urbanisation réseau finale de l'OGEC

Une IP publique fixe est attribuée au lien Internet site St Joseph et permet d'abandonner totalement le VPN Altitude Télécom.

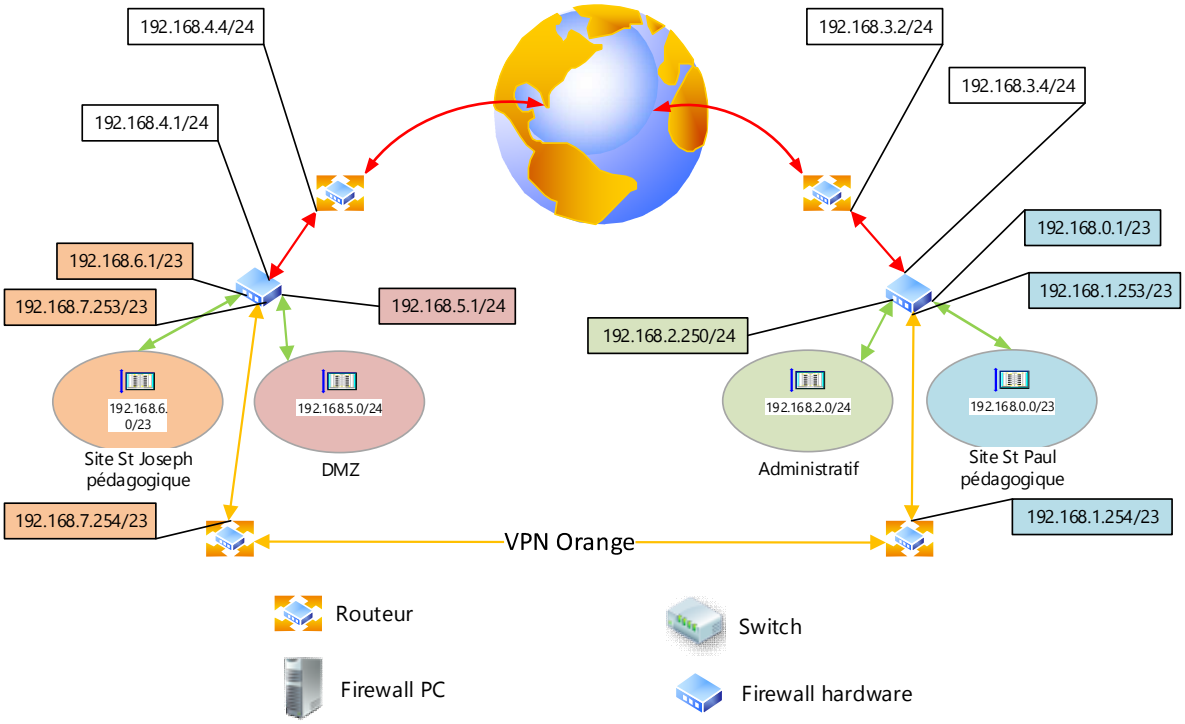


Figure 24 : urbanisation finale de l'OGEC

4.8.5 Réadressage IP des différents sites

Le plan d'adressage des sites St Joseph et St Paul doit être modifié afin de devenir des domaines de diffusion à part entière au sein du futur LAN étendu de l'OGEC. De plus, le parc informatique ayant considérablement augmenté, il convient de prévoir un plan d'adressage IP en conséquence. Pour le site St Joseph, il s'agit d'un changement complet d'adressage IP CIDR.

Tableau 11 : plan d'adressage IP du sous-réseau 192.168.6.0/23 site St Joseph

Plan d'adressage IP site St Joseph	
@ du réseau	192.168.6.0/23
Première @IP disponible	192.168.6.1
Dernière @IP disponible	192.168.7.254
@ de diffusion	192.168.7.255

Pour le site St Paul, il s'agit d'un changement de masque de sous-réseau.

Tableau 12 : plan d'adressage IP du sous-réseau 192.168.0.0/23 site St Paul pédagogique

Plan d'adressage IP site St Paul	
@ du réseau	192.168.0.0/23
Première @IP disponible	192.168.0.1
Dernière @IP disponible	192.168.1.254
@ de diffusion	192.168.1.255

Tableau 13 : plan d'adressage IP du sous-réseau 192.168.0.0/24 site St Paul administratif

Plan d'adressage IP site St Paul Administratif inchangé	
@ du réseau	192.168.2.0/24
Première @IP disponible	192.168.2.1
Dernière @IP disponible	192.168.2.254
@ de diffusion	192.168.2.255

Enfin l'adressage de la DMZ site St Joseph reste inchangé :

Tableau 14 : plan d'adressage IP du sous-réseau 192.168.5.0/24 DMZ site St Joseph

Plan d'adressage IP DMZ inchangé	
@ du réseau	192.168.5.0/24
Première @IP disponible	192.168.5.1
Dernière @IP disponible	192.168.5.254
@ de diffusion	192.168.5.255

4.8.5.1Les différentes tâches à effectuer

- Répertorier toutes les IP statiques machines type serveurs, switchs, imprimantes …
- Répertorier les services impactés par site

- Modifier le scope DHCP pour refléter le changement de masque. On choisit de gérer l'adressage DHCP par site plutôt que de passer par un relai DHCP, ceci afin de conserver un maximum d'autonomie sur les sites en cas d'indisponibilité du lien inter-sites.
- Procéder aux modifications du masque et de l'IP sur les machines, switchs, imprimantes qui ne sont pas encore adressées par DHCP. On optera pour un adressage automatique lorsque cela est possible.

4.8.5.2Inventaire des services impactés

Seuls les services opérant directement sur les couches 2, 3 et 4 du modèle OSI peuvent être impactées par un changement d'adresse IP. A moins de paramétrages spécifiques, tous les services des couches supérieures ne sont pas touchés tant que le système de résolution d'adresse et de localisation de services est fonctionnel. On réduit donc les opérations sur les machines fournissant les services DNS et DHCP avec une attention particulière portée sur les services ADDS.

Tableau 15 : rôles installés sur les serveurs

Rôle	Impacté	Commentaires
Serveur d'application – composants COM	Non	
Serveur IIS	Non	Toutes les IP sont autorisées dans les liaisons de site pour le protocole http
Service d'impression	Oui	Adapter les nouvelles IP de ports
Service de déploiement Windows	Non	
DNS	Oui	Adapter les zones inversées
ADDS	Oui	
WSUS	Non	
Serveur DHCP	Oui	Adapter le scope
Service de certificats	Non	
Services de stratégies d'accès réseau	Non	
Service de fichiers -DFS	Non	

- Firewall : Modifier l'adressage IP et le script Netfilter afin de refléter les changements opérés.
- Services DNS : Ajouter les zones inverse dans le DNS pour les sous-réseaux modifiés ou ajoutés afin de permettre les inscriptions lors de la remise du bail

DHCP. Apporter les modifications nécessaires au système de Round Robin mis en place pour équilibrer la charge sur les fermes RDS.

- Sites et services : Adapter les sous-réseaux de site au nouvel adressage IP
- Services DHCP : Les serveurs DHCP doivent refléter le nouvel adressage. On en profitera pour passer un certain nombre d'éléments en adressage dynamique avec réservation (les copieurs en l'occurrence).
- Serveurs d'impression : Ajouter les nouveaux ports TCP et les mapper aux imprimantes correspondantes.
- Proxy web : Modifier l'adressage IP du serveur Proxy, les ACL du fichier de configuration de Squid ainsi que dans le fichier de configuration de SquidGuard afin de refléter les changements opérés.
- GLPI : Ce service de gestion de parc informatique est hébergé sur la machine serveur.Reporter la modification de l'adressage dans les fichiers de configuration d'apache apache httpd.conf, ainsi que dans le fichier de connexion à la base de données GLPI config.db.
- BCDI : Réadressage du serveur BCDI à effectuer sur les clients BCDI. Opération manuelle à effectuer par les documentalistes sur leurs postes → Information à transmettre.

5 Renommage du domaine AD stpaul.org Administratif

Une relation de confiance unidirectionnelle entre notre forêt Active Directory administrative et notre forêt AD pédagogique est à mettre en place. Cette relation d'approbation permettra aux utilisateurs administratifs de se connecter en toute transparence sur l'ensemble de notre SI. A contrario les utilisateurs pédagogiques resteront cantonnés à la partie pédagogique. Pour établir ce lien entre ces deux forêts, l'unicité des noms de forêt et de domaine doit être respectée. Historiquement nos forêts AD n'ont pas été montées sans la perspective d'une interconnexion et partagent depuis cette époque le même nom d'où la nécessité d'en renommer une des deux.

La procédure de renommage implique des opérations sur chaque contrôleur de domaine et chaque station de travail. La forêt administrative étant beaucoup moins importante en termes de nombre de serveurs, de stations de travail, et de services impactés, notre choix se porte donc sur cette dernière.

5.1 Planning

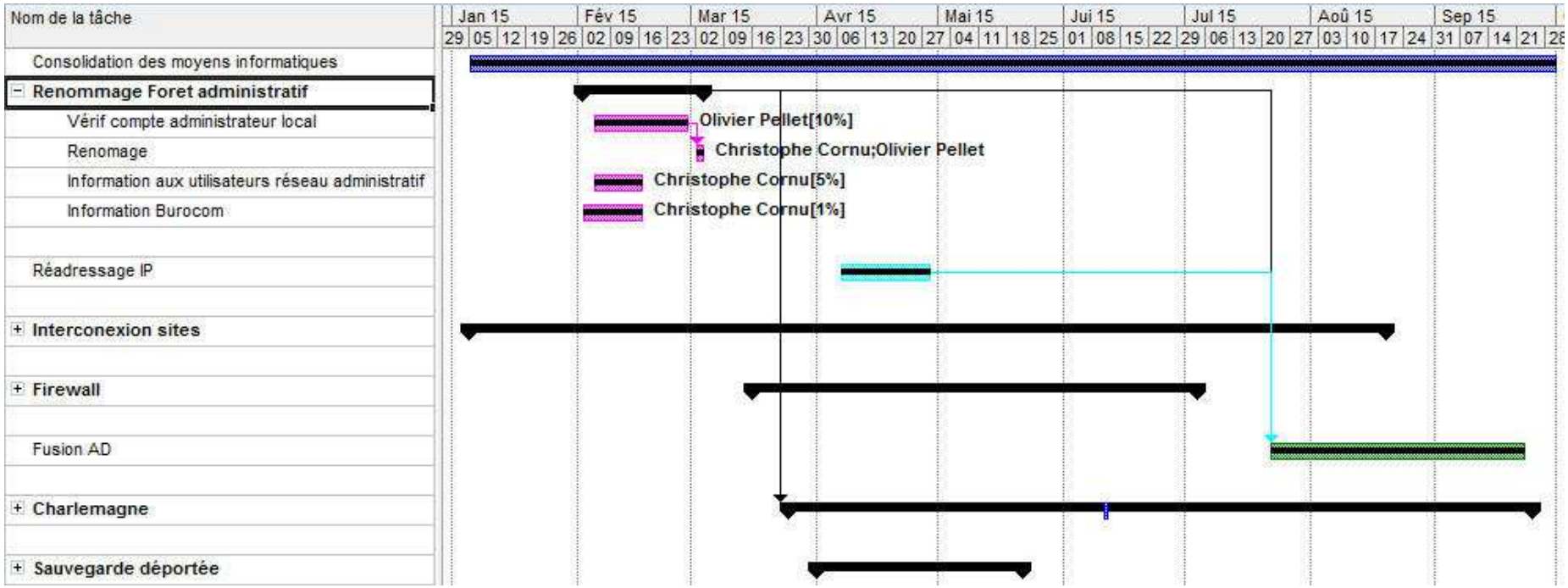


Figure 25 : planning de renommage de la forêt administratif

5.2 Qu'est-ce que le renommage de domaine Active Directory

Ce processus est utilisé lorsque l'on doit renommer un ou plusieurs domaines AD, ou lorsque l'on doit modifier la structure d'un arbre AD au sein d'une forêt. Cela implique la mise à jour du DNS, des relations d'approbations, des GPO et des Service Principal Name (SPN).

Dans une forêt certaines opérations ne sont pas possibles :

- Changer de domaine racine. Il est par contre possible de changer le nom du domaine racine.
- Ajouter ou supprimer des domaines de la forêt. Le nombre de domaines dans la forêt doit rester identique.
- Renommer un domaine avec un nom de domaine d'un autre domaine de la forêt au cours de la même opération de renommage. Cette opération est toutefois possible en enchaînant les renommages, le premier « libérant le nom de domaine », le second le réattribuant.

Le processus de renommage est décomposé en une série de changements opérés indépendamment sur chaque DC de la forêt. Il s'agit de commandes de mises à jour de la base AD reflétant le renommage et qui, étant opérés individuellement sur les DC, ne sont pas transmises au travers de la réplication AD à l'ensemble de la forêt.

L'outil Rendom permet de réaliser les opérations nécessaires au renommage :

- Gel de l'état courant de la forêt afin qu'aucun changement ne soit ni effectué ni répliqué durant l'opération de renommage.
- Préparation des changements de la base AD du ou des domaines de la forêt pour le renommage au travers de multiples scripts.
- Exécution du renommage
- Nettoyage des noms de domaines

L'outil Gpfixup permet de corriger les GPO afin qu'elles reflètent le changement de nom de domaine.

Ces outils sont inclus dans le Remote Server Administration Tools (RSAT) installés sous forme de features sur les serveurs Windows 2008 R2.

5.3 Scénarii de renommage de domaine

Les possibilités de renommage permettent de réaliser des changements de plusieurs sortes au sein d'une forêt AD. Par exemple :

- Renommer des domaines sans repositionnement dans la structure de la forêt
- Créé une nouvelle arborescence en repositionnant les domaines dans le même arbre, ou dans un nouveau.
- Créer une nouvelle racine d'arborescence
- Réutiliser un nom de domaine

5.3.1 Renommage sans repositionnement

Le renommage n'impacte pas la structure de la forêt. C'est cette opération que nous allons réaliser.

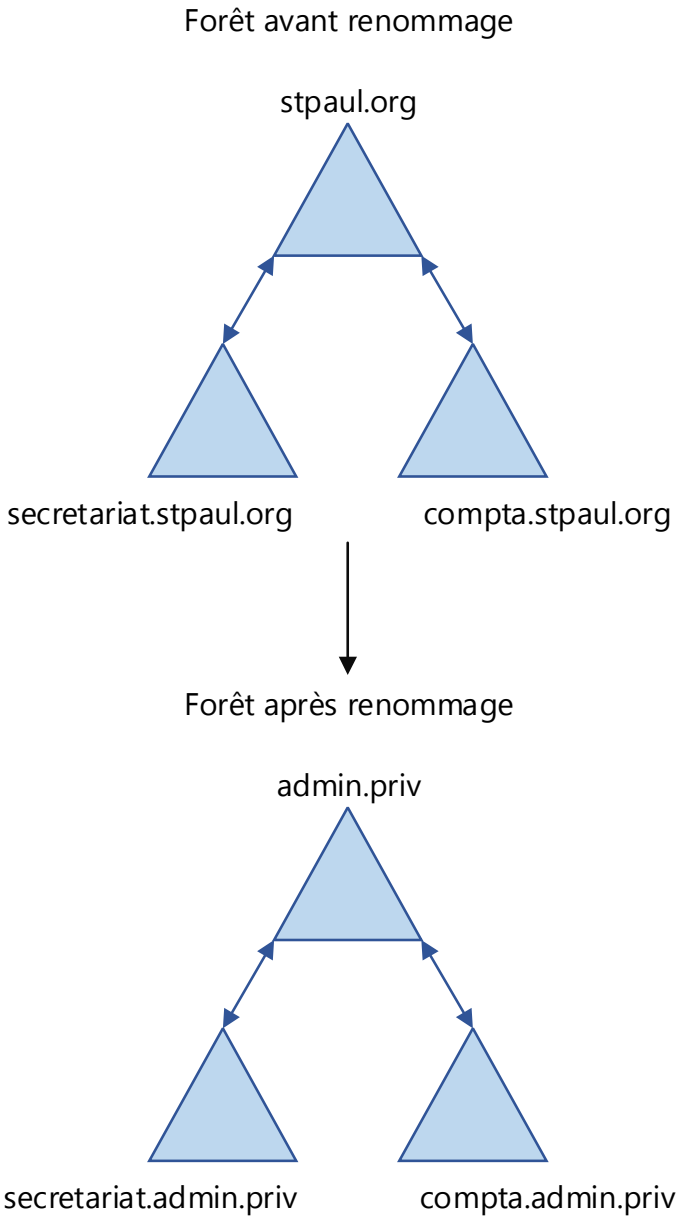


Figure 26 : exemple de renommage de forêt AD sans repositionnement

En renommant le domaine racine de la forêt, une condition est créée dans laquelle tous les domaines enfants du domaine racine de l'arborescence doivent également être renommés afin de préserver la structure originelle de la forêt.

5.4 Dépendance des opérations de renommage et interactions avec les technologies en place dans le SI

5.4.1 Effet sur la résolution DNS

Chaque client ADDS trouve les services ADDS grâce aux enregistrements SRV inscrits dans la zone DNS de son domaine. Si la zone DNS est indisponible, le client ADDS ne peut fonctionner correctement. Il faut donc s'assurer qu'une zone pour chaque domaine renommé soit créée avant le renommage. Il est recommandé de configurer ces nouvelles zones pour qu'elles acceptent les mises à jour dynamiques sécurisées et non sécurisées le temps du renommage.

Au cours des opérations de renommage, les noms des DC et des serveurs membres doivent être mis à jour :

- Les suffixes DNS des DC concernés doivent être mis à jour pour refléter les changements de nom de domaine
- Les suffixes des serveurs membres et des stations sont mis à jour soit lors de la réplication du changement de nom de domaine, soit par GPO en modifiant le suffixe DNS avant le changement de nom de domaine, une solution excluant l'autre. Attention cependant, le suffixe DNS n'est mis à jour que lorsque l'on se logue à la machine et que l'on redémarre celle-ci. Démarrer une machine et la redémarrer au bouton n'aura aucun effet. Il faudra donc s'assurer qu'un compte administrateur local est actif pour réaliser cette opération.

5.4.2 Effets sur la réplication lors du renommage d'un grand nombre de machines membres

Dans les conditions de renommage automatique d'un nombre important d'ordinateurs membres, c'est-à-dire sans utiliser de GPO pour modifier le suffixe DNS de ces machines, la réplication de ces changements peut avoir un impact néfaste sur le trafic réseau. Le changement de FQDN déclenche la mise à jour des attributs dnsHostName et servicePrincipalName du compte ADDS de la machine. De plus les enregistrements A

et les pointeurs DNS doivent également être mis à jour. Dans un environnement Windows pur, c'est-à-dire ou les services DNS sont pris en charge par le DC, on imagine aisément la charge à laquelle doivent faire face ces machines en sus de la réplication entre DC de ces mises à jour et autres services installés. Il est donc recommandé de procéder via GPO à la mise à jour du suffixe principal des machines avant le renommage. De cette manière, les changements qui doivent être opérés peuvent être planifiés et avoir un impact maîtrisé sur la bande passante et les DCs en constituant par exemple des groupes de machines à traiter.

Il faudra cependant configurer le domaine pour qu'il accepte les machines dont le suffixe DNS est différent du nom DNS de domaine en les ajoutant à l'attribut de l'objet domaine. Cette opération est à réaliser avant la mise en place du changement de suffixe DNS sur les machines membres.

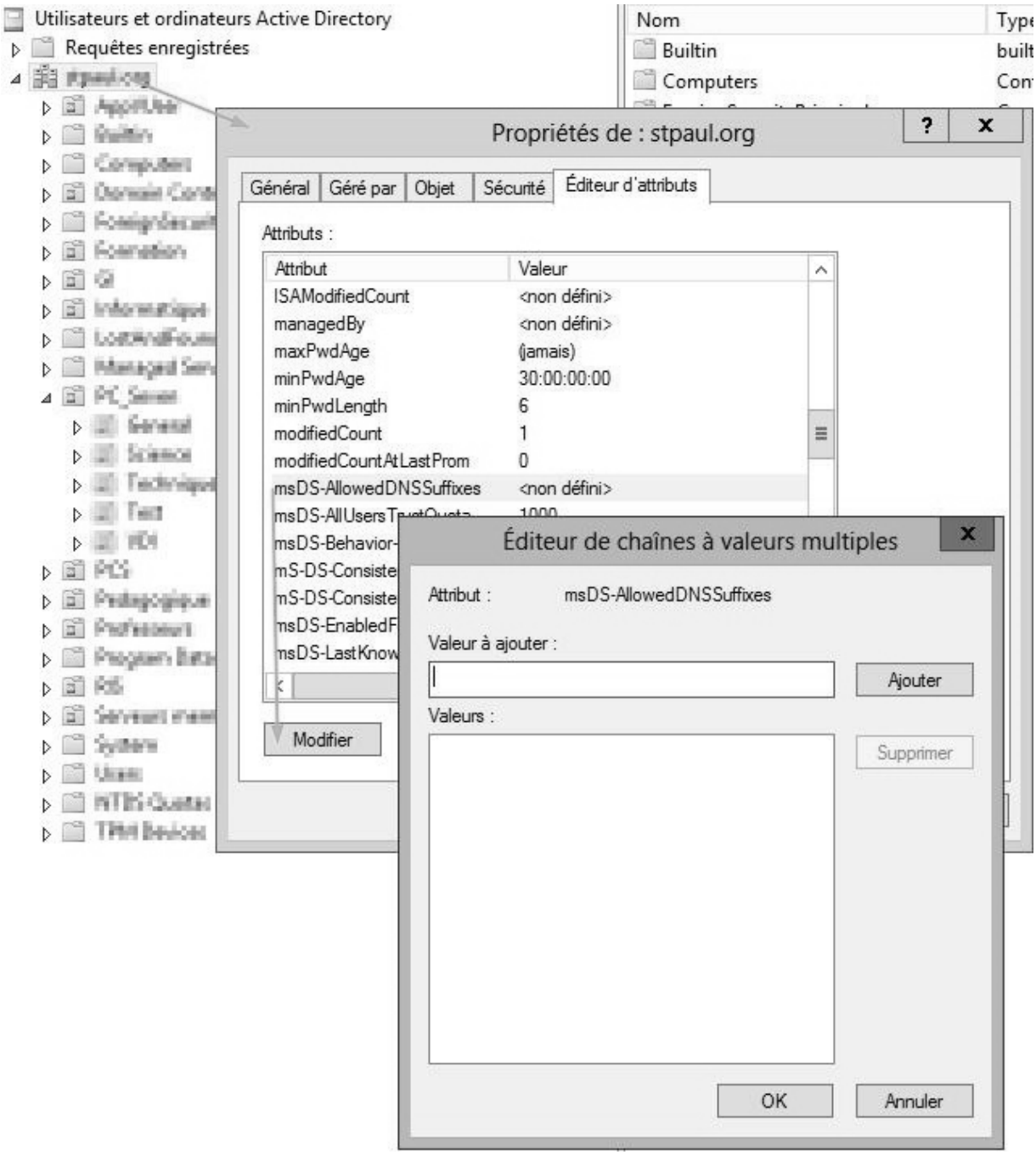


Figure 27 : ajout des suffixes DNS supplémentaires

5.4.3 Effets sur les autorités de certifications

Les services de CA (Certificate Authority) peuvent continuer d'être fonctionnels durant une procédure de renommage si les conditions suivantes sont remplies :

- La CA n'est pas installée sur un DC
- La CA inclut dans son AIA (Authority Information Access) et dans sa CRL (Certificate Revocation List) des URLs LDAP et http afin de perpétuer l'accès.

Dans notre cas, nous n'avons pas de CA à gérer.

5.4.4 Divers autres effets induits par le renommage

Les SPNs sont utilisés par les DC pour s'authentifier mutuellement avec leurs partenaires de réplication, et doivent donc également être mis à jour.

Les relations d'approbations de domaines parent-enfant garantissent la sécurité de l'infrastructure et permettent le partage de ressources entre domaines de la même forêt ainsi que la mise en place de délégations sur les objets ADDS. Lors d'un changement dans la structure d'un arbre, les relations d'approbations de domaines parent-enfant doivent être recréées dans la nouvelle arborescence.

La redirection des dossiers utilisateurs et des profils itinérants est impactée par les changements de nom de domaine. Les chemins d'accès doivent donc être mis à jour en conséquence si nécessaire, et les données relocalisées au besoin. Si le chemin d'accès n'est pas basé sur un FQDN, le renommage n'a pas d'impact sur la continuité des accès.

5.5 Les différentes étapes du processus de renommage

Le processus de renommage que nous allons effectuer se résume au renommage du domaine racine de la forêt stpaul.org administratif. Toutes les opérations seront effectuées sur l'unique serveur contrôleur de domaine Jocaste sous Windows Server 2008 R2.

5.5.1 Identification des risques et récupération

Le risque majeur est ici de se retrouver avec un domaine AD inaccessible du fait d'une erreur au cours du renommage.

Avant toute chose, il est donc indispensable d'effectuer une sauvegarde de l'état des DC afin de permettre un retour arrière en cas de problème. Nous disposons d'une sauvegarde complète quotidienne du serveur. Nous allons cependant réaliser une sauvegarde de l'état du serveur avant de débuter le renommage. Cette sauvegarde beaucoup plus légère comprend entre autres choses les informations nécessaires à la récupération de l'AD.

Afin de retrouver le domaine dans l'état fonctionnel « pré renommage », il faudra redémarrer le DC en mode Directory Services Restore Mode (DSRM). On choisira indifféremment une restauration autoritaire ou non autoritaire puisque le domaine ne possède pas d'autre DC.

Toutes ces opérations seront effectuées en période non ouvrée et en début de semaine afin de disposer de suffisamment de temps afin de reconstruire le système en cas de grave défaillance.

5.5.2 Choix du nouveau nom de domaine racine

On choisit un nom de domaine dont l'extension TLD (Top Level Domain) est fermée, ainsi nous ne sommes pas susceptibles de voir aboutir une résolution DNS non désirée sur une de nos machines. Nous retenons le nom de domaine admin.priv.

5.5.3 Création des zonez DNS pour le nouveau domaine

Chaque nouveau domaine doit faire l'objet d'une création de zone DNS avant le lancement de la procédure de renommage. Nous créons donc la zone principale admin.priv.

5.5.4 Pré création des relations d'approbation

Créer les relations d'approbation transitives bidirectionnelles selon la nouvelle structure de forêt. Aucune relation n'est à créer dans notre cas.

5.5.5 Créer le fichier de description

L'outil Rendom permet de dresser la liste des noms de domaine dans la structure de forêt existante en produisant le fichier de description de la forêt.

```
Rendom /list
```

```
PS C:\> more .\Domainlist.xml
<?xml version ="1.0"?>
<Forest>
        <Domain>
                <!-- PartitionType:Application -->
                <Guid>600ea7ba-69c8-47f9-a0ae-12b3ec4eafe9</Guid>
                <DNSname>ForestDnsZones.admin.priv</DNSname>
                <NetBiosName></NetBiosName>
                <DcName></DcName>
        </Domain>
        <Domain>
                <!-- PartitionType:Application -->
                <Guid>c21822dc-8c0e-44a3-bb9c-1d44eab1a0dd</Guid>
                <DNSname>DomainDnsZones.admin.priv</DNSname>
                <NetBiosName></NetBiosName>
                <DcName></DcName>
        </Domain>
        <Domain>
                <!-- ForestRoot -->
                <Guid>321d9ba9-91f9-450e-beb3-373977a2513b</Guid>
                <DNSname>admin.priv</DNSname>
                <NetBiosName>ADMIN</NetBiosName>
                <DcName></DcName>
        </Domain>
</Forest>
```

Figure 28 : fichier de description DomainList.xml

5.5.6 Spécifier la structure de forêt cible

La nouvelle structure de forêt est établie en éditant le fichier de description précédemment créé. Il suffit de modifier les balises <DNSname> et <NetBiosName> pour refléter la nouvelle structure de forêt. Attention à ne pas spécifier un nom NetBIOS trop long, ce dernier ne doit pas excéder 16 caractères. Attention, les GUID sont des identifiants uniques et permanents qui ne doivent en aucun cas être modifiés.

La commande *rendom /showforest* permet d'afficher et de vérifier la nouvelle structure de la forêt.

```
C:\>rendom /showforest
admin.priv [ForestRoot Domain, FlatName:ADMIN]
        DomainDnsZones.admin.priv [PartitionType : Application]
        ForestDnsZones.admin.priv [PartitionType : Application]

L'opération a réussi.
```

Figure 29 : Sortie de la commande rendom /showforest

5.5.7 Transférer les instructions de renommage à l'AD

Rendom /upload contacte arbitrairement un DC de chaque domaine de la forêt afin de traduire les changements spécifiés dans le fichier de structure cible et ainsi générer un script contenant les séquences de modifications de l'AD pour chaque DC de la forêt (cf. annexe 10.2 Transfert des instructions et monitoring du processus de renommage). Il est toutefois possible de désigner un DC particulier pour effectuer cette opération à l'aide de la balise <DcName> du fichier Domainlist.xml.

5.5.8 Vérification de l'état des DCs

La commande *rendom /prepare* exécute la séquence de tests inclue dans le script de renommage présent sur chaque DC. Sur ces DCs, une vérification des autorisations de l'utilisateur ayant exécuté la commande est également opérée (notamment des droits en écriture sur l'attribut msDS-UpdateScript) ainsi qu'une vérification de l'authenticité du script par validation de la signature contenue dans le script. Selon les résultats des tests, le fichier d'état est mis à jour en conséquence en passant d'Initial à Prepared.

5.5.9 Exécution des instructions de renommage et gel de la forêt

La commande *rendom /execute* déclenche l'exécution des instructions de renommage sur chaque DC. Les services AD de chaque DC passent en mode Single-User interdisant toute interaction avec l'AD et les services dépendants afin d'effectuer les opérations de renommage sur la base AD.

Un switch entre les valeurs dnsRoot et msDS-DnsRootAlias est effectué.

L'attribut msDS-ReplicationEpoch de l'objet NTDS Settings est incrémenté, interdisant toute réplication avec un partenaire n'ayant pas la même valeur d'attribut. On évite ainsi des réplications entre DC ayant terminé leur renommage et ceux en cours de renommage. A l'issue de l'exécution des instructions, le DC reboote.

Une fois le processus de renommage enclenché, la forêt est mise dans un état empêchant les ajouts/suppressions de domaine ou de partition d'application,

l'ajout/suppression d'un DC, l'ajout/suppression d'une relation d'approbation. On dit que la forêt est gelée et ce jusqu'à ce que la commande *rendom /end* soit exécutée.

5.5.10 Modification du suffixe DNS sur les DC

C'est une opération à réaliser à la main et nécessite un redémarrage.

5.5.11 Réparation des GPOs

Lorsque le nom de domaine change, toutes les références à des objets GPO dans le nouveau domaine sont rendues invalides. De plus, toutes GPO dont l'attribut gpcFileSysPath contient un chemin UNC pointant vers un template de GPO contenu dans le dossier des templates du dossier SYSVOL sont également impactées.

L'outil Gpfixup permet de corriger automatiquement ces GPO et doit être exécuté au sein de chaque domaine renommé dès la fin du processus de renommage.

```
Gpfixup /olddns:oldDomainDNSname /newdns:newDomainDNSname
/oldnb:oldDOmainNetBIOSname /newnb:newDomainNetBIOSname
/dc:DC.newDomainDNSname 2>&1 >gpfixup.log
```

Par exemple:

```
Gpfixup /olddns:stpaul.org /newdns:admin.priv /oldnb:STPAUL
/newnb:ADMIN /dc:jocaste.admin.priv
```

5.5.12 Reboot des clients

A réaliser 2 fois, la première fois pour détecter le changement et le second pour l'appliquer.

5.5.13 Nettoyage de la partition de configuration du domaine

La commande *rendom /clean* a pour but de supprimer le contenu des attributs msDS-DnsRootAlias et msDS-UpdateScript sur le DC ayant le FSMO maître d'attribution des noms de domaine puis des DC de la forêt par réplication. Ainsi les enregistrements

CNAME et SRV obsolètes seront également supprimés. A l'issue de cette commande, la forêt est à nouveau prête pour un nouveau renommage.

5.5.14 Dégel de la forêt

Une fois tous les DCs redémarrés, il faut dégeler la forêt pour la rendre opérationnelle avec la commande *rendom /end*.

5.5.15 Post configuration

Nettoyer les zones DNS devenues obsolètes.

Passer en revue toutes les GPO afin de mettre à jour les chemins non UNC. Les éventuels scripts de démarrage sont également à mettre à jour.

5.5.16 Récapitulatif des séquences

Le renommage est planifié sur 2 journées, cependant le reste de la semaine est encore à disposition dans l'éventualité où un problème nous obligerait à une récupération voire à une reconstruction de l'AD.

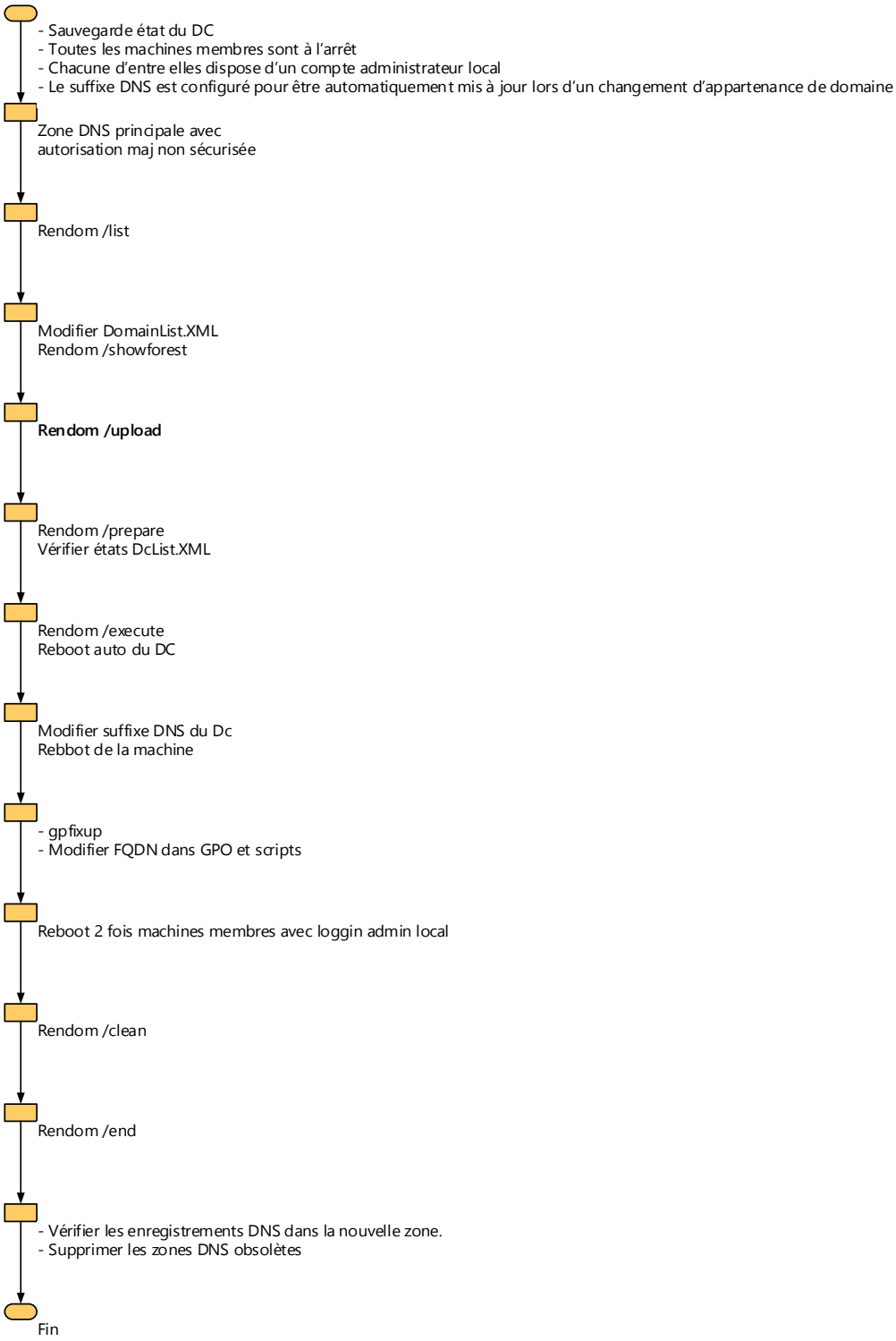


Figure 30 : déroulé des tâches de renommage de la fôret administatif

6 Fusion des différentes entités de gestion Active Directory

Ce processus est utilisé lorsque l'on souhaite relocaliser des objets Active Directory d'un domaine source d'une forêt vers un domaine cible d'une autre forêt et ainsi consolider des infrastructures informatiques. Nous allons donc déplacer tous nos objets AD de notre forêt stjoseph.org vers la forêt stpaul.org.

Pour ce faire, Microsoft met à disposition l'outil ADMT v3.2 (Active Directory Migration Tool). Ce dernier impose que les forêts sources et cibles soient au même niveau fonctionnel de forêt et que les domaines sources et cibles soient au moins au niveau fonctionnel de domaine Windows Server 2003 afin d'établir une relation d'approbation bidirectionnelle transitive.

Tableau 16 : niveaux fonctionnels de domaines et forêts

Domaine	Niveau fonctionnel de domaine	Niveau fonctionnel de forêt
Stjoseph.org	Windows 2008	Windows 2003
Stpaul.org	Windows 2008	Windows 2008

Le niveau fonctionnel de forêt de la forêt stjoseph.org doit donc être amené au niveau Windows 2008.

Il faut cependant retenir qu'une fois une valeur attribuée à cette option, on ne peut revenir à sa valeur précédente ou réduire le niveau fonctionnel de la forêt, à une exception près : lorsqu'on augmente le niveau fonctionnel d'une forêt à Windows Server 2008 R2 ou supérieur et que la corbeille Active Directory n'est pas activée. Il reste possible de restaurer le niveau fonctionnel de la forêt jusqu'à Windows Server 2008. On ne peut donc diminuer le niveau fonctionnel de la forêt que de Windows Server 2008 R2 vers Windows Server 2008.

Cette manipulation n'apporte rien en matière de fonctionnalité supplémentaire mais garanti que tous les domaines sont au niveau fonctionnel Windows 2008 et que donc tous contrôleurs de domaines sont sous Windows 2008 minimum.

La restructuration des domaines AD entre forêts nécessite une planification et une préparation des domaines de l'organisation. La figure suivante présente le processus dans ces grandes phases.

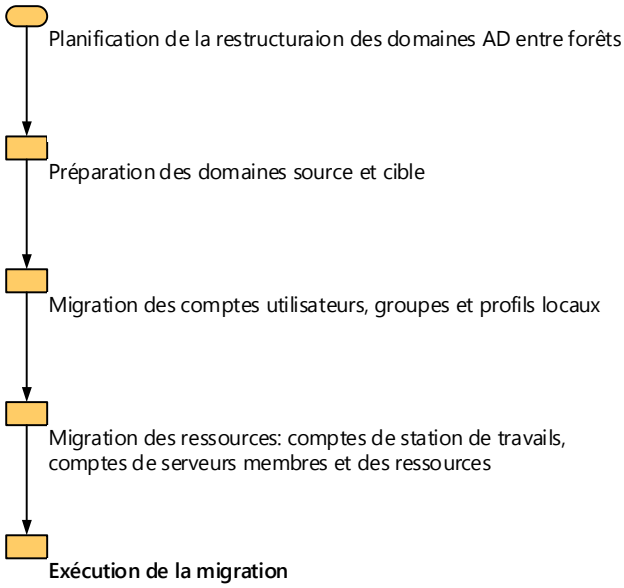


Figure 31 : Processus de migration de domaine AD

L'ensemble du processus est dit non destructif puisque tous les objets migrés continuent d'exister dans le domaine source jusqu'à suppression de celui-ci. Ils sont simplement désactivés, permettant un retour arrière facilité en cas de problème.

6.1 Planning

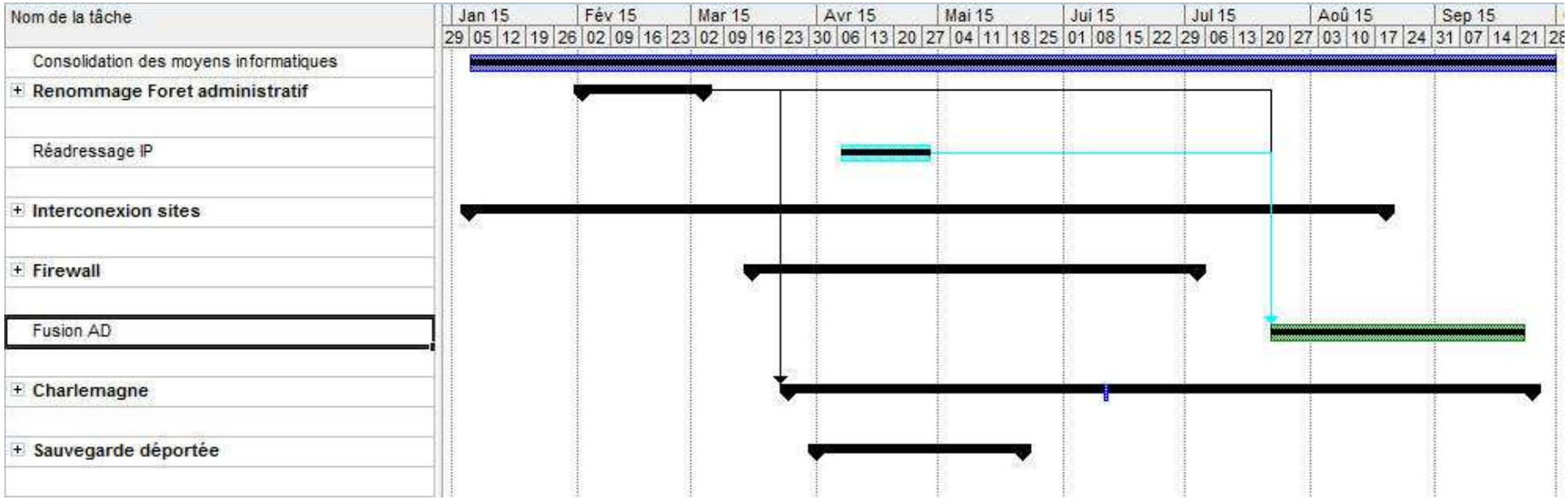


Figure 32 : planning fusion AD

6.2 Processus de migration de comptes de machines et d'utilisateurs

ADMT permet d'effectuer la migration tout en préservant les accès des utilisateurs aux ressources grâce à l'attribut SIDHistory des objets de classe compte d'utilisateur et de classe groupe de l'annuaire Active Directory. Cet attribut permet de disposer dans le domaine cible des SIDs du compte dans le domaine source.

Il est à noter que ce mécanisme est dépendant de la configuration de la relation d'approbation qui lie les domaines source et cible, si le filtrage des SID est activé sur cette relation, l'historique des SIDs n'est pas inclus dans le TGT.

Les stratégies de groupe utilisées pour gérer les redirections de dossiers peuvent être impactées et doivent être vérifiées lors de la migration de comptes utilisateurs. En effet, si l'on a choisi de s'appuyer sur l'appartenance de groupe pour mettre en place la redirection de dossiers, le changement de domaine AD doit être reporté dans la ou les GPO en question.

6.3 Processus de migration de ressources

La migration des stations de travail et des serveurs membres est un processus simple dans le sens ou la base SAM (Security Account Manager) locale propre à chaque machine et contenant tous les comptes d'utilisateurs locaux est déplacée en même temps que la machine et ne nécessite aucune migration de compte supplémentaire.

La migration d'un contrôleur de domaine est moins évidente, puisqu'il faut supprimer les services AD de la machine pour la migrer en tant que serveur membre. Une fois migrés, les services ADDS peuvent être réinstallés dans la nouvelle forêt. On comprend dès lors qu'une fois tous les DCs migrés plus aucun retour arrière n'est possible, c'est pourquoi on créera et l'on conservera encore un certain temps la machine virtuelle AD-RescueStJoseph DC du domaine source pour palier à toute éventualité.

6.4 Identification des risques liés à la restructuration inter forêts

Le risque majeur réside dans l'incapacité des utilisateurs à se connecter à leur machine après migration, ou à ne pas pouvoir accéder à toutes leurs ressources habituelles. Comme indiqué précédemment, on conservera à minima un DC afin de permettre un retour arrière. Il suffira pour un compte utilisateur de le réactiver dans le domaine source. Pour une station de travail ou un serveur membre, on modifiera l'appartenance au domaine.

6.5 Impact de la restructuration inter forêts sur le SI

Cette restructuration impose de repenser l'organisation du SI. En effet, même si les utilisateurs et stations du site stpaul.org ne sont pas directement impactés, il faut néanmoins veiller à ce qu'ils ne pâtissent pas des adaptations nécessaires qui sont à réaliser pour accueillir les machines et les utilisateurs migrés du site stjoseph.org.

Les services Active Directory étant au cœur du système de gestion de l'infrastructure, un plus grand soin est apporté à l'adaptation de la structure d'OU du domaine stpaul.org. De cela découle toute la stratégie de gestion des serveurs, des stations et des utilisateurs. Cette architecture doit permettre de gérer le parc avec la plus grande souplesse afin de répondre aux exigences dictées par les spécificités des enseignements. La granularité des GPOs doit donc être conservée autant que faire se peut.

6.5.1 Structure d'OU

En s'appuyant sur les technologies inhérentes aux GPO (héritage, ordre d'application GPO local → GPO Site → GPO Domaine → GPO d'OUs, traitement par bouclage des stratégies de groupe, …), la structure suivante est retenue :

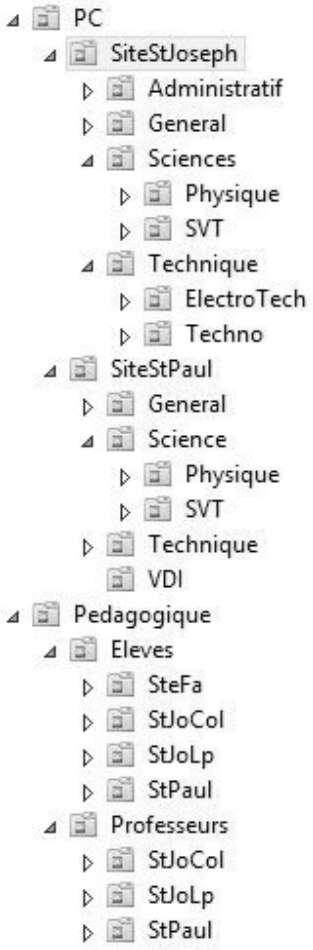


Figure 33 : structure d'OU cible

Ainsi les paramétrages liés aux sites pourront être traités par *GPO de site*, la structure d'OUs permettant de gérer les spécificités restantes.

6.5.2 Services de mises à jour

Les machines du domaine stjoseph.org s'adressaient au serveur Callisto.stjoseph.org pour se mettre à jour. Après migration du serveur Callisto.stjoseph.org, le service reste fonctionnel, mais compte tenu du changement de nom de domaine, tous les paramètres basés sur un FQDN nécessitent des modifications qui peuvent être appliquées aux stations par GPO.

De plus, un paramètrage du client WSUS permet d'autoriser celui-ci à cibler les mises à jour dont il a besoin en fonction de la version du système d'exploitation et des logiciels mis à jour par WSUS. Ainsi plusieurs conteneurs sont disponibles, chacun regroupant un ensemble de mises à jour par grande famille de système d'exploitation (Windows 7 x86, Windows 7 x64, …). Le paramétrage de ciblage ne pourra donc pas être inclus dans une GPO de site, mais dans une GPO d'OU appliquée par catégorie de système d'exploitation. Une GPO de site permettra par contre d'orienter les stations vers le serveur WSUS désigné par site.

Le service est déployé différemment afin de faciliter la gestion des mises à jour (choix des mises à jour, assignation à tel type de système d'exploitation…). Ainsi le serveur WSUS.stpaul.org devient un serveur amont et transmet ses mises à jour et/ou tout le paramétrage qui s'y rattache au serveur WSUS Callisto.stpaul.org aval en mode réplica. Ce dernier effectue la tâche de distribution des mises à jour en fonction des informations reçues du serveur amont.

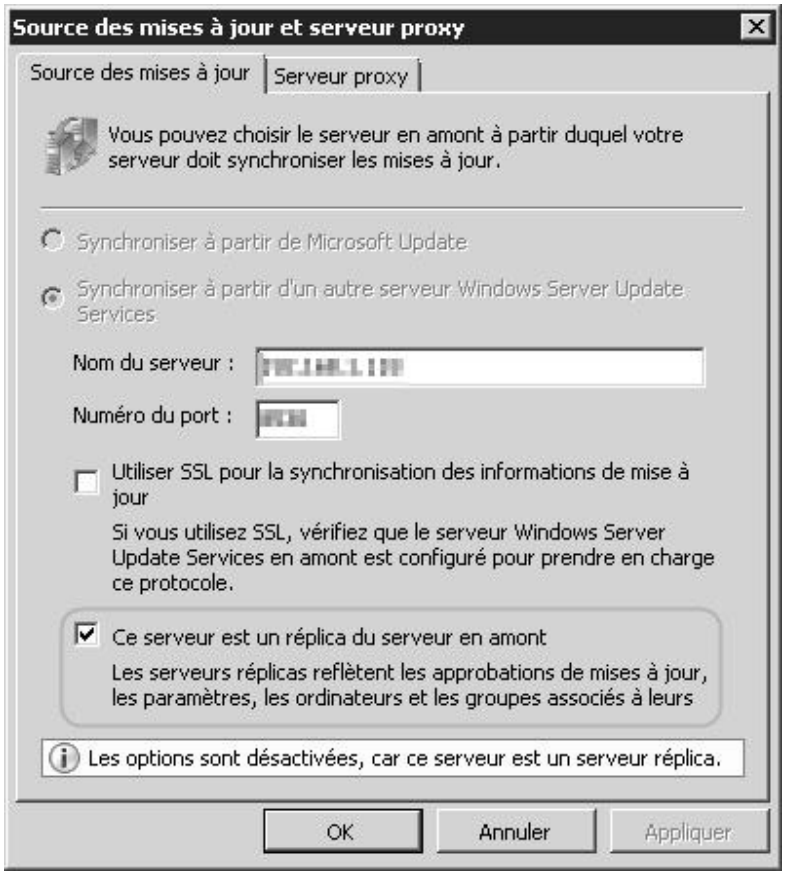


Figure 34 : paramétrage serveur WSUS en mode réplica

Ce serveur aval télécharge les mises à jour retenues par le serveur amont à partir de Microsoft Update.

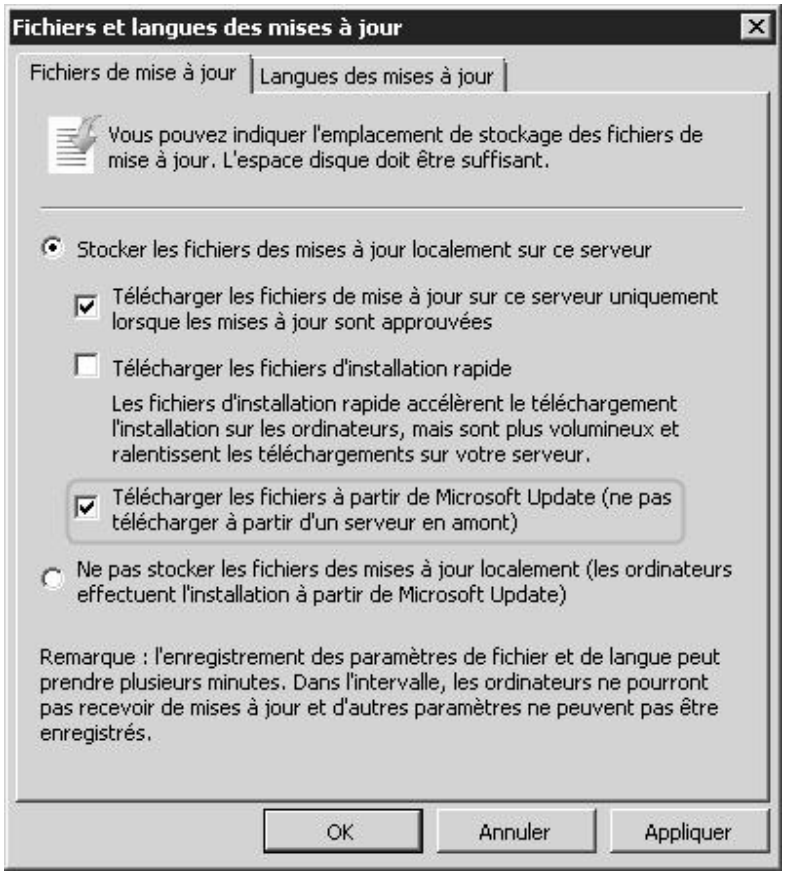


Figure 35 : paramétrage de la source de téléchargement des mises à jour WSUS

6.5.3 Affectation des imprimantes

Les services d'impression offerts par le serveur Callisto.stjoseph.org, seront migrés vers le domaine stpaul.org. La structure d'OU permet de conserver les affectations d'imprimantes par station et par type d'utilisateur (professeur ou élève).

6.5.4 Profils itinérants

La liste de contrôle d'accès des profils itinérants obligatoires sera traduite au cours de la migration. La structure d'OU permet de conserver les affectations de profils itinérants obligatoires en fonction de l'OU d'appartenance de la station, ainsi que du type d'utilisateur (professeur ou élève).

6.5.5 Anti-virus Kaspersky

Dans l'optique de consolidation du SI, nous allons mettre en place une hiérarchie de serveurs Kaspersky. Nous allons ainsi bénéficier d'une vue centralisée à l'échelle du LAN étendu tout en maîtrisant l'utilisation de la bande passante du lien inter site, puisqu'à l'instar du service de mise à jour WSUS, seules des métadonnées seront échangées entre notre serveur maître AV-01.stpaul.org site St Paul et un serveur secondaire à créer AV-02.stpaul.org site St Joseph auquel se réfèreront les stations du site St Joseph pour s'inscrire et récupérer la stratégie antivirus ainsi que les mises à jour de la base antivirus.

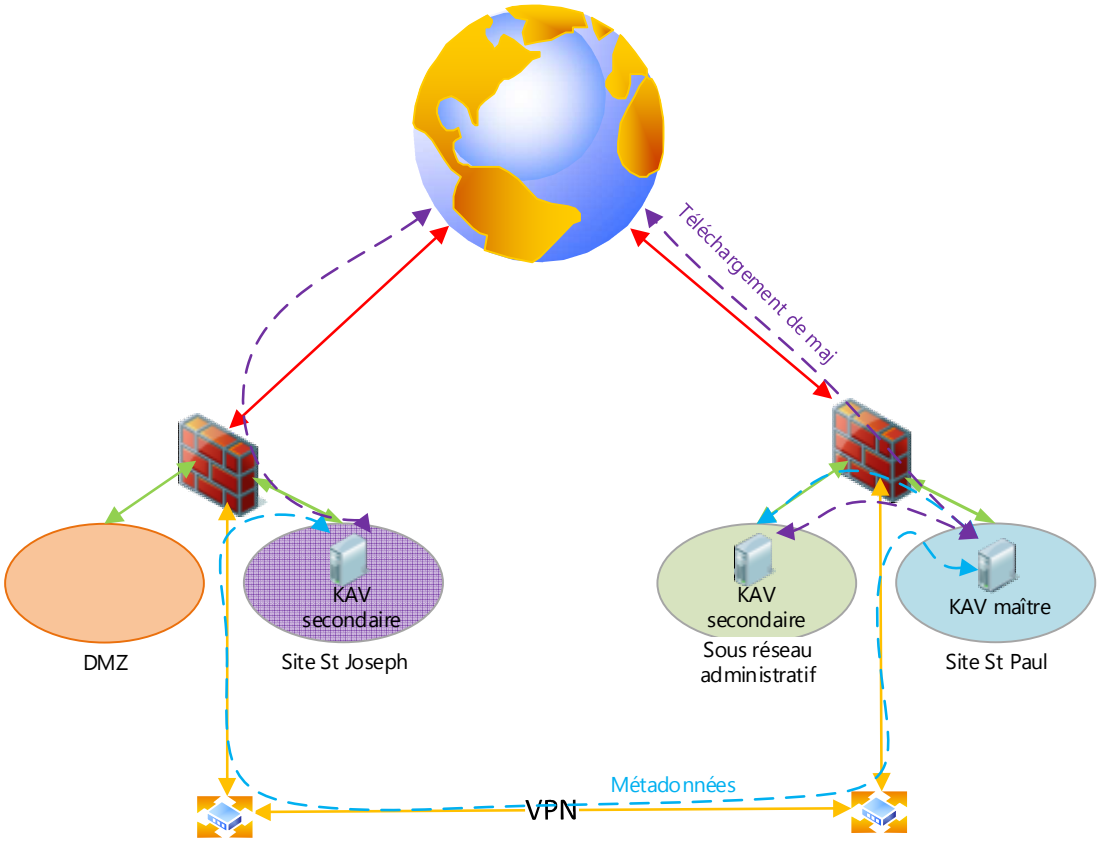


Figure 36 : Hiérarchie de serveurs Kaspersky

6.5.6 Distribution d'applications virtuelles AppV

On conserve le serveur d'applications virtuelles AppV-01 déjà en place sur le site St Joseph. La structure d'OU permet de conserver les paramètres de diffusion des applications disponibles par site. On va pouvoir cependant mettre en place un groupe

de réplication DFS du répertoire contenant les applications virtuelles entre nos serveurs de contenu AppV et ainsi disposer d'un référentiel commun à l'échelle du groupe scolaire.

Au cours du processus de migration, le service de management AppV devra être reconfiguré. On retrouve les paramètres directement dans la base de registre que l'on peut donc éditer par GPO.

6.5.7 Système de fichiers distribués Distributed Files System Namespaces (DFSN)

DFSN est un système de fichiers distribué qui permet de présenter aux applications et aux utilisateurs un espace de nom unique regroupant des ressources fichiers disséminées sur le réseau. Nous disposons dans chacun des domaines stpaul.org et stjoseph.org d'un DFS de type Domain-based (basé sur un nom de domaine).

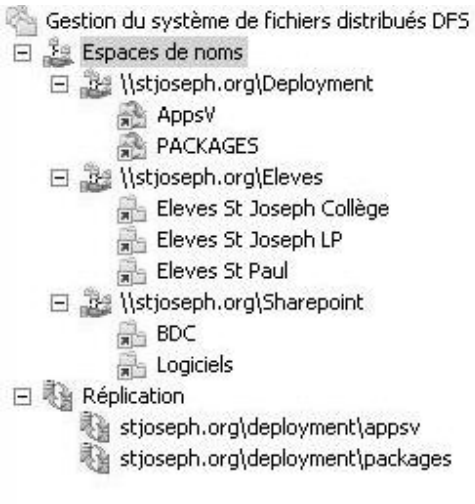


Figure 37 : système de fichiers distribués site stjoseph.org

Nous allons donc intégrer le DFS stjoseph.org au DFS stpaul.org en respectant le phasage suivant :

1- Export des différents espaces de nom DFSN pour une reconstruction éventuelle.

```
dfsutil                          /root:\\olddomain.com\rootname
/export:exportedroot.txt /verbose
```

2- Migration des machines participantes.
3- Traduction de la sécurité sur les partages cibles liés aux espaces de noms.
4- Modification des espaces de nom existants sur le domaine stpaul.org pour intégrer les partages de fichiers stjoseph.org.

6.5.7.1Réplication inter-sites

On veillera à activer la compression différentielle RPC sur toutes nos réplications inter-sites (cf. chapitre *4.3.7 Flux DFSR*) et à adapter la planification en fonction des heures ouvrées.

6.5.7.2Preseeding

Le *preseeding* permet d'implanter sur un nœud DFSR enfant les fichiers provenant d'un serveur DFSR maître avant l'ajout du nœud enfant au groupe de réplication. On minimise de cette façon la quantité de données échangée entre les serveurs durant le processus de synchronisation initial accélérant d'autant la mise en service du nœud enfant. On procèdera par sauvegarde/restauration des volumes à dupliquer sur le site St Joseph en prenant soin de restaurer également les ACLs.

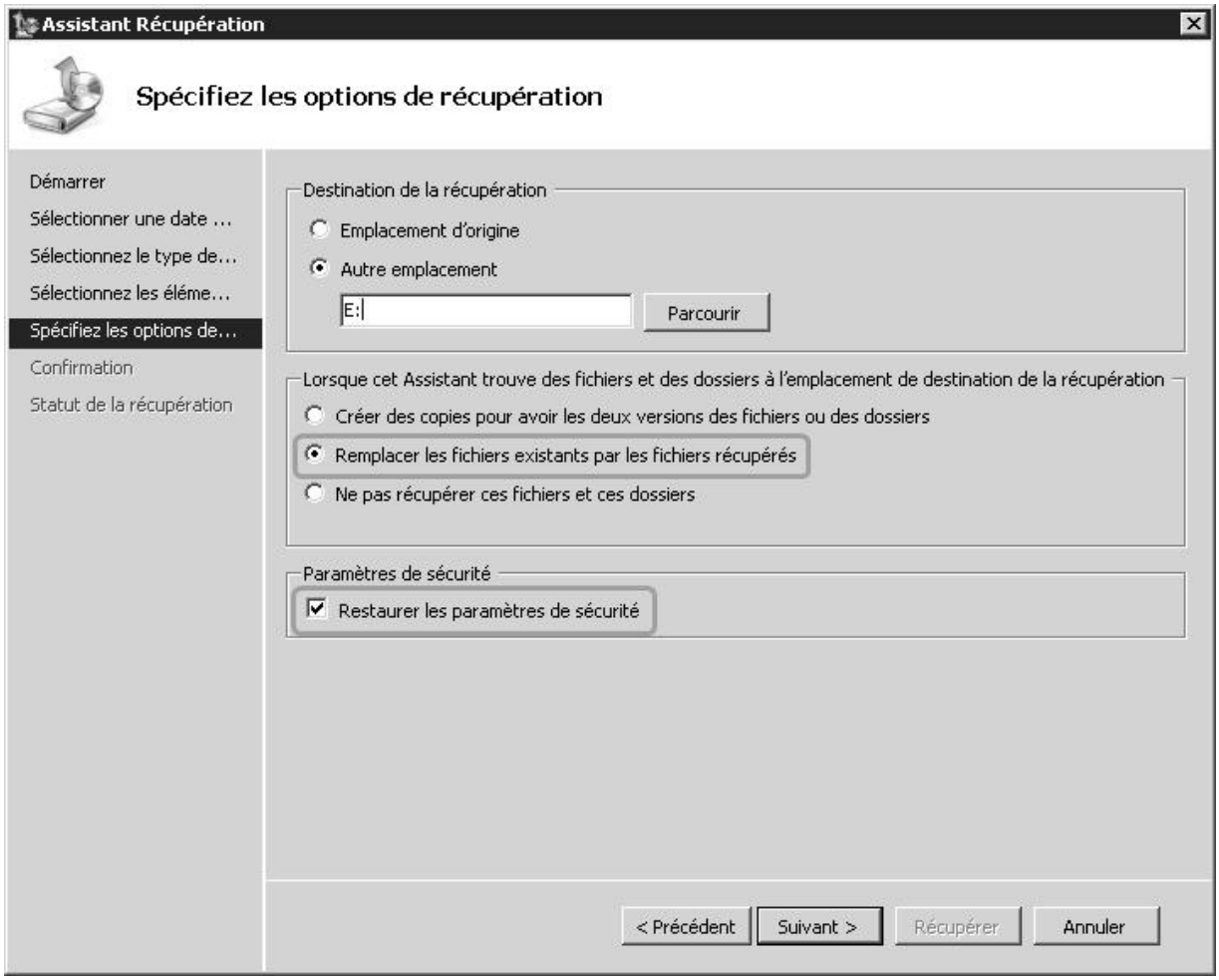


Figure 38 : restauration d'un volume de réplication

Nous allons ainsi pouvoir mettre en place un certain nombre d'espaces répliqués entre nos sites sans impacter notre lien inter-sites.

Il convient cependant de valider le *preseeding* afin de s'assurer qu'il n'existe aucune différence entre les fichiers situés sur le nœud DFSR maître et le nœud DFSR enfant au risque de provoquer une réplication de fichiers intégrale. La comparaison est effectuée et validée en comparant les hashes d'une dizaine de fichiers sources et cibles à l'aide de la commande *Dfsrdiag* exécutée sur le nœud maître puis sur le nœud enfant :

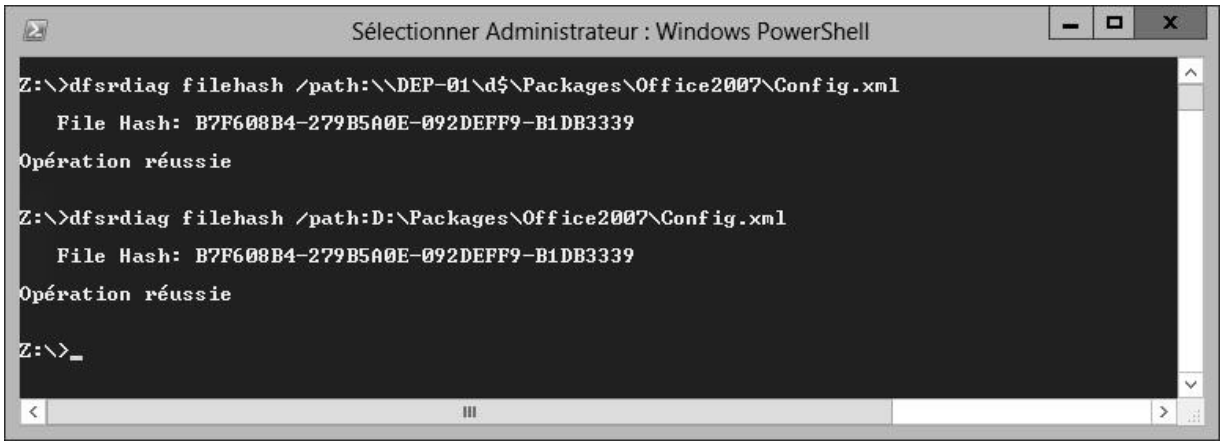


Figure 39 : comparaison des hashes de fichiers

6.5.7.3Cibles DFS

On souhaite bien évidemment privilégier les serveurs de contenu DFS se trouvant sur les mêmes sites que les clients qui les sollicitent afin de limiter l'utilisation du lien inter-sites. On exclura donc les cibles DFS hors du site client dans les propriétés des espaces de noms.

Figure 40 : Exclusion des cibles hors site client DFS

6.5.8 Déploiement logiciels

La majeure partie des logiciels est déployée par GPO, soit directement en s'appuyant sur un fichier .msi soit en ayant recours à un script. Tous les chemins utilisés pour cibler les fichiers empruntent au minimum la racine DFS \\stjoseph.org\deployment\Packages pour le site à migrer stjoseph.org. Nous n'avons pas de GPO spécifiant la « Désinstallation de l'application lorsqu'elle se trouve en dehors de l'étendue de gestion » (lorsqu'un ordinateur est retiré de l'UO sur laquelle est appliquée la GPO).

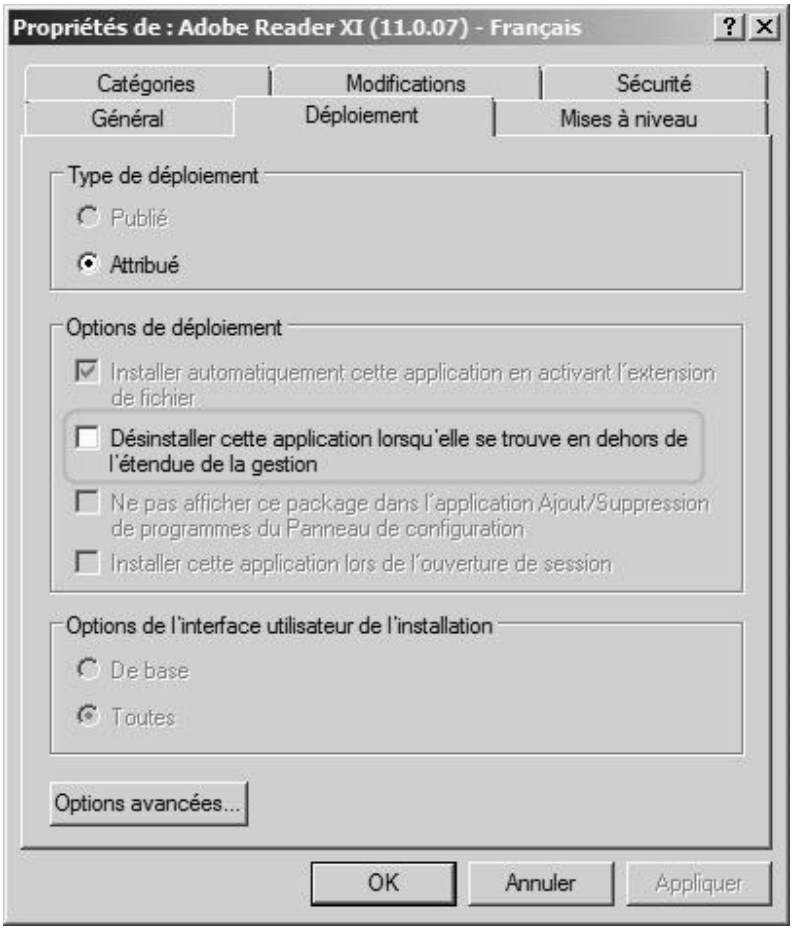


Figure 41 : propriétés d'un déploiement de package

En ce qui concerne plus spécifiquement les scripts, ces derniers loguent les erreurs d'exécution dans des fichiers déposés dans un partage créé à cet effet. On créé la variable d'environnement système LogPath que l'on déploie par GPO de site afin de l'intégrer dans le chemin pointant vers le répertoire de log. Ainsi chaque script modifié loguera sur son site local plutôt que de transiter par le lien VPN.

Tableau 17 : variables d'environnement par site

Variable d'environnement système LogPath par site AD	Valeur
St Paul	AD-01
St Joseph	Callisto

Les machines migrées conserveront leur configuration logicielle intacte. Les paramètres de ces GPOs ainsi que leurs scripts seront réappliqués lors du rafraîchissement des GPO qui a lieu au démarrage des machines ou à l'ouverture de session d'utilisateur en spécifiant les chemins correspondant à la racine DFS du domaine stpaul.org.

6.5.9 Délégations

Chaque professeur a la possibilité de réinitialiser le mot de passe d'un élève à l'aide d'un script afin de répondre aux situations suivantes :

- Oubli du mot de passe
- Le mot de passe est connu d'un ou plusieurs autres utilisateurs. Le compte est compromis.

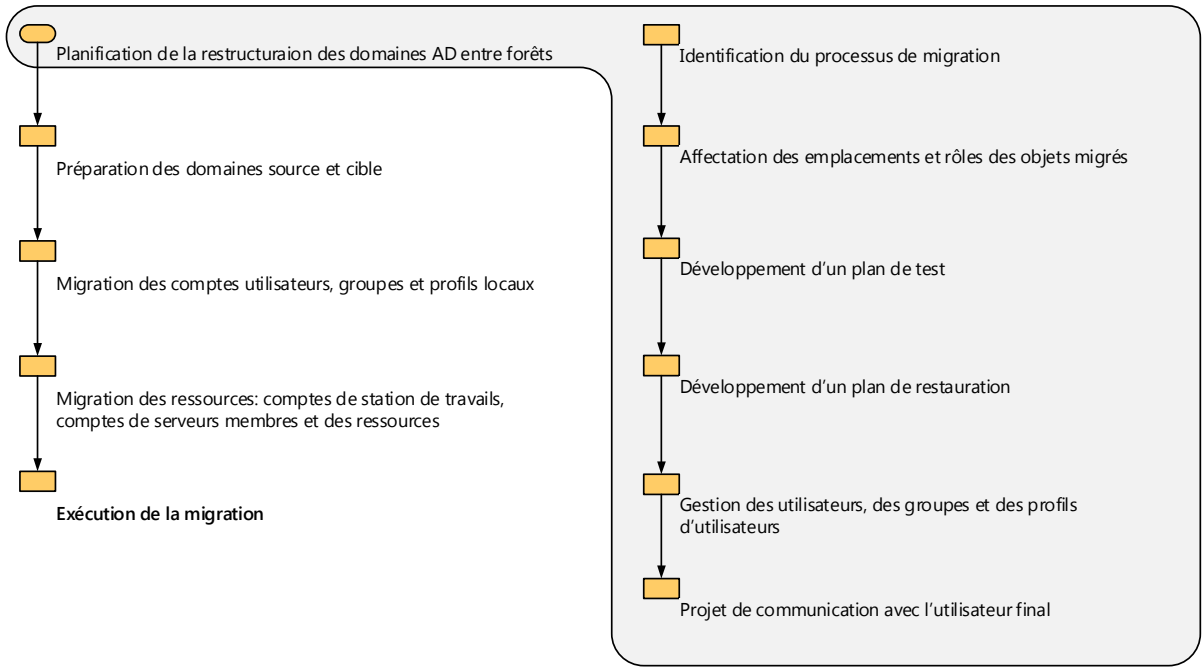
Pour réaliser cette opération, l'enseignant doit disposer d'une délégation sur l'OU contenant le compte de l'utilisateur. Ces délégations doivent être accordées aux groupes d'enseignants migrés sur les OUs des comptes élèves migrés.

6.5.10 Utilisateurs itinérants

Ces utilisateurs possèdent un compte dans le domaine admin.priv, et sont susceptibles de se connecter aussi bien au sein de leur forêt native que dans la forêt pédagogique stpaul.org grâce à l'approbation inter forêt mise en place. Dans ce dernier cas, les GPOs utilisateurs ne sont par défaut pas appliquées. Lorsque l'utilisateur administratif se connecte sur une machine pédagogique, le système détecte que l'utilisateur n'appartient pas à sa forêt, et déclenche le mécanisme de *loopback policy en mode remplacer* qui au lieu de permettre l'application des GPOs utilisateurs habituelles, les remplace par les paramétrages utilisateurs présents dans l'UO ou réside la machine. Si aucune GPO utilisateur n'est attachée à cette UO, aucun paramètre utilisateur n'est appliqué. On peut changer ce comportement et permettre l'application des GPOs

« étrangères ». Ce paramètre se situe dans les *Stratégie ordinateur/Modèles d'administration/Système/Stratégie de groupe/Autoriser la stratégie utilisateur et les profils itinérants entre forêts*.

6.6 Planification de la restructuration inter forêts



6.6.1 Identification du processus de migration

ADMT permet d'utiliser l'historique SID afin de conserver l'accès aux ressources du domaine source durant tout le processus de migration. Il faudra cependant désactiver le filtrage SID de l'approbation existante entre le domaine source et cible. Dans notre cas, rien ne nous empêche d'établir une relation d'approbation bidirectionnelle sans filtrage de SID entre nos domaines stpaul.org et stjoseph.org.

6.6.1.1 Utilisation de l'historique SID pour conserver l'accès aux ressources

Lorsqu'un utilisateur est migré, l'attribut SIDHistory de l'objet LDAP correspondant à son nouveau compte est peuplé par les SIDs de son compte source. Ainsi, lors de la création d'un jeton d'accès, toutes les informations d'appartenance à des groupes sources et cibles sont incluses. L'utilisateur migré peut ainsi tout aussi bien continuer d'accéder aux

ressources du domaine source comme celles du domaine cible si les ACLS des ressources le permettent.

Les groupes globaux ne pouvant contenir que des utilisateurs ou d'autres groupes globaux de leur domaine d'origine, il faudra également les migrer.

De plus, l'accès aux ressources partagées entre les forêts nous amène à reconsidérer l'attribution des droits d'accès, ceci afin de limiter le travail fastidieux d'adaptation et de modification des ACLs.

6.6.1.1.1 Adaptation de la stratégie d'imbrication des groupes à la nouvelle architecture

Les bonnes pratiques en matière d'octroi d'accès aux ressources consistent à utiliser des groupes globaux afin d'organiser les utilisateurs, puis de placer ces groupes dans des groupes locaux de domaine. Ces derniers sont utilisés pour effectivement attribuer les droits sur la ressource.

Tableau 18 : imbrication des groupes AD

Étendue du groupe	Le groupe peut inclure comme membres…	Le groupe peut recevoir des autorisations dans…	L'étendue du groupe peut être convertie en…
Universelle	• Comptes de tout domaine de la forêt où réside ce groupe universel • Groupes globaux de tout domaine de la forêt où réside le groupe universel • Groupes universels de tout domaine de la forêt où réside le groupe universel	Tout domaine ou forêt	• Domaine local • Global (si aucun autre groupe universel n'existe en tant que membres)
Globale	• Comptes du même	Les autorisations des	Universelle (s'il ne

	domaine en tant que groupe global parent • Groupes globaux du même domaine en tant que groupe global parent	membres peuvent être attribuées dans tout domaine de toute forêt	s'agit pas d'un membre de tout autre groupe global)
Domaine local	• Comptes de tout domaine • Groupes globaux de tout domaine • Groupes universels de tout domaine • Groupes locaux du même domaine que le groupe local parent	Les autorisations des membres peuvent être attribuées dans le même domaine que le groupe local parent	Universelle (si aucun autre groupe local n'existe en tant que membre)

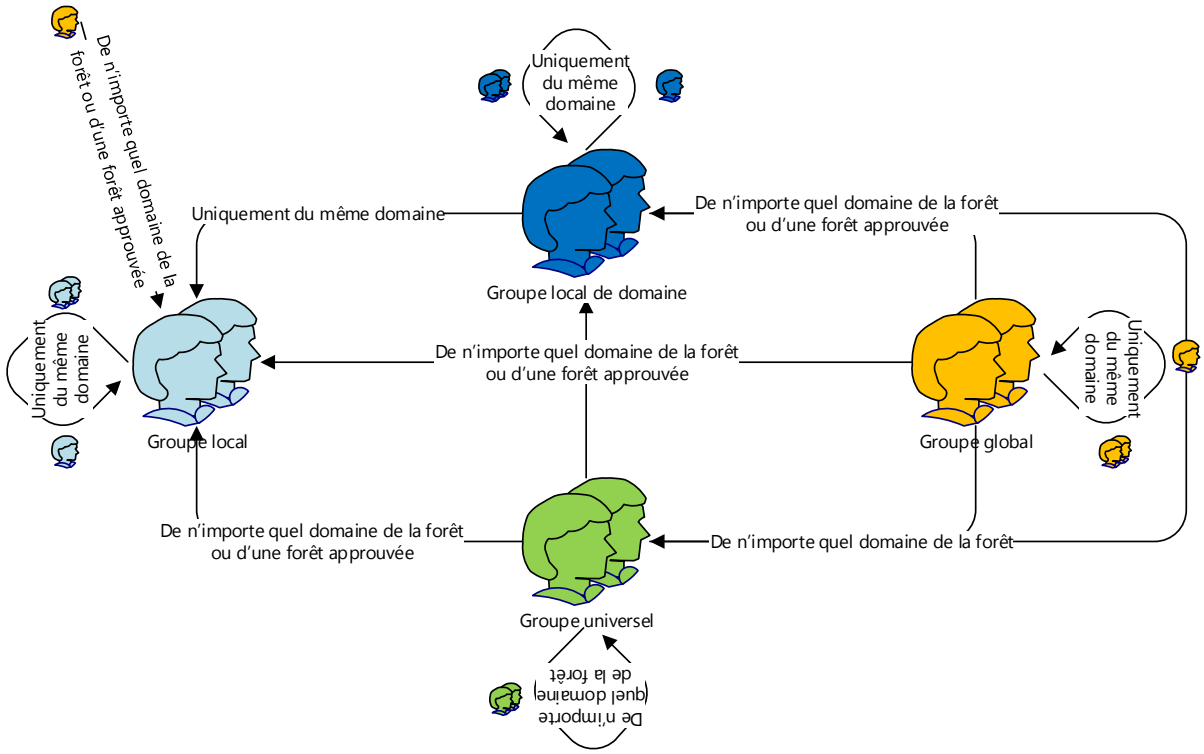


Figure 42 : Schéma d'imbrication des groupes

On souhaite par exemple autoriser l'accès aux partages et dossiers des élèves au groupe ADMIN\Direction (cet exemple reste vrai pour tous les accès opérés par les élèves ou les professeurs sur les partages de fichiers). Les autorisations d'accès à ces dossiers étant assez fines et complexes, il serait beaucoup plus simple d'ajouter le groupe global ADMIN\Direction au groupe global STPAUL\ProfsStPaul pour lequel les réglages sont déjà en place. Seulement il n'est possible d'ajouter un groupe global à un autre groupe global que si ces groupes appartiennent au même domaine (cf. tableau imbrication des groupes AD ci-dessus), ce qui n'est pas du tout le cas ici. Il faudrait que le groupe global STPAUL\ProfsStPaul soit de type local de domaine afin qu'il puisse accepter d'inclure un groupe global d'un domaine ou d'une forêt différente de son domaine local. Il est donc nécessaire de changer le type de ce groupe d'abord en universelle puis en local de domaine (cf. tableau imbrication des groupes AD ci-dessus).

Dans notre exemple, il faut donc suivre la démarche suivante afin de respecter les bonnes pratiques et la formule magique AGUDLP (Accounts/Global groups/Universal groups/Domain Local groups/Permissions) édictées par Microsoft :

- transformer le groupe global STPAUL\ProfsStPaul en groupe local de domaine
- créer le groupe global STPAUL\ProfsStPaulG
- faire du groupe global STPAUL\ProfsStPaulG un membre du groupe local de domaine STPAUL\ProfsStPaul
- inclure le groupe ADMIN\Direction à un groupe universel ADMIN\AdministratifU à créer et faire de ce dernier un membre du groupe local de domaine STPAUL\ProfsStPaul. On peut tout aussi bien ajouter le groupe global ADMIN\Administratif au groupe local de domaine STPAUL\ProfsStPaul puisque la forêt ADMIN ne contient qu'un seul domaine et qu'un seul groupe d'utilisateur présente un besoin d'accès aux ressources de la forêt STPAUL. On économise ainsi la création et la gestion d'un groupe universel.
- déplacer les membres du groupe STPAUL\ProfsStPaul vers le groupe global STPAUL\ProfsStPaulG

Toutes ces manipulations sont-elles moins fastidieuses à réaliser que de changer les ACLs ? Cela dépendra de la complexité des attributions de droits. C'est également l'occasion de respecter les bonnes pratiques.

Dans notre cas les groupes concernés sont assez réduits, et compte tenu du nombre limité d'opérations à réaliser, nous allons nous affranchir de toute intervention sur les ACLs et simplement jouer sur le type de groupe et les imbrications entre ces derniers.

Ne perdons pas de vue que lors d'un changement de type pour un groupe, il va falloir vérifier toute la chaîne imbriquée afin de s'assurer de la possibilité de l'opération. Par exemple, si le groupe global STPAUL\ProfsStPaul devient un groupe local de domaine, il ne peut plus être membre d'un groupe global. Cela nécessite donc de modifier le type

de tous les groupes auxquels appartient le groupe STPAUL\ProfsStPaul ainsi que tous ceux auxquels appartiennent ces groupes…

On doit donc avant tout établir un inventaire portant sur l'imbrication des groupes entre eux et ainsi déterminer les types de groupes ainsi que l'ordre de modification de ces derniers.

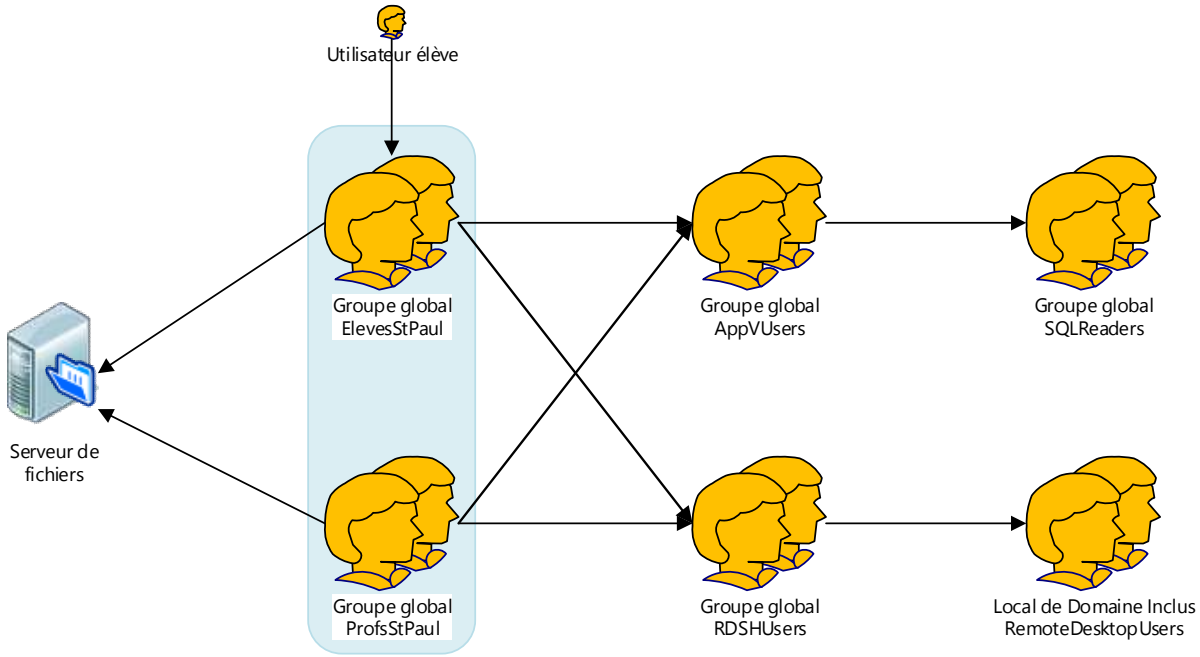


Figure 43 : Schéma d'imbrication de groupes domaine stpaul.org

Les groupes ElevesStPaul ainsi que ProfsStPaul sont les groupes « centraux » accueillants les utilisateurs élèves et professeurs. Ce sont sur eux que reposent les accès aux ressources et aux différents services (partages, applications virtuelles, …) et que se concentrent les modifications à effectuer selon le schéma ci-dessous :

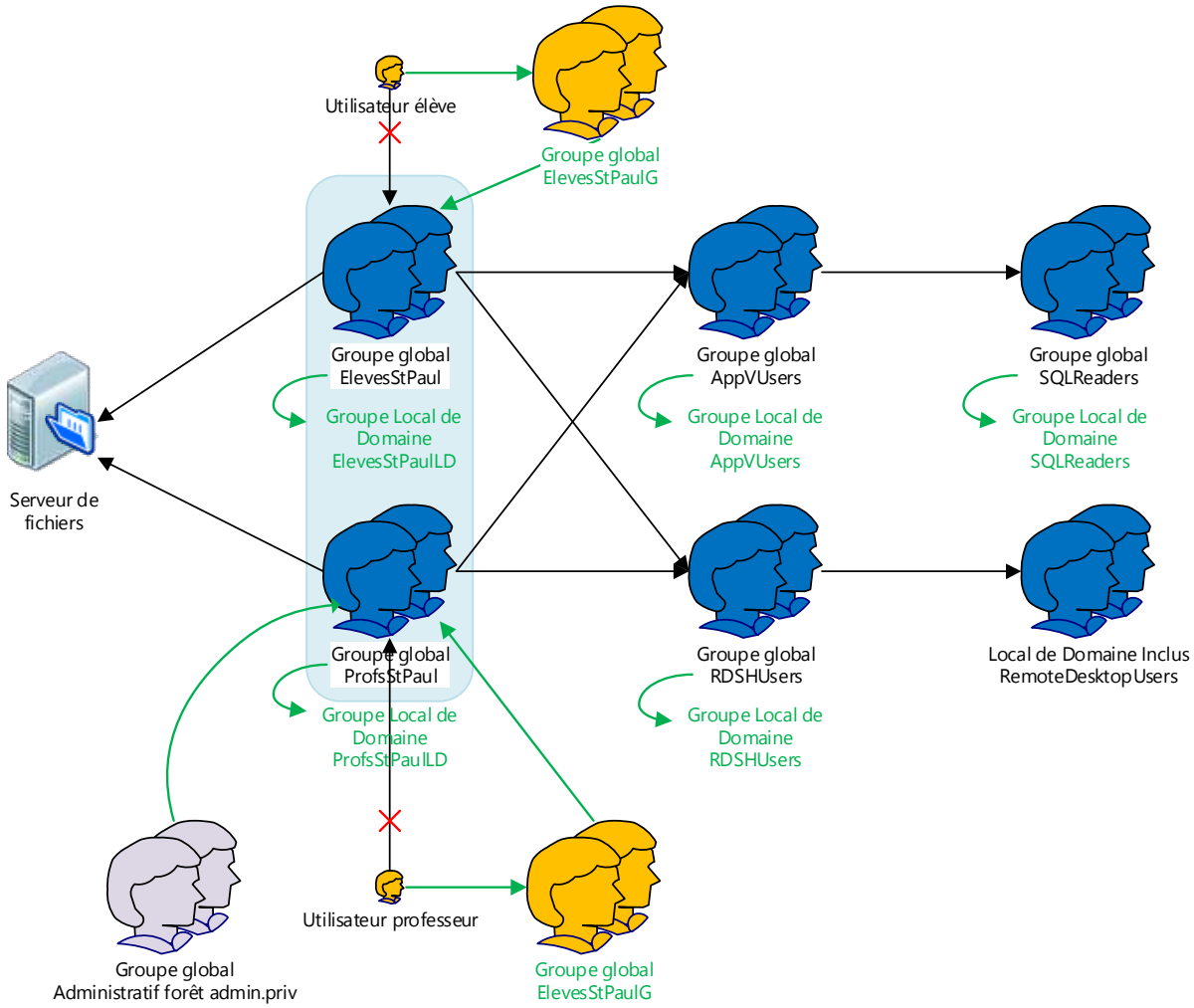


Figure 44 : Opérations à réaliser sur les imbrications de groupe de la forêt stpaul.org

En ce qui concerne les groupes de la forêt stjoseph.org, et dans la mesure où ces derniers vont être migrés vers la forêt stpaul.org, on va également s'assurer que les noms de groupes ne rentrent pas en conflits avec ceux de la forêt stpaul.org. Le cas échéant, ils seront renommés.

6.6.2 Stratégie de migration des groupes d'utilisateurs

Lors de toutes les tâches de migration, ADMT opère une comparaison entre ce qui est migré et ce qui a déjà été migré. Ainsi un utilisateur qui appartenait à tel groupe dans le

domaine source sera automatiquement réaffecté à ce groupe dans le domaine cible si ce dernier a été migré auparavant.

En se basant sur l'imbrication des types de groupes, on définit donc l'ordre de migration des groupes comme suit :

1- Les groupes locaux de domaine

2- Les groupes globaux

   Nous avons développé dans le chapitre précédent le placement des utilisateurs dans les groupes de type globaux et l'imbrication de ces derniers dans des groupes de type locaux de domaine. Le processus de migration ADMT permet de conserver les accès aux ressources grâce à l'attribut SIDHistory des utilisateurs et des groupes migrés mais ne permet pas l'affectation à la volée à de nouveaux groupes, ce qui nous oblige à procéder comme pour les groupes de la forêt Stpaul.org à la mise en application de la formule AGUDLP afin que l'étape de traduction de la sécurité se déroule au mieux (cf. chapitre *6.8.4.2.1 Traduction de la sécurité en mode ajouter*).

3- Les comptes utilisateurs

   En ce qui concerne le cas des comptes élèves et dans la mesure où leurs dossiers personnels ne sont pas conservés d'une année scolaire sur l'autre hormis les sections BTS, ces utilisateurs seront simplement créés dans la forêt StPaul.org.

   Les comptes administratifs de la forêt StJoseph.org seront recréés dans la forêt Admin.priv. En effet l'outil ADMT implique d'établir une relation d'approbation bidirectionnelle entre les forêts source et cible, ce qui n'est pas envisageable dans notre cas.

   Au final seuls les comptes d'utilisateurs professeurs seront migrés avec ADMT.

6.6.3 Table d'affectation des objets migrés

On créé des tables d'affectation afin de répertorier les objets à migrer dans lesquelles on retrouve les utilisateurs, groupes et comptes de services ainsi que les ordinateurs, serveurs membres ainsi que leur destination dans l'arborescence d'OU.

6.6.4 Développement d'un plan de test de migration

Il est impératif de mettre en place un plan de test afin d'identifier et corriger tout problème éventuel et ainsi de s'assurer qu'après migration les utilisateurs peuvent ouvrir une session et accéder aux ressources du domaine cible sur la base de leurs nouvelles informations de sécurité.

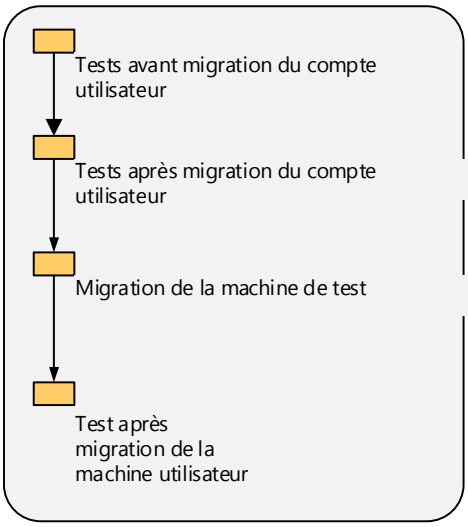


Figure 45 : plan de test de migration

On créera un utilisateur dans le domaine source par grande fonction en l'incluant dans les groupes appropriés. Une station de travail lui sera également attribuée. On pourra ainsi valider chaque étape du processus après tests grâce à la matrice de migration suivante :

Tableau 19 : matrice de test de migration

Migration Test Matrix			
Prepared By	Christophe Cornu	Date	01/04/15

Source Forest Name	StJoseph.org
Target Forest Name	StPaul.org
Source Domain Name	StJoseph.org
Target Domain Name	StPaul.org

Test Name	Performed Before Migration	Result	Notes
Ouverture de session dans le domaine source sur la machine de test non migrée	Oui	Succès	
Vérification de l'accès aux imprimantes et partages de fichiers sur la machine de test non migrée	Oui	Succès	
Ouverture de session dans le domaine cible sur la machine de test non migrée	Non	Succès	
Vérification de l'accès aux imprimantes et partages de fichiers sur la machine de test non migrée	Non	Succès	
Ouverture de session dans le domaine cible sur la machine de test migrée	Non	Succès	
Vérification de l'accès aux imprimantes et partages de fichiers sur la machine de test migrée	Non	Succès	

En cas d'échec d'une opération, il faudra en identifier l'origine puis la corriger. Le cas échéant on procédera à la restauration de la configuration d'origine grâce au plan de restauration.

6.6.5 Plan de restauration

Dans le cadre d'une migration inter forêt, un objet est simplement désactivé dans le domaine source. Il suffit de le réactiver pour le rendre à nouveau opérant.

S'il s'agit d'une machine, il faudra modifier l'appartenance de domaine et redémarrer la machine. En ce qui concerne les DC et les serveurs membres, une sauvegarde complète de la machine avant migration est réalisée.

6.6.6 Gestion des utilisateurs, des groupes et des profils d'utilisateurs

Le processus de migration peut s'étendre sur une période prolongée et nécessite de maintenir l'administration des objets dans le domaine source pendant cette période. En cas de retour arrière, il suffira de réactiver un compte d'utilisateur pour le rendre à nouveau opérationnel dans le domaine source. Ce compte doit bénéficier de toutes les évolutions, modifications opérées dans le domaine source depuis sa migration, appartenances aux groupes globaux comprises.

L'option *Migrer et fusionner les objets conflictuels* d'ADMT autorise la migration des comptes d'utilisateurs aussi souvent que nécessaire, permettant ainsi de propager les modifications apportées au compte résidant dans le domaine source au compte dans le domaine cible.

Dans les environnements actuels, les utilisateurs hors administratif se voient assigner un profil obligatoire. On ne traduira pas la sécurité sur ce profil avec l'outil ADMT, mais simplement en ajoutant les groupes cibles adéquats.

Pour les utilisateurs administratifs, on traduira la sécurité de leur profil itinérant « à la main » puisque la relation d'approbation entre les forêts Admin.priv et Stpaul.org ne permet pas l'utilisation de l'outil ADMT en place.

6.6.7 Projet de communication avec l'utilisateur final

Il faut informer les utilisateurs concernés, afin de leur expliquer la démarche engagée, l'impact des actions menées, que leur mot de passe devra être changé à la première ouverture de session sur le nouveau domaine… On publiera également un planning des interventions.

6.7 Préparation des domaines source et cible

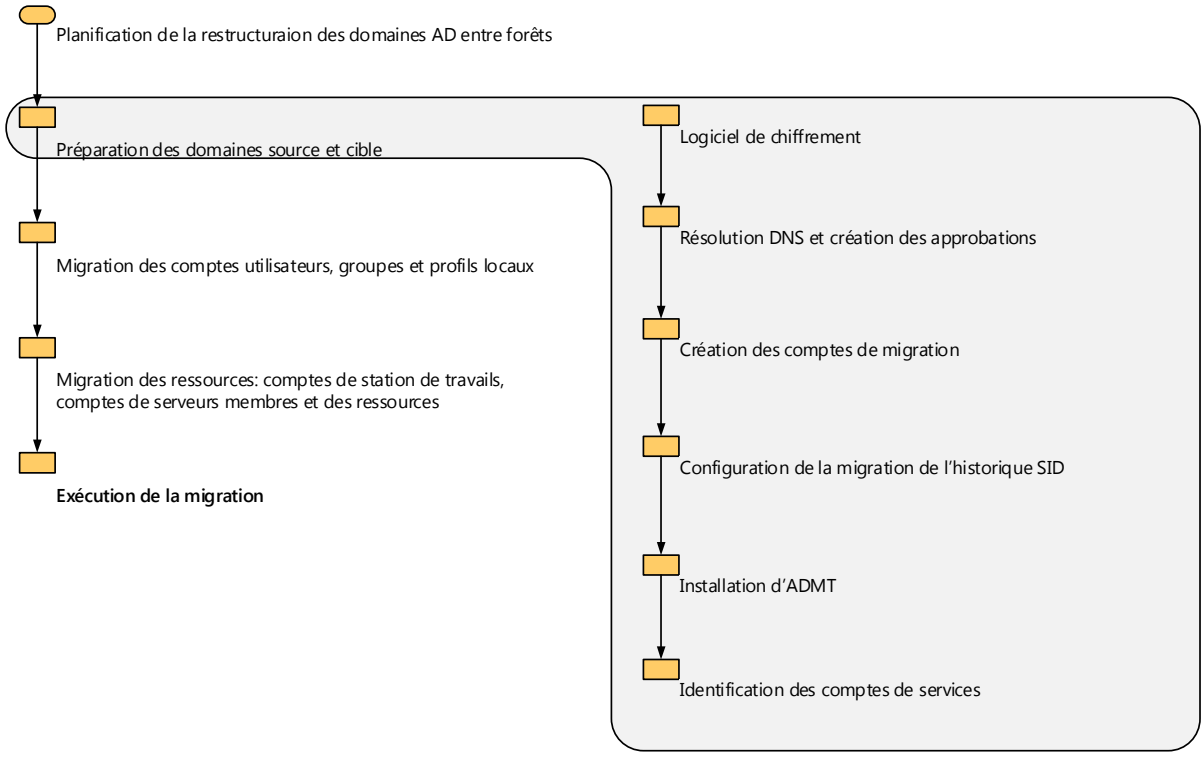


Figure 46 : préparation des domaines source et cible

6.7.1 Chiffrement de haut niveau

Le chiffrement 128 bits nécessaire à la sécurisation des flux inhérents aux opérations ADMT est installé en standard sur les machines Windows Server 2003 et ultérieures. Nous n'avons donc rien d'autre à faire sur ce point.

6.7.2 Résolution DNS et relation d'approbation

Avant de créer la relation d'approbation entre nos deux domaines, il faut s'assurer que la résolution DNS est bien en place. On configurera les redirecteurs conditionnels DNS adéquats dans chaque domaine.

Dans notre cas, nous avons besoin d'une relation d'approbation de forêt bidirectionnelle et sans filtrage de SID pour maintenir l'accès aux ressources pendant toute la durée de la migration.

Le filtrage de SID étant activé par défaut lors de la création d'une telle relation, il faut le désactiver avec la commande suivante :

```
netdom trust stjoseph.org /domain:stpaul.org
/enableSIDhistory:oui /userd:STJOSEPH\Administrateur
/passwordd:P@ssw0rd
```

Cette commande n'est valide que sur l'approbation de forêt sortante, soit celle du domaine approuvant (stjoseph.org) vers le domaine approuvé (stpaul.org).

6.7.3 Création des comptes de migration

Le processus de migration des comptes et ressources entre les forêts, nécessitent la création de comptes de migration possédant les droits adéquats dans les deux domaines concernés. ADMT utilise ces identifiants pour effectuer ses opérations. Selon l'objet à migrer, les droits à attribuer aux comptes de migration sont différents :

Tableau 20 : autorisations nécessaires en fonction des objets à migrer

Objet de migration	Informations d'identification nécessaires dans le domaine source	Informations d'identification nécessaires dans le domaine cible
Utilisateur/compte de services administrés/groupe sans historique SID	Autorisation **Lire toutes les informations utilisateur** déléguée sur l'unité d'organisation de l'utilisateur ou du groupe et informations d'identification d'administrateur de domaine	**Autorisations** Créer, supprimer et gérer les comptes d'utilisateurs. Créer, supprimer et gérer les groupes **et** Modifier l'appartenance d'un groupe **délégué pour l'unité d'organisation de l'utilisateur ou du groupe,**

		et administrateur local sur l'ordinateur sur lequel ADMT est installé
Utilisateur/compte de services administrés/groupe avec historique SID	Autorisation **Lire toutes les informations utilisateur** déléguée sur l'unité d'organisation de l'utilisateur ou du groupe et informations d'identification d'administrateur de domaine	**Autorisation déléguée sur l'unité d'organisation de l'utilisateur ou du groupe, autorisation étendue de migration de l'historique SID et administrateur local sur l'ordinateur sur lequel ADMT est installé**
Ordinateur	Administrateur de domaine ou administrateur dans le domaine source et sur chaque ordinateur	**Autorisation déléguée sur l'unité d'organisation de l'ordinateur et administrateur local sur l'ordinateur sur lequel ADMT est installé**
Profil	**Administrateur local ou administrateur de domaine**	**Autorisation déléguée sur l'unité d'organisation de l'utilisateur et administrateur local sur l'ordinateur sur lequel ADMT est installé**

Dans la mesure où la migration ne sera effectuée que par une seule personne, un seul compte de migration est créé. Ce dernier disposera des caractéristiques suivantes afin de mener à bien toutes les étapes de la migration :

- Compte MigrAdmin créé dans le domaine cible stpaul.org
- Membre du groupe *Admins du domaine* cible stpaul.org
- Droit de « Migrer l'historique SID » au niveau du domaine ou d'UO spécifiques :

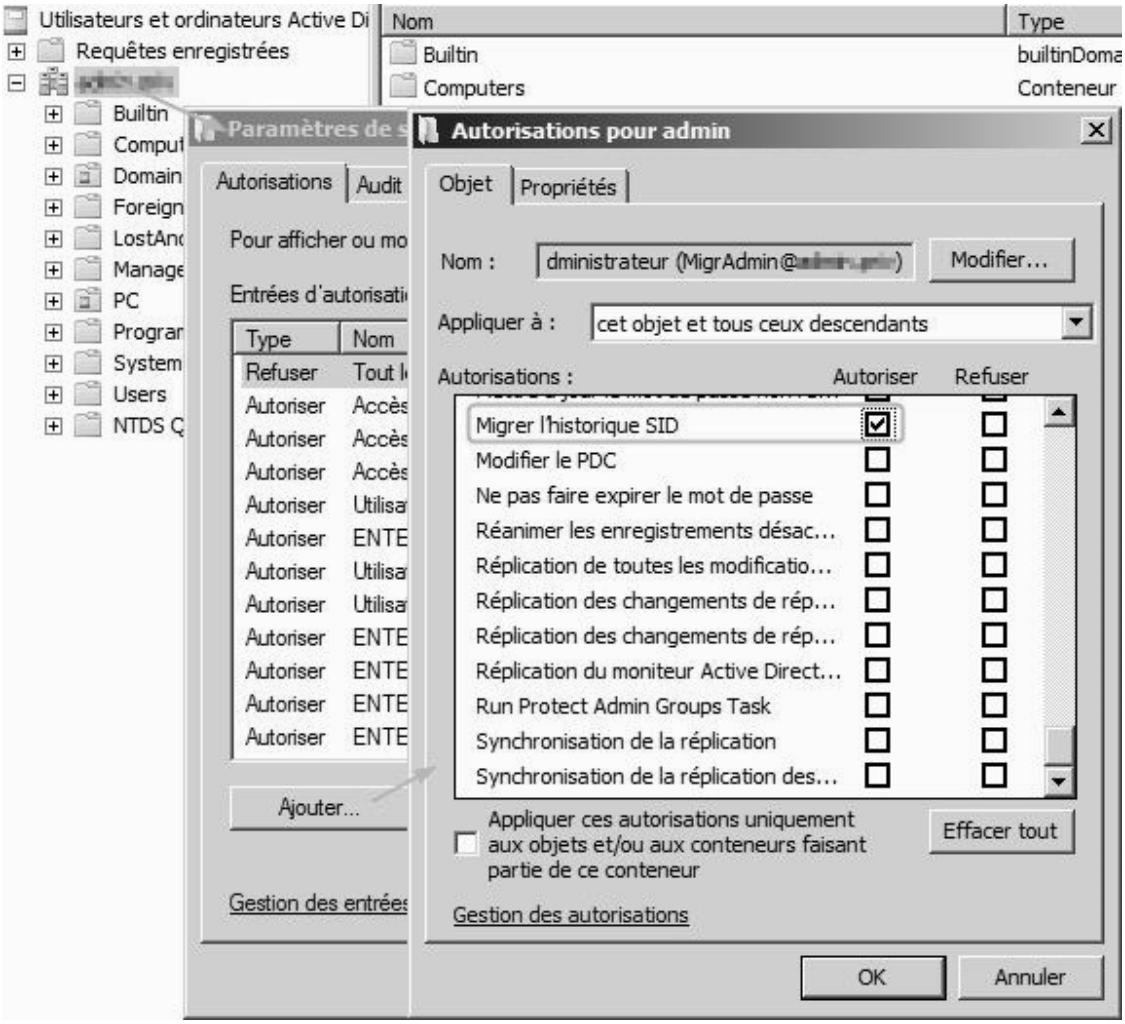


Figure 47 : Autorisations de migrer l'historique SID

- Membre du groupe *BUILTIN\Administrateurs* du domaine source

- Membre du groupe *Administrateurs* de chaque machine membre du domaine source. Cette opération peut être réalisée à l'aide d'une GPO nommée Migration.

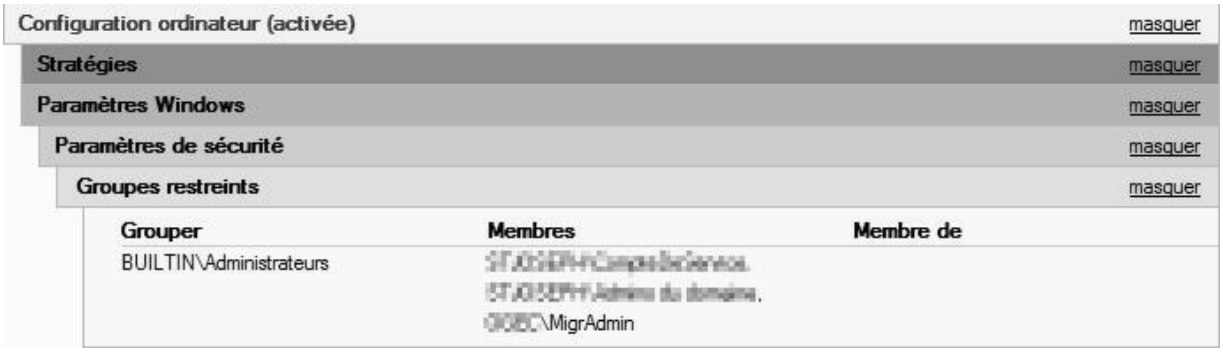


Figure 48 : GPO ajout compte de migration au groupe Administrateurs locaux

Toutes les communications entre ADMT et les agents ADMT installés sur les machines se font par l'intermédiaire de RPCs. Ces dernières utilisant potentiellement tous les ports TCP compris entre 1024 et 5000, on autorisera l'exception « Fichiers et partages » dans le firewall des machines via la GPO Migration.

6.7.4 Configuration des domaines pour la migration de l'historique SID

Cette configuration concerne la mise en place de l'audit de la gestion des comptes ainsi que l'audit d'accès au service d'annuaire. Elle est réalisée automatiquement lors de l'installation d'ADMT.

6.7.5 Configuration de la structures d'UO cible

La structure d'OU cible doit être définie afin d'accueillir les nouveaux objets utilisateurs, groupes et ordinateurs. Les OUs Administratif et AdministratifPeda du domaine source ne seront pas migrées dans des OUs cibles. Les comptes d'utilisateur Administratif seront créés dans le domaine Admin.priv après le renommage du domaine stpaul.org Administratif. En effet, au vu du nombre réduit d'utilisateurs, des nouveaux paramétrages du logiciel Charlemagne et de la mise en service de ce dernier mi-août 2015, il n'y a pas d'intérêt à mettre en place un processus de migration stjoseph.org admin.priv pour ces comptes.

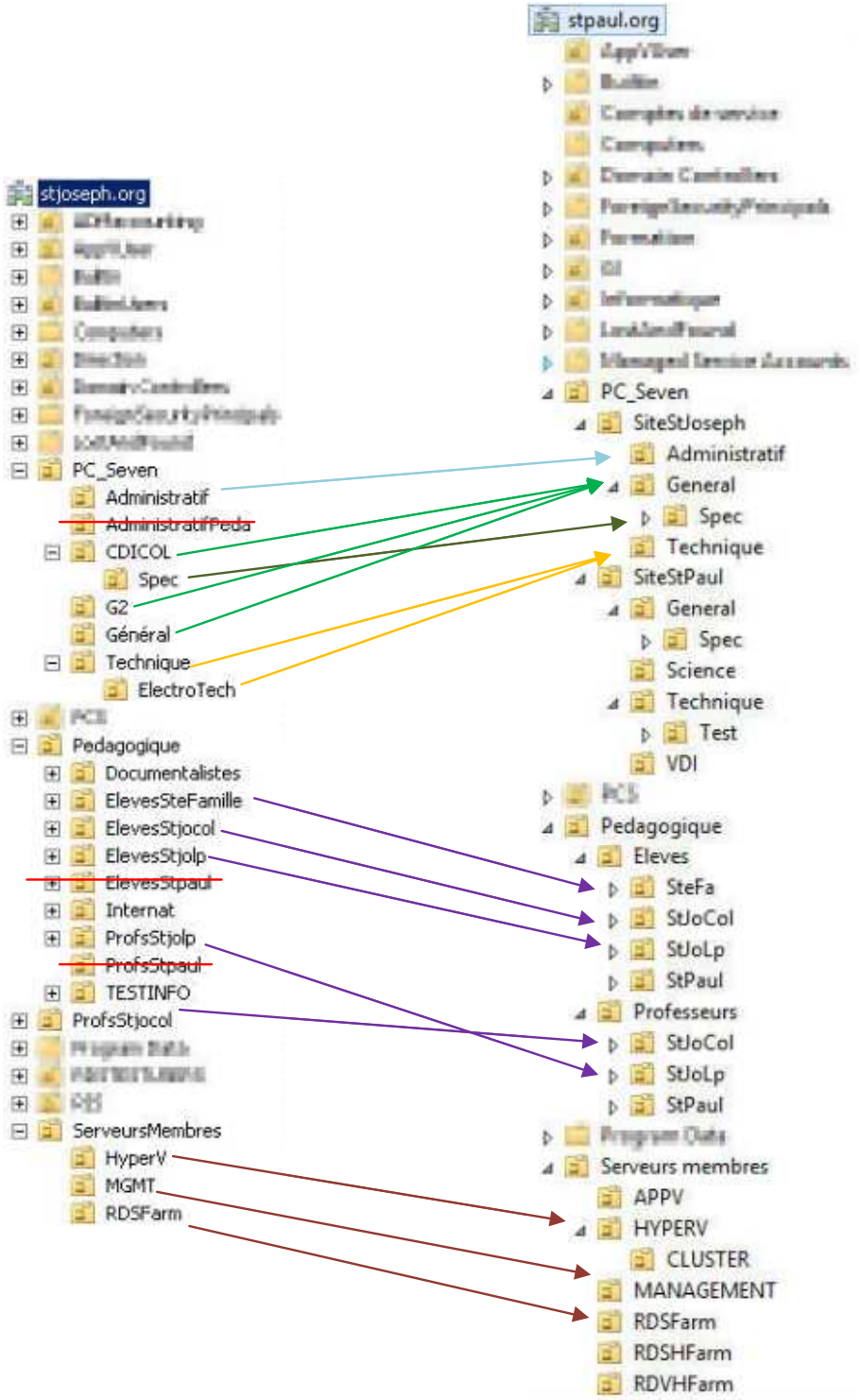


Figure 49 : Mouvements des objets des OUs sources vers les OUs cibles

Les comptes de l'OU AdministratifPeda du domaine stjoseph.org sont abandonnés, leur seul raison d'exister étant la nécessité d'accéder au logiciel Aplon pour l'édition des bulletins de notes, ce qui ne sera plus le cas avec Charlemagne.

Les fermes RDSH nécessitent des OUs distinctes du fait des versions serveurs différentes sur lesquelles elles s'appuient et du fonctionnement inhérents à ces versions. En effet, la ferme RDSH St Paul sous Windows Server 2012 ne nécessite pas la même infrastructure que la version Windows server 2008 R2 de la ferme St Joseph. De plus des OUs séparées facilitent la lecture et l'application des GPO.

6.7.6 Installation d'ADMT v3.2 et de PES v3.1

ADMT v3.2 ne peut être installé que sur un serveur 2008 R2, le portage vers Windows Server 2012 n'étant pas encore effectif à ce jour. Cette machine sera un serveur membre du domaine cible stpaul.org, ainsi si la relation d'approbation de forêts doit être plus sécurisée en supprimant la relation entrante pour le domaine stjoseph.org, la machine se trouvera toujours du côté du domaine approuvé.

Tout le paramétrage se fera dans le contexte de sécurité de l'utilisateur MigrAdmin précédemment créé.

6.7.6.1 Prérequis

ADMT requiert l'installation d'une base de données SQL. La version SQL Server 2008 Express SP1 est gratuite et suffisante, mais nous oblige à utiliser la console ADMT sur le poste où le serveur de base de données est installé, ce qui ne constitue un inconvénient que lorsque la migration doit être effectuée par plusieurs personnes. L'instance SQL sera exécutée dans le contexte de sécurité AUTORITE NT\Système du serveur ADMT.

6.7.6.2 Installation de Password Export Server PES

Afin de migrer les mots de passe utilisateurs, ADMT s'appuie sur un serveur d'exportation de mots de passe. Ce dernier doit être installé sur un DC du domaine

source. Il cryptera les mots de passe avant de les transmettre à ADMT. Afin de réaliser les opérations de cryptage/décryptage, les tenants doivent utiliser une clé symétrique partagée générée au préalable par une commande sur la machine ADMT. Cette clé sera demandée lors de l'installation du service PES.

```
Admt key /option:create /sourcedomain:stjoseph.org
/keyfile:path_to_migration.pes /keypassword:P@sswOrd
```

PES est installé sur le DC AD-RescueStJoseph du domaine source stjoseph.org en tant que service. Pour des raisons de sécurité, il conviendra de ne démarrer ce service que lorsqu'un processus de migration le nécessitera.

Lors des tests de migration de comptes d'utilisateurs l'erreur suivante peut se produire.

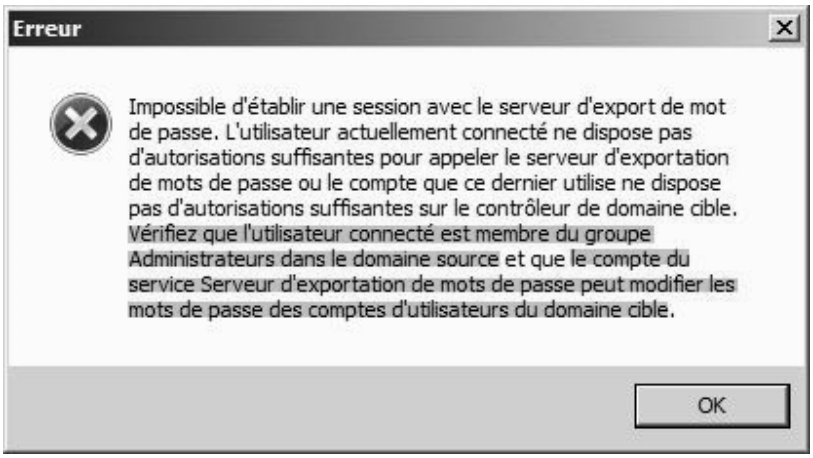


Figure 50 : Message Erreur PES

Le compte de service du service PES doit avoir le droit de modifier les mots de passes des comptes d'utilisateurs du domaine cible. On choisira donc d'exécuter le service PES sous le compte de migration MigrAdmin.

6.7.6.3Architecture de déploiement ADMT

Nous avons vu que la machine ADMT appartenait au domaine cible stpaul.org, il reste cependant à choisir un emplacement physique pour cette machine. Il semble judicieux d'effectuer toute les opérations de migration sur le site stjoseph.org, et de s'appuyer sur

la réplication AD inter-sites pour propager les modifications à l'ensemble des contrôleurs de domaine de la forêt stpaul.org. On bénéficie ainsi de la bande passante du site local.

La machine ADMT ainsi qu'un nouveau contrôleur de domaine AD-03.stpaul.org de la forêt stpaul.org sont placés sur le site stjoseph.org.

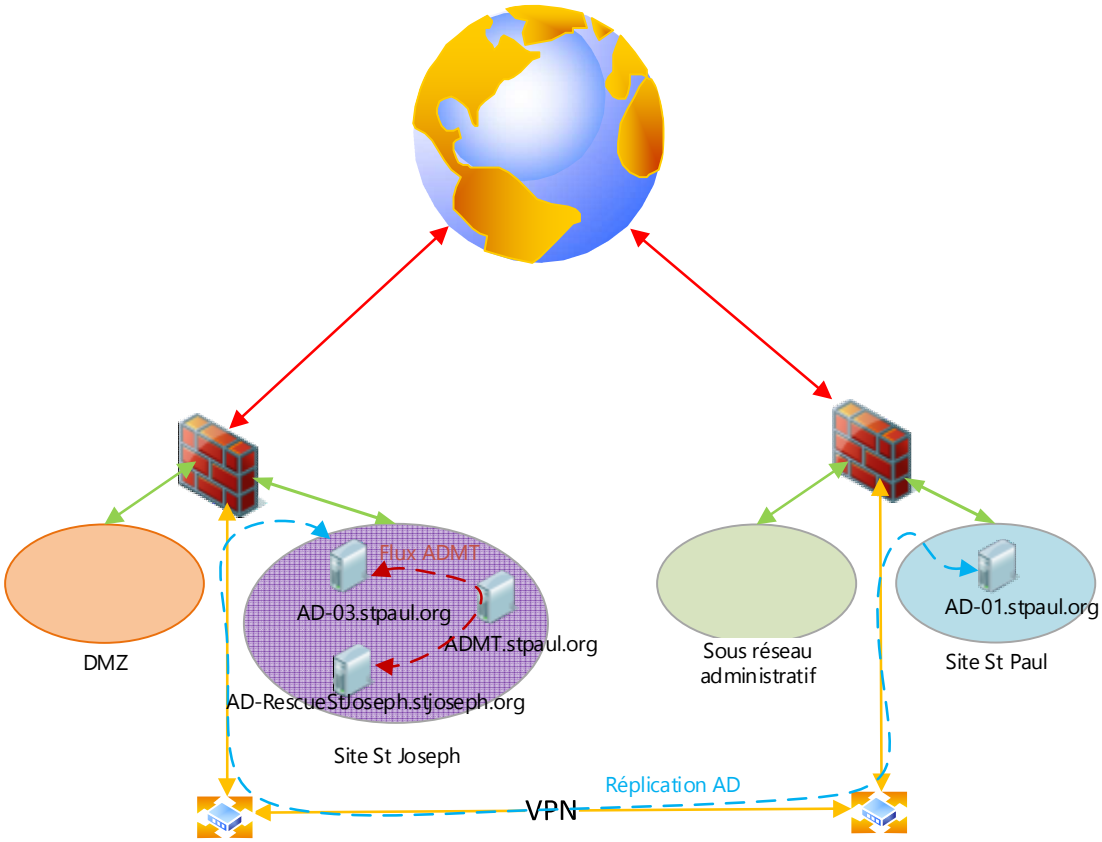


Figure 51 : Architecture ADMT

6.7.7 Initialisation et test d'ADMT

Afin d'initialiser ADMT, il suffit de lancer la migration d'un groupe global Test créé à cet effet dans le domaine source stjoseph.org. ADMT demande de renseigner les domaines source et cible, et de désigner un DC dans chaque domaine à moins de le laisser en choisir un lui-même. On préfère cependant orienter ADMT vers les DCs les moins

chargés soit AD-RescueStJoseph.stjoseph.org pour le domaine source, et AD-03.stpaul.org pour le domaine cible.

Lors de ce premier lancement, on choisira également de tester la migration de SID en cochant l'option dans l'assistant. A la fin de l'opération, l'objet doit être migré et l'attribut sIDHistory renseigné.

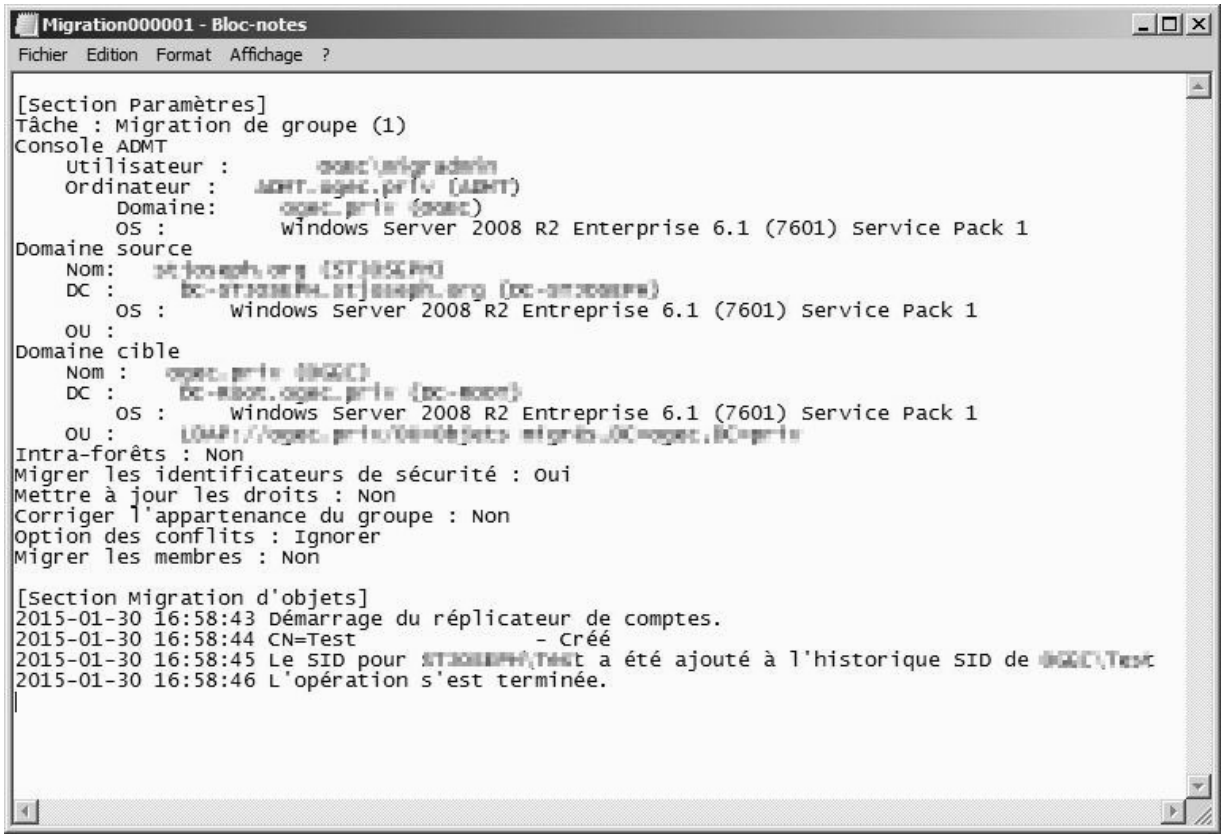


Figure 52 : fichier de log d'une opération de migration ADMT

Toute erreur consignée dans le journal de l'assistant ADMT devra être corrigée.

6.7.8 Identification des comptes de services

Un compte de service est un compte d'utilisateur qui offre un contexte de sécurité à des applications et des services qui disposent des autorisations inhérentes à ce compte pour ouvrir une session en tant que service, accéder aux ressources du réseau… Les comptes

de services locaux (service local et service réseau) sont migrés en même temps que la machine.

L'assistant ADMT permet d'identifier ces comptes en lançant un agent sur des machines spécifiées. Lorsqu'un compte de service est identifié, il est enregistré dans la base de données ADMT pour pouvoir être migré ultérieurement en même temps que les comptes d'utilisateurs du domaine source. Il est à noter que le mot de passe d'un compte de service n'est jamais migré, ADMT régénère un mot de passe complexe lors de la migration d'un compte de service.

On peut dresser le tableau suivant afin de répertorier les comptes de services renvoyés par ADMT pour le domaine source stjoseph.org. Il nous servira également lors de la migration des comptes de services afin d'identifier plus facilement les paires machine/compte de service.

Tableau 21 : comptes de service renvoyés par ADMT

Machine	Service	Compte de service
Amalthee	Kaspersky Lab Administration Server	STJOSEPH\KL-AK-F4074FAA269B89
AD-RescueStJoseph	Service d'exportation des mots de passe	STPAUL\migradmin

On dénombre peu de compte de service. Ceci est dû au fait que la très grande majorité des services sont lancés dans un contexte de sécurité offert par des comptes de services prédéfinis gérés par le système d'exploitation. Il existe 3 comptes de service Windows, chacun bénéficiant de droits plus ou moins étendus :

- Compte système local : compte puissant qui a un accès total à l'ordinateur. Il peut accéder au réseau sous le nom du compte d'ordinateur.
- Compte Service local : compte disposant de privilèges limités à l'instar d'un compte utilisateur local authentifié. Il n'a pas d'accès particulier au réseau.

- Compte Service réseau : ce compte dispose des mêmes droits d'utilisateur que le compte de Service local. Il accède au réseau sous le nom du compte d'ordinateur.

Dans l'éventualité où le compte « administrateur du domaine » est également utilisé comme compte de service et compte tenu du fait que ce compte n'est pas migré, deux solutions sont possibles pour assurer la continuité des services exécutés dans ce contexte de sécurité : soit les services sont repris une fois la machine migrée, et les services sont reconfigurés pour utiliser un nouveau compte de service du domaine cible, soit on effectue l'opération inverse.

6.8 Migration des comptes

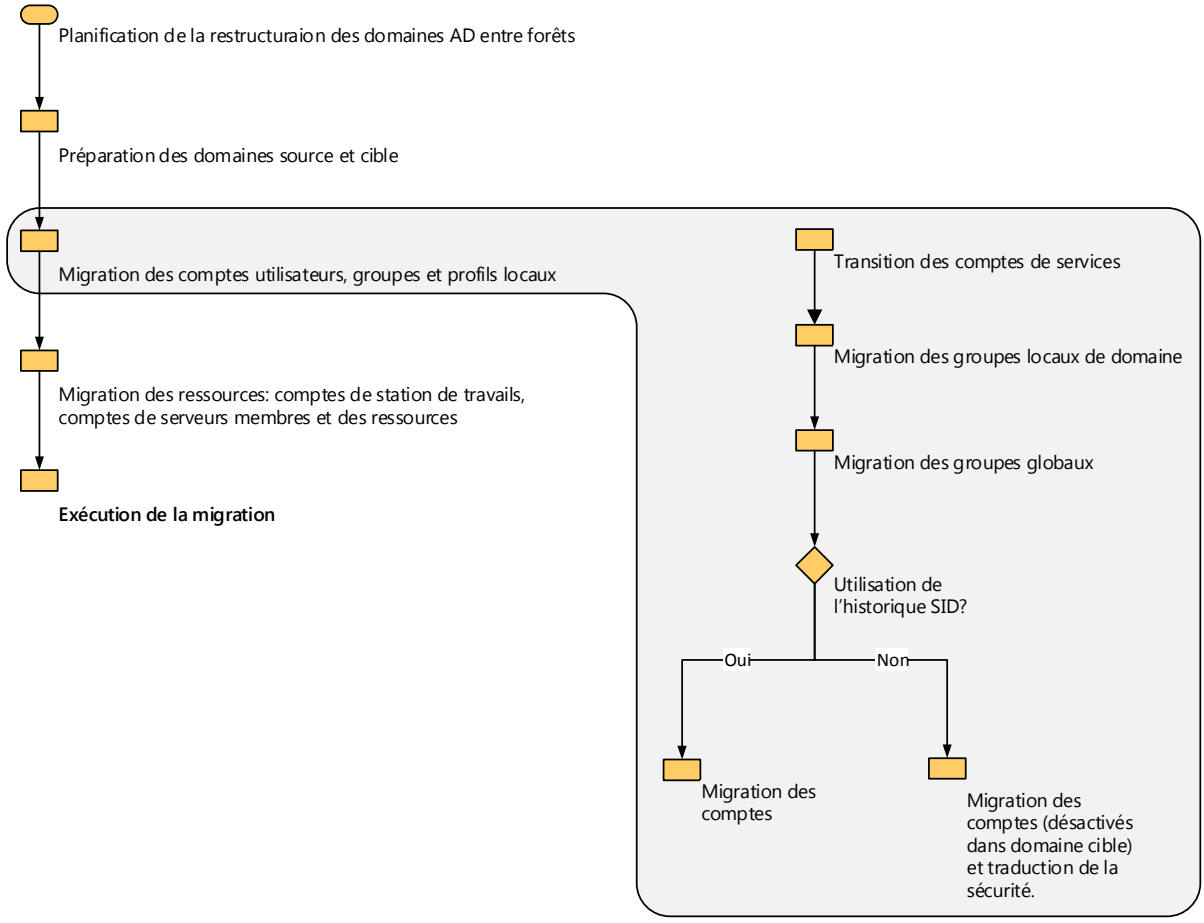


Figure 53 : matrice de migration des comptes

6.8.1 Transfert des comptes de services

Cette opération effectue la migration du compte de service vers le domaine cible, puis modifie les services sur toute les machines membres spécifiées afin d'utiliser le compte migré.

L'assistant ADMT « Migration des comptes d'utilisateurs » réalise toutes ces actions automatiquement. Pour rappel, ADMT régénère les mots de passes des comptes de services quel que soit le choix effectué :

Figure 54 : Assistant 1 ADMT de Migration de comptes d'utilisateurs

Le compte est activé dans le domaine cible et la migration des SID est effectuée en même temps. Sans cela, les services du domaine cibles ne pourront redémarrer avec le nouveau compte de service.

Figure 55 : Assistant 2 ADMT de Migration de comptes d'utilisateurs

Les droits du compte de service doivent également être migrés. En effet, ces comptes bénéficient souvent de privilèges plus élevés requis par les services qui les utilisent pour s'exécuter, on se doit donc d'en assurer la continuité.

Figure 56 : Assistant 3 ADMT de Migration de comptes d'utilisateurs

L'assistant propose une liste des comptes de services précédemment identifiés. Il suffit d'inclure ces comptes et de sélectionner « Effectuer la migration … et mettre à jour Service Control Manager ».

Figure 57 : Assistant 4 ADMT de Migration de comptes d'utilisateurs

Après migration, on vérifiera que les services sont actifs et reflètent le changement de compte de service.

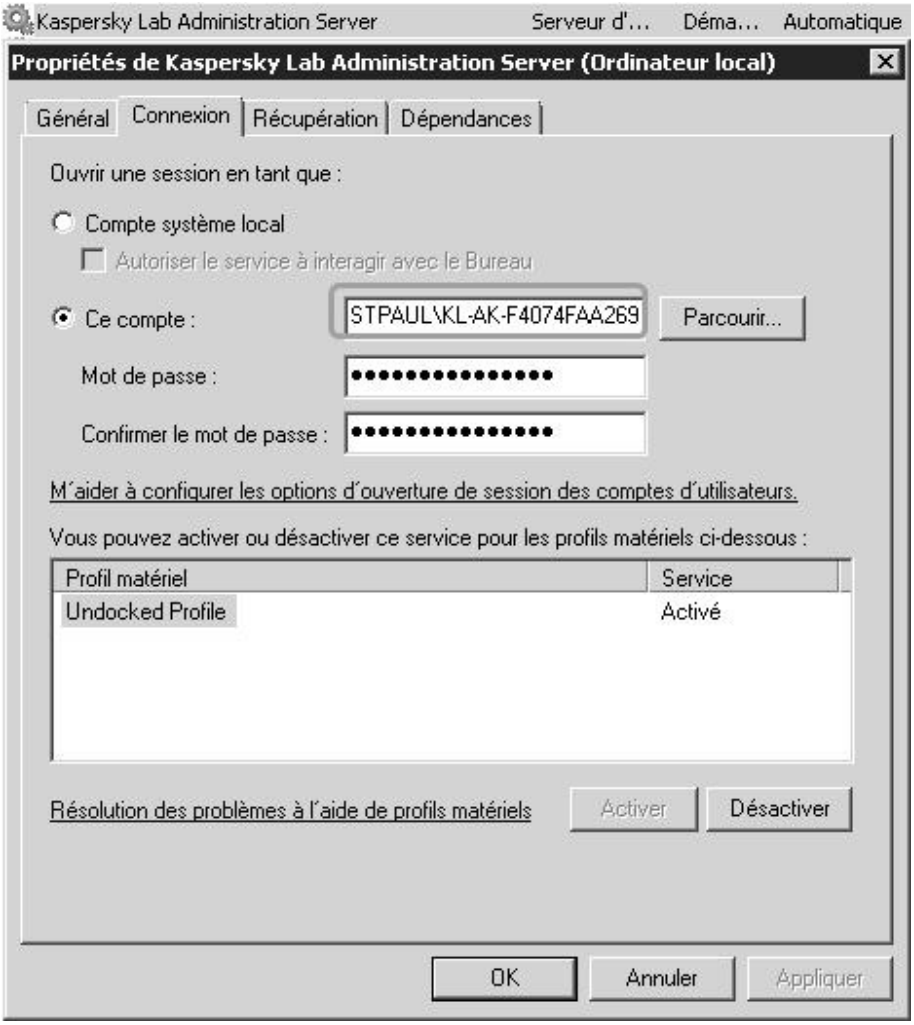


Figure 58 : Compte de service Kaspersky Administration Service après migration

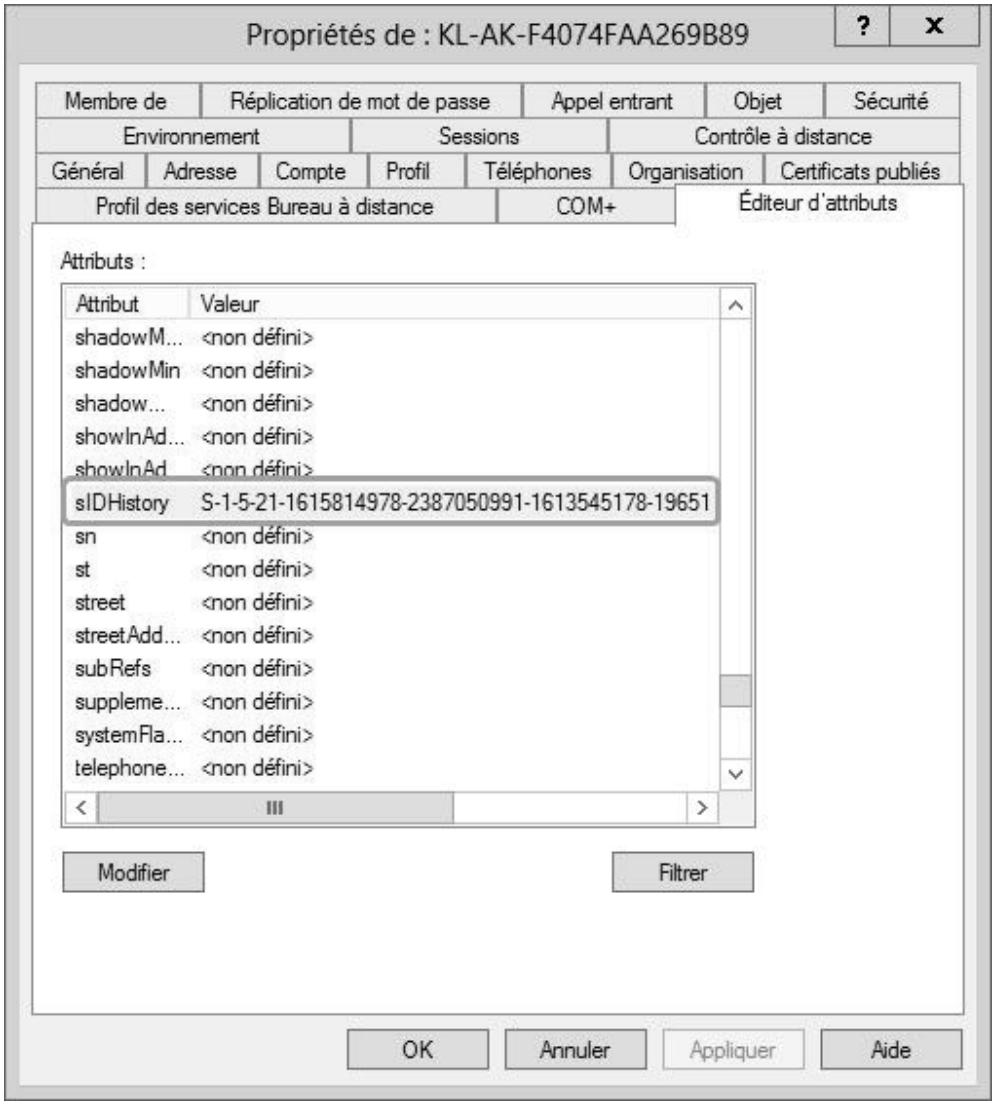


Figure 59 : sIDHistory compte de service Kaspersky

6.8.2 Migration des groupes locaux de domaine

On conservera l'historique SID des groupes afin d'assurer la continuité des accès.

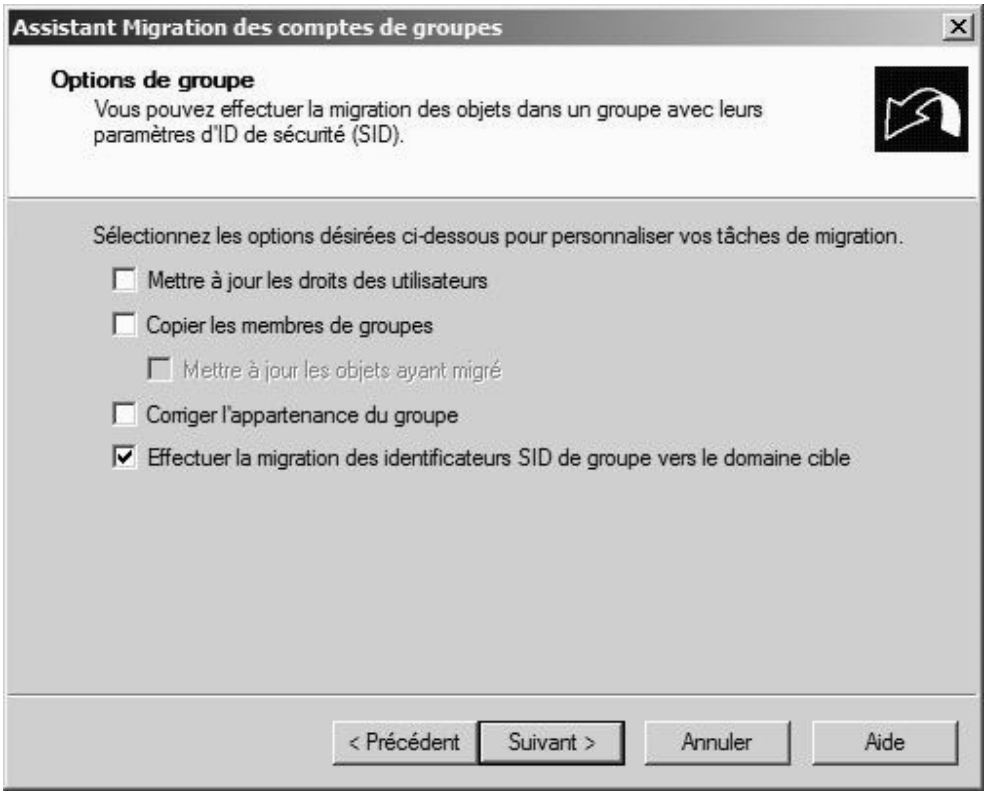


Figure 60 : Assistant 1 ADMT de Migration de comptes de groupes

6.8.3 Migration des groupes globaux

Comme explicité au chapitre *6.6.2 Stratégie de migration des groupes d'utilisateurs*, il est important de migrer les groupes globaux avant les comptes d'utilisateurs, cela permet une réassignation automatique des comptes d'utilisateurs aux groupes globaux lors de la migration.

ADMT identifie les groupes globaux du domaine source auxquels appartiennent les utilisateurs, puis détermine si les groupes globaux ont été migrés. Si tel est le cas, ADMT ajoute les comptes d'utilisateurs aux groupes correspondants dans le domaine cible.

On conservera l'historique SID des groupes afin d'assurer la continuité des accès et la correction d'appartenance aux groupes locaux de domaine précédemment migrés.

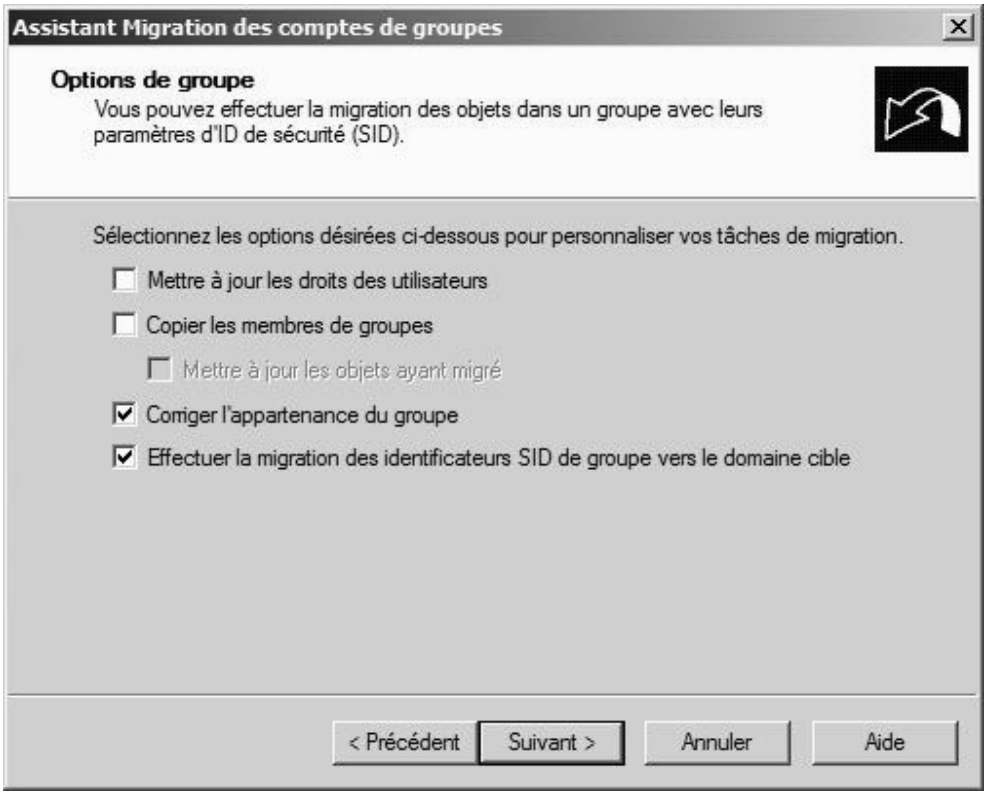


Figure 61 : Assistant 2 ADMT de Migration de comptes de groupes

6.8.4 Migration de comptes avec l'historique SID

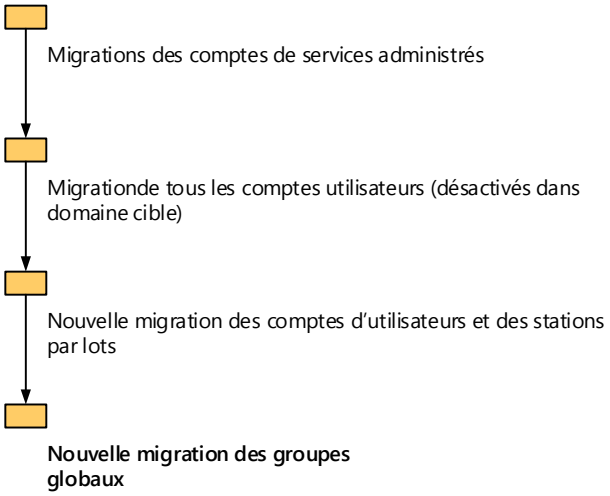


Figure 62 : matrice de migration de comptes avec historique SID

6.8.4.1Migration des comptes de services administrés

A l'instar des comptes de service précédemment cités, les comptes de services administrés offrent un contexte de sécurité pour l'exécution des services, à ceci près qu'ils fournissent en sus une gestion automatique des mots de passe et une gestion simplifiée du nom principal du service, ainsi que de la délégation de ces fonctionnalités de gestion à d'autres administrateurs. ADMT permet dans un premier temps de les identifier, puis de les migrer. Nous n'en disposons sur aucun de nos sites.

6.8.4.2Migrations de tous les comptes d'utilisateur

Les comptes d'utilisateurs sont migrés sans être activés dans le domaine cible, ceci permettant de peupler les différents OU et de commencer la traduction de sécurité. On choisira de générer un mot de passe complexe lors de cette opération afin de sécuriser les comptes et d'éviter qu'un utilisateur se connecte au domaine cible en cours de migration.

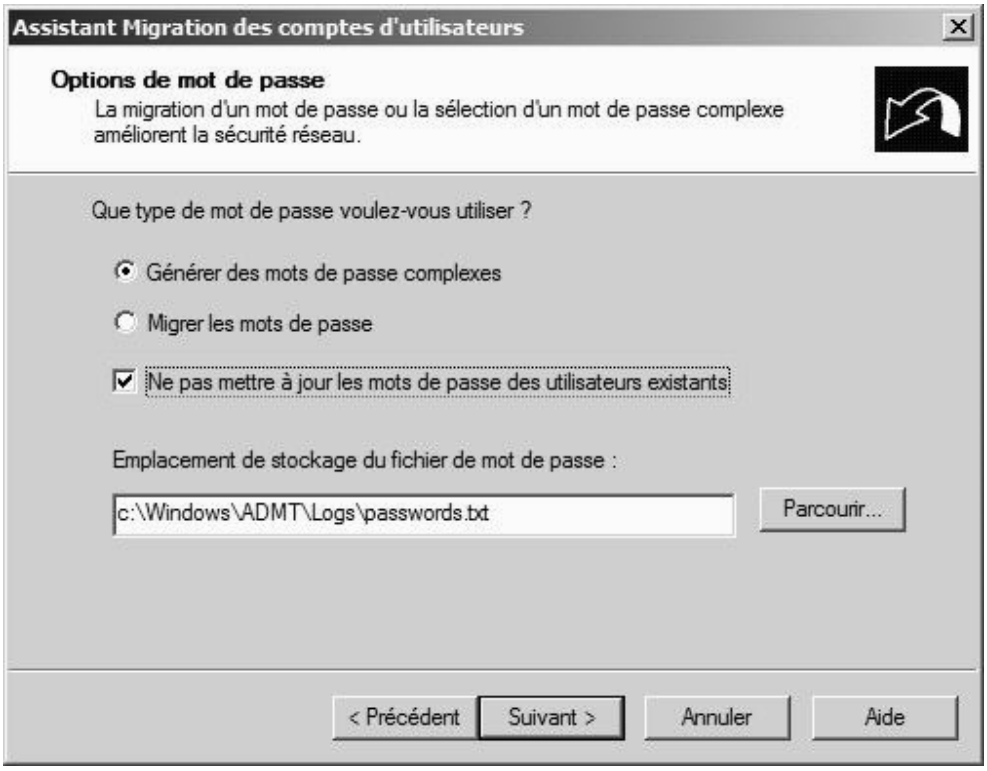


Figure 63 : Assistant 5 ADMT de Migration de comptes d'utilisateurs

Attention à ne pas désactiver le compte dans le domaine source. On pourra cependant définir une date de désactivation.

Figure 64 : Assistant 6 ADMT de Migration de comptes d'utilisateurs

6.8.4.2.1 Traduction de la sécurité en mode ajouter

Il s'agit ici d'ajouter les SIDs des utilisateurs et groupes migrés vers le domaine cible aux ressources de type partage de fichiers, fichiers, et groupes locaux.. Sont donc concernés les serveurs de fichiers du domaine source :

Tableau 22 : ressources à traduire

Nom de la machine	Ressources hébergée
Callisto	Dossiers et profiles utilisateurs
Appv-01	Contenu AppV

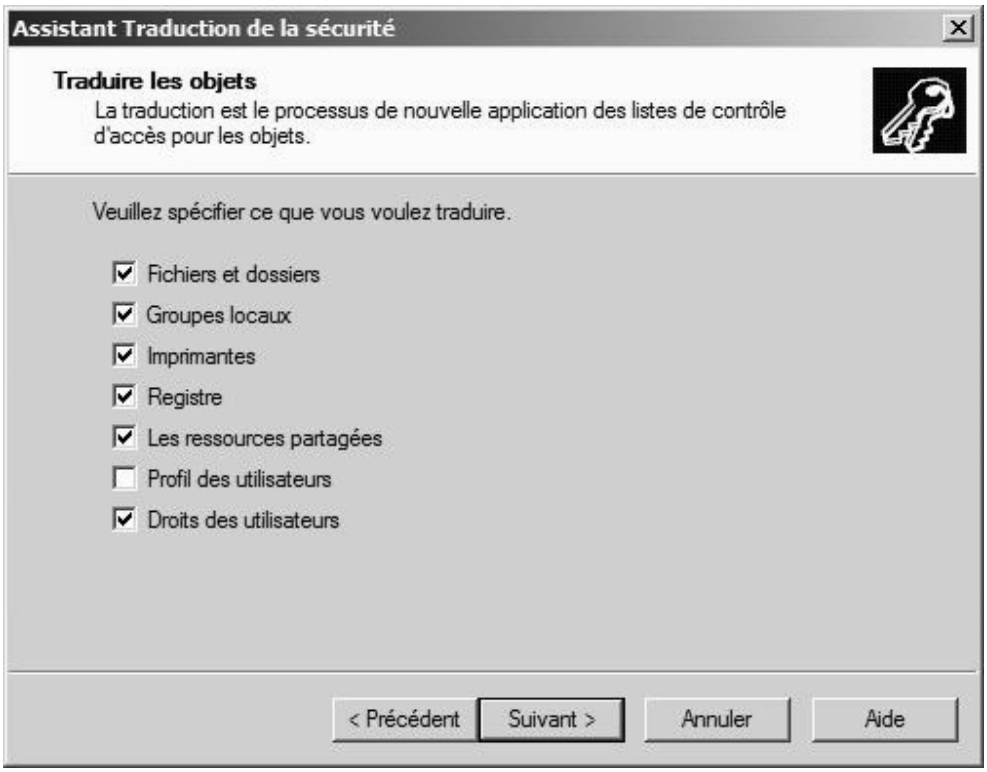


Figure 65 : Assistant 1 ADMT traduction de la sécurité

Cette opération peut accaparer un pourcentage des ressources non négligeable sur les machines ciblées. On veillera donc à réaliser la traduction sur des périodes de faible activité.

6.8.4.3Nouvelle migration des comptes d'utilisateurs et migration des stations par lots

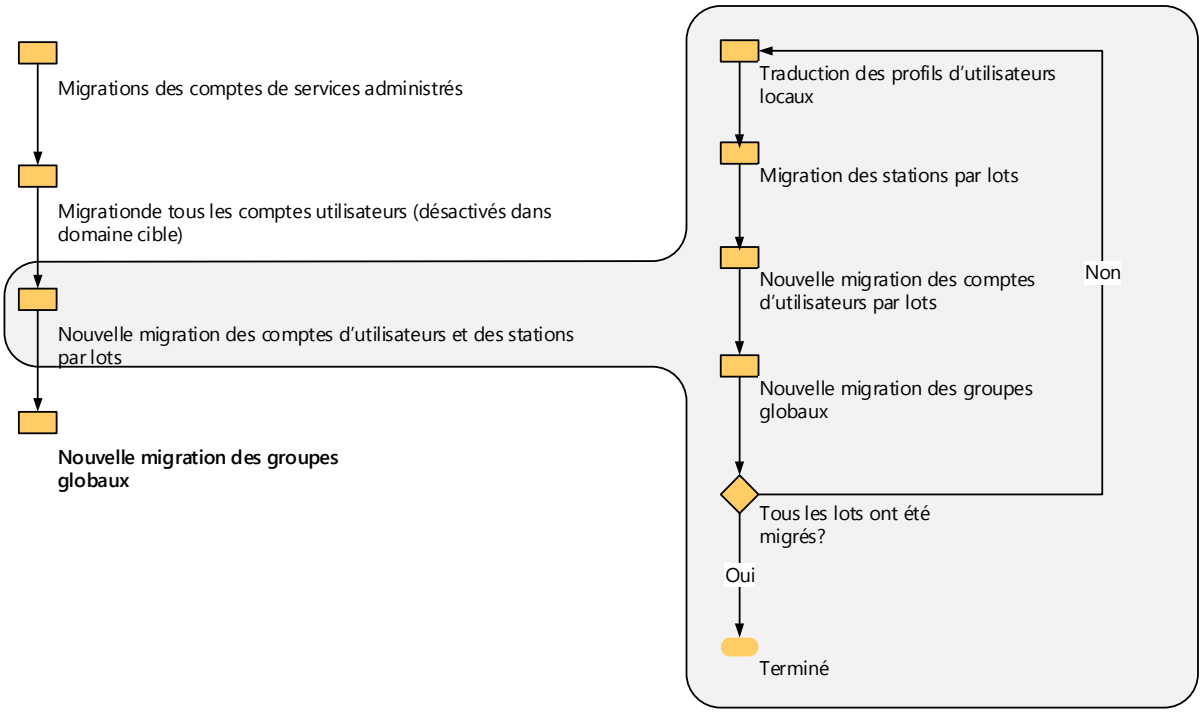


Figure 66 : matrice de migration des utilisateurs et machines par lots

6.8.4.3.1 Traduction des profils utilisateurs locaux

Cette étape consiste à traduire la sécurité des profils utilisateurs locaux. Dans la mesure où nous avons fait le choix depuis plusieurs années d'utiliser des profils itinérants obligatoires pour tous nos utilisateurs, cette étape ne nous concerne pas.

6.8.4.3.2 Migration des stations de travail par lots

Cette étape va créer un compte de machine dans le domaine cible, puis installer un agent ADMT sur la station à migrer. Cet agent va permettre entre autres choses de redémarrer la machine afin de terminer sa migration.

6.8.4.3.2.1 Préparation des machines à migrer

Nous avons vu que l'opérateur de migration MigrAdmin devait faire partie du groupe Administrateurs de chaque machine membre à migrer. Il faut également autoriser ADMT à communiquer avec l'agent ADMT installé en fin de migration. Une fois la machine

migrée et redémarrée, l'agent effectue des vérifications post migration afin de s'assurer que la station se trouve bien dans le domaine cible. Les exceptions de pare feu doivent donc être elles aussi appliquées dans le domaine cible, ce qui est déjà le cas dans le domaine stpaul.org.

6.8.4.3.2.2 Migration des stations

Il s'agit maintenant de migrer les stations correspondantes aux profils locaux précédemment traduits. La base SAM dans laquelle sont déclarés les utilisateurs et groupes locaux sera migrée avec l'ordinateur, il n'est donc pas nécessaire de procéder spécifiquement à leur migration.

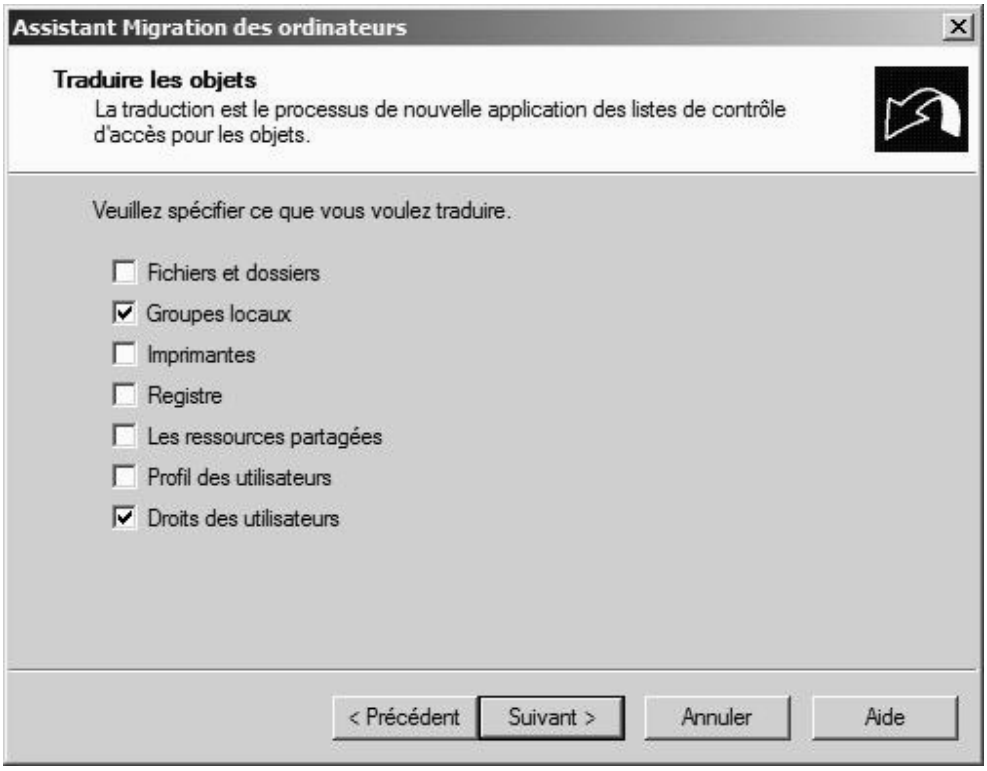


Figure 67 : Assistant 1 ADMT de Migration de comptes d'ordinateurs

On choisit d'ajouter les références de sécurités plutôt que de les remplacer, ceci afin de conserver la possibilité d'un accès à la machine par un utilisateur non encore migré.

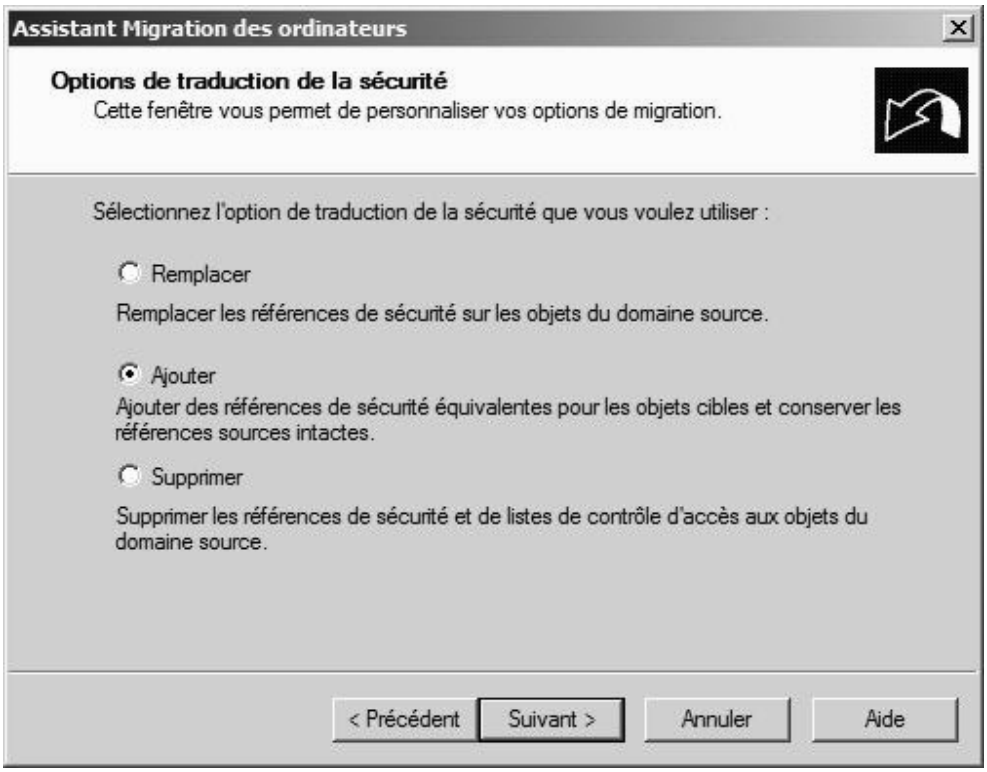


Figure 68 : Assistant 2 ADMT de Migration de comptes d'ordinateurs

Un temps avant redémarrage de la machine est à spécifier. On choisira au moins 5 minutes afin de laisser le processus de traduction s'achever correctement.

6.8.4.3.3 Nouvelle migration des comptes d'utilisateurs

On procède cette fois à la migration des comptes d'utilisateurs en les activant dans le domaine cible cette fois (on choisira de programmer une désactivation dans le domaine source). Les mots de passes des utilisateurs sont conservés dans la mesure où les stratégies de comptes du domaine cible sont identiques à celles du domaine source. Le système demandera tout de même de changer le mot de passe à la première connexion.

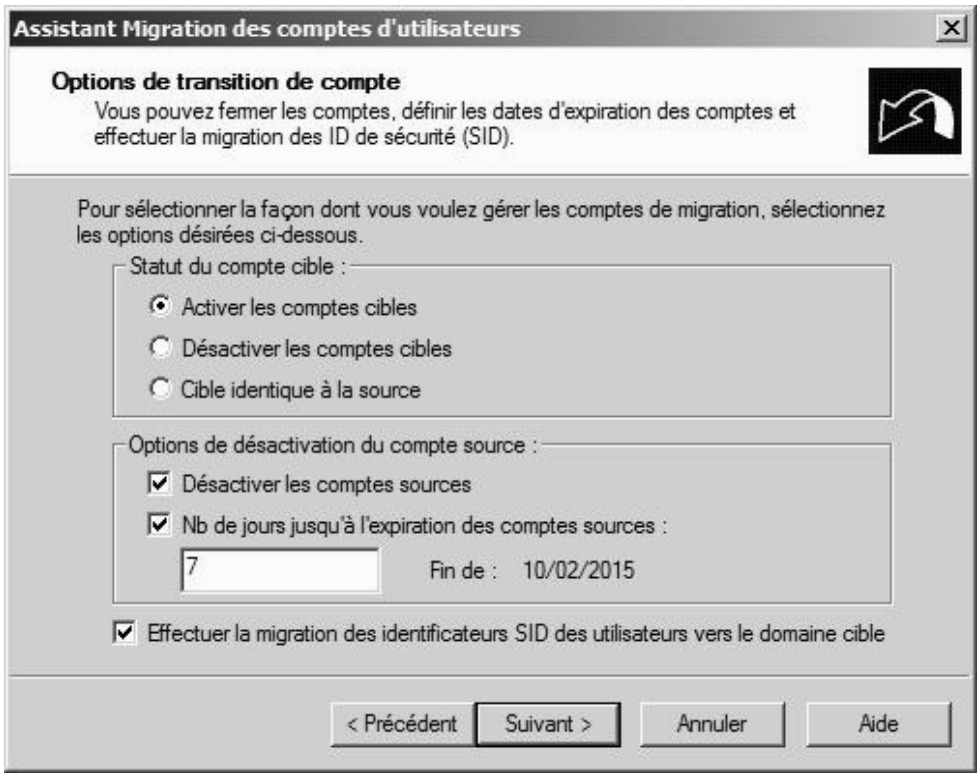


Figure 69 : Assistant 10 ADMT de Migration de comptes d'utilisateurs

Les profils itinérants peuvent être traduits à cette étape si cela n'a pas été déjà fait lors de la première migration de comptes d'utilisateurs. Comme les profils itinérants sont obligatoires, la traduction de la sécurité peut être effectuée « à la main » en ajoutant les groupes d'utilisateurs cibles nécessaires.

6.8.4.4Nouvelle migration des groupes globaux

Une nouvelle migration des groupes globaux permet de garantir que toute modification ayant eu lieu dans le domaine source est bien répercutée dans le domaine cible.

6.8.4.5Traduction de la sécurité en mode supprimer

Cette étape a pour but de supprimer tous les SID du domaine source dans les ACLS et ne peut être effectuée qu'après la désactivation des comptes sources correspondants. Cela s'apparente à un nettoyage administratif. Il faut bien entendu avoir procédé à la

migration de tous les comptes d'utilisateurs au risque de voir les utilisateurs non migrés dans l'incapacité d'accéder aux ressources traduites.

On sélectionnera les ordinateurs possédant les ressources à traduire en incluant les fichiers, les dossiers partagés, les imprimantes, les groupes locaux …

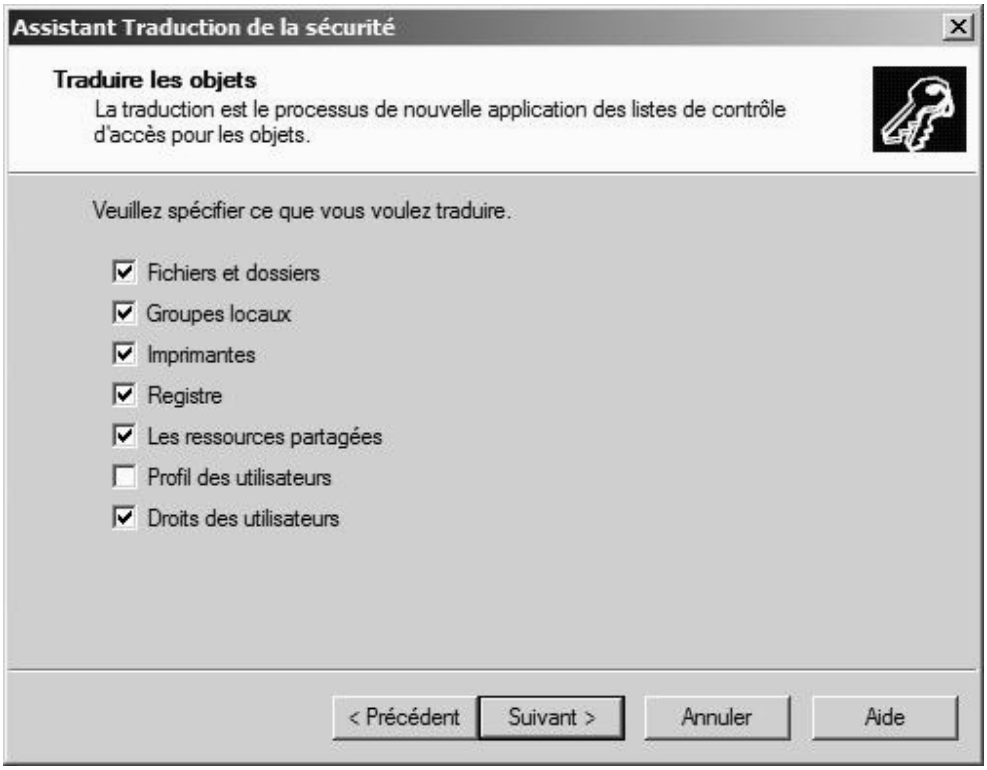


Figure 70 : Assistant 2 ADMT traduction de la sécurité

6.9 Migrations des ressources serveurs

Les comptes de services des stations membres ayant été migrés, il reste à traiter les serveurs membres eux même, ainsi que les contrôleurs de domaine.

Au terme de cette dernière étape, le domaine source peut être mis hors service.

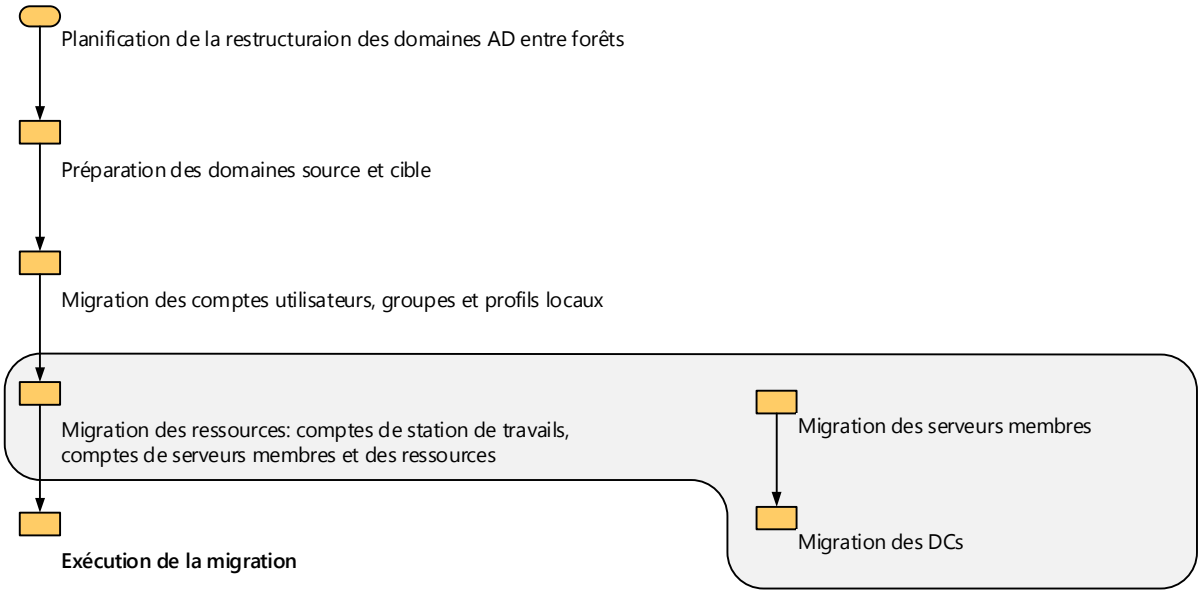


Figure 71 : matrice de migration des serveurs membres et DCs

6.9.1 Migration des serveurs membres

La procédure à suivre est la même que pour la migration des stations de travail. Il faut tout de même tenir compte du fait que la migration de ces machines nécessitera un redémarrage. Le moment pour effectuer ces opérations doit donc être bien choisit.

6.9.2 Migration des DCs

Il n'est pas possible de migrer directement un DC d'un domaine source vers un domaine cible. Il faut supprimer le service ADDS du DC et le migrer en tant que serveur membre. Une fois migré, ADDS peut être réinstallé sur le serveur.

6.10 Exécution de la migration

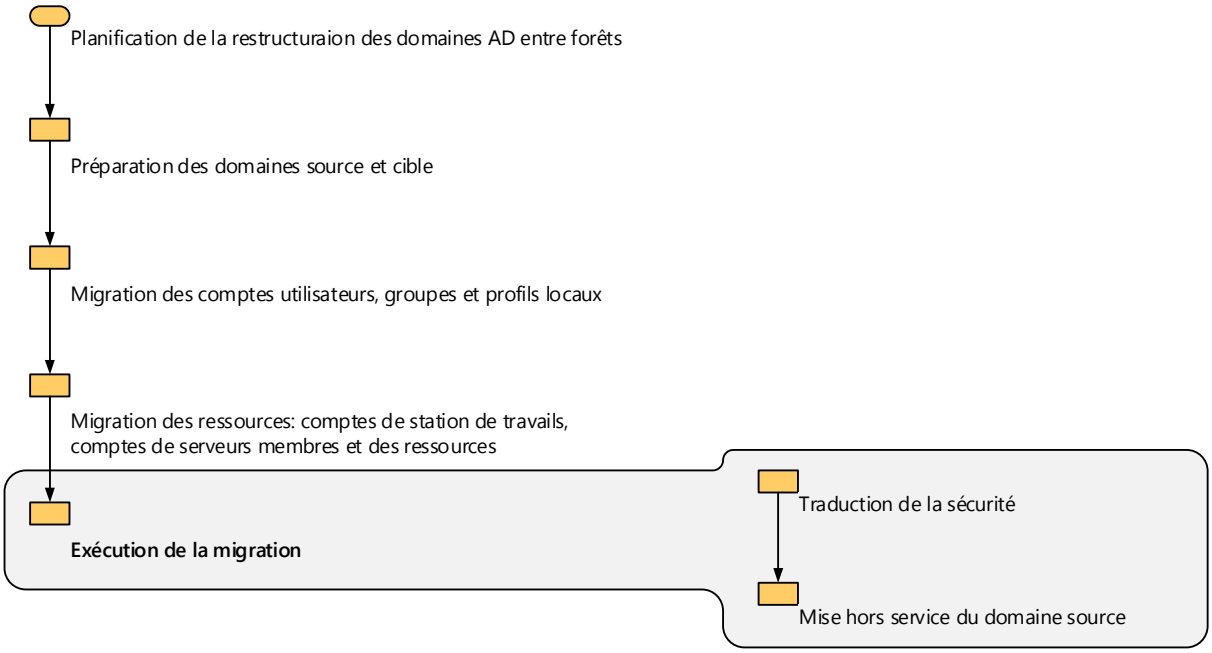


Figure 72 : matrice d'exécution de la migration

6.10.1 Traduction de la sécurité

Cette étape de « toilettage » consiste à nettoyer les ACLs sur les serveurs membres en supprimant les SID correspondants au domaine source.

On sélectionnera la traduction en mode *remplacer* de toutes les ressources hormis les profils des utilisateurs qui sont traités à la main.

6.10.2 Mise hors service de domaine source

Cette ultime étape consiste à supprimer les relations d'approbations établies entre les forêts, à désactiver les comptes créés spécialement pour la migration (MigrAdmin), ainsi qu'à désinstaller PES.

7 Migration vers la suite logicielle Charlemagne

Le logiciel Aplon est abandonné au profit de la suite Charlemagne. Cette dernière permet de gérer les bases administratives pédagogiques ainsi que toute la partie comptable du groupe scolaire. Charlemagne étant déployé sur un autre établissement d'enseignement privé situé à Besançon, un rendez-vous est organisé avec le responsable SI afin d'échanger sur l'installation, notamment le déploiement RDSH, et de calibrer le futur serveur.

Cet entretien permet de dégager une configuration peu gourmande en ressources et nous autorise à envisager la virtualisation du serveur RDSH en nous appuyant sur l'architecture Hyper-V existante sans autre coût supplémentaire que l'achat de CAL (Client Access Licence) et de licences Office Pro 2013 pour chaque utilisateur du service RDS, soit 10 personnes.

7.1 Planning

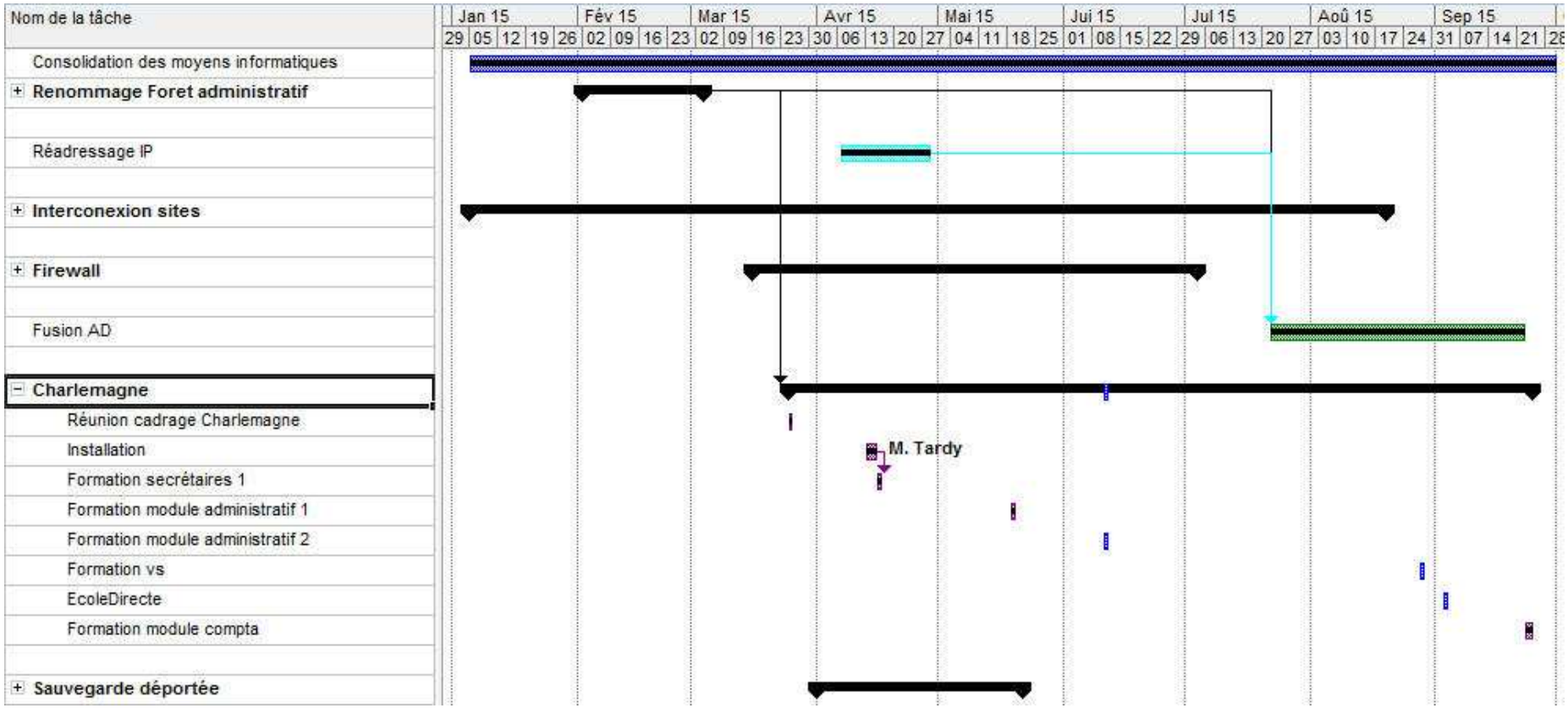


Figure 73 : planning de déploiement de la suite Charlemagne

7.2 Installation et déploiement

Ce logiciel est développé en WinDev et ne nécessite rein d'autre qu'un partage de fichier. Un client est déployé sur chaque machine afin d'accéder aux fichiers nécessaires.

Les prérequis systèmes nous permettent d'installer Charlemagne sur notre serveur de fichier administratif. L'installation du logiciel est réalisée par l'équipe STATIM qui se charge également de la migration de nos données Aplon.

7.2.1 Serveur RDSH

Cette machine virtuelle est hébergée sur un serveur Hyper-V existant avec les ressources suivantes:

Tableau 23 : configuration serveur virtuel RDSH administratif

Ressource	
Système d'exploitation	Windows server 2012
Mémoire dynamique	1024 Mo à 8192 Mo
Processeurs	4 cœurs
Espace disque	80 Go
Connectique réseau	1 carte Gigabit dédiée

Une collecte de données de performance sur l'utilisation des ressources de cette machine est lancée afin de valider les choix d'architecture. On mesure les éléments suivants :

Tableau 24 : compteurs de performances

Compteur de performance	Description
Processeur : % Processor Time	Pourcentage d'utilisation du processeur. Doit être inférieur à 85 %.
Physical Disk : Avg. Disk Queue Length	Nombre moyen de requêtes d'entrée/sortie disque en attente de traitement. Si la valeur est supérieure au nombre de disque durs + 2, cela signifie que le (s) disque (s) est un goulot d'étranglement.
Memory : Page Faults/Sec	Taux auquel le serveur lit et écrit dans la swap. Traduit le manque de mémoire. Doit être inférieur à 20.
Terminal Services Session : % Processor Time	Pourcentage de temps processeur par session.
Memory : Free Megaoctets	Mémoire libre en Mégaoctets. Doit être inférieur à 5 % de la RAM totale.
Terminal Server Services : Number of active sessions	Nombre de sessions actives sur le serveur RDSH.

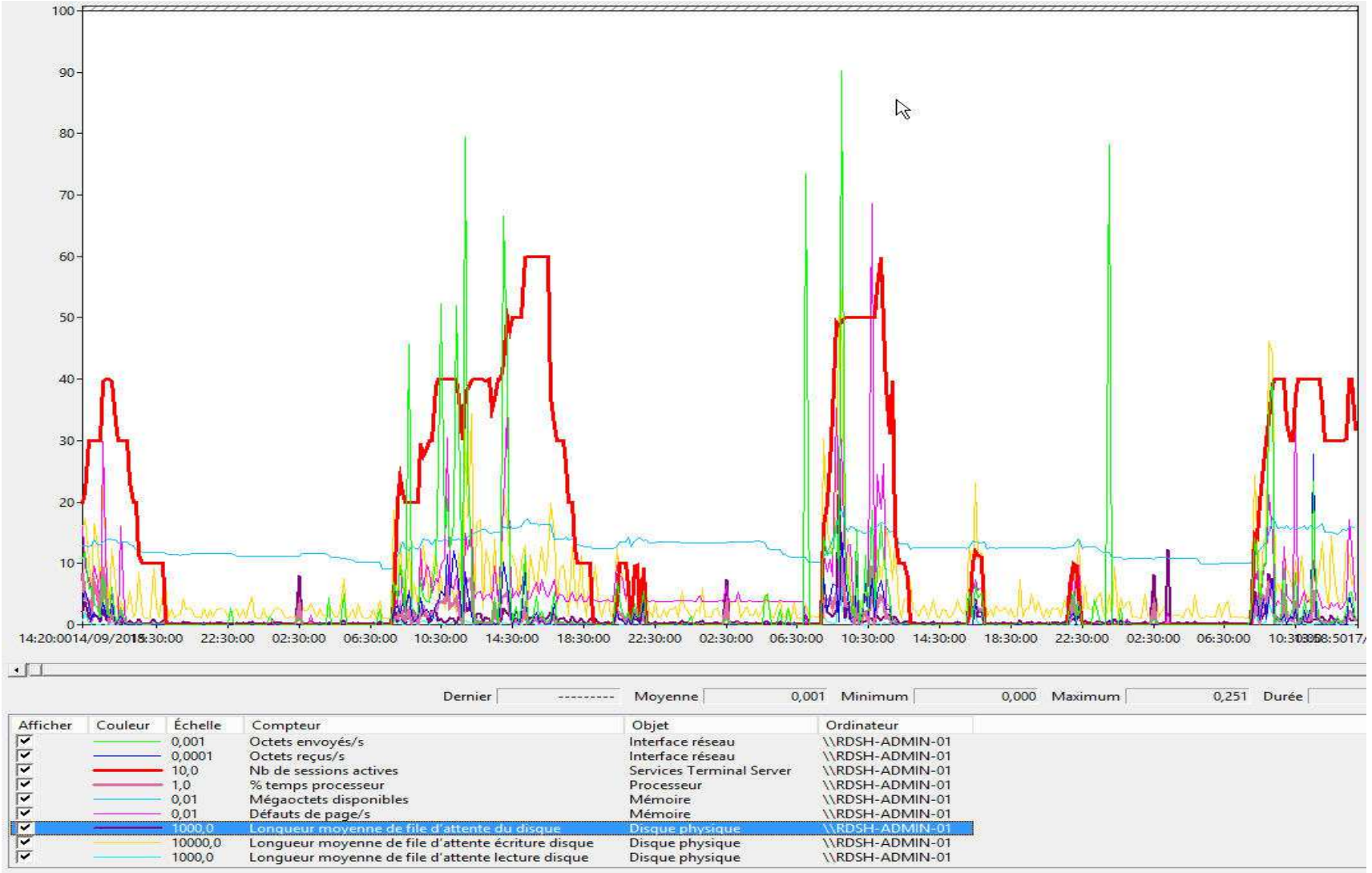


Figure 74 : collecte de données de performances RDSH-ADMIN-01

On constate que la machine est à même de supporter la charge engendrée par nos 10 utilisateurs, puisque toutes les données recueillies restent en deçà des seuils autorisés.

On réalise également une collecte de données sur le serveur Jocaste sur lequel on trouve le partage de fichiers Charlemagne afin de vérifier que la machine est à même de supporter la charge engendrée par les accès disques.

Il n'y a rien de particulier à noter, si ce n'est les pics en écriture sur le disque E : qui correspondent aux sauvegardes réalisées sur les heures non ouvrées.

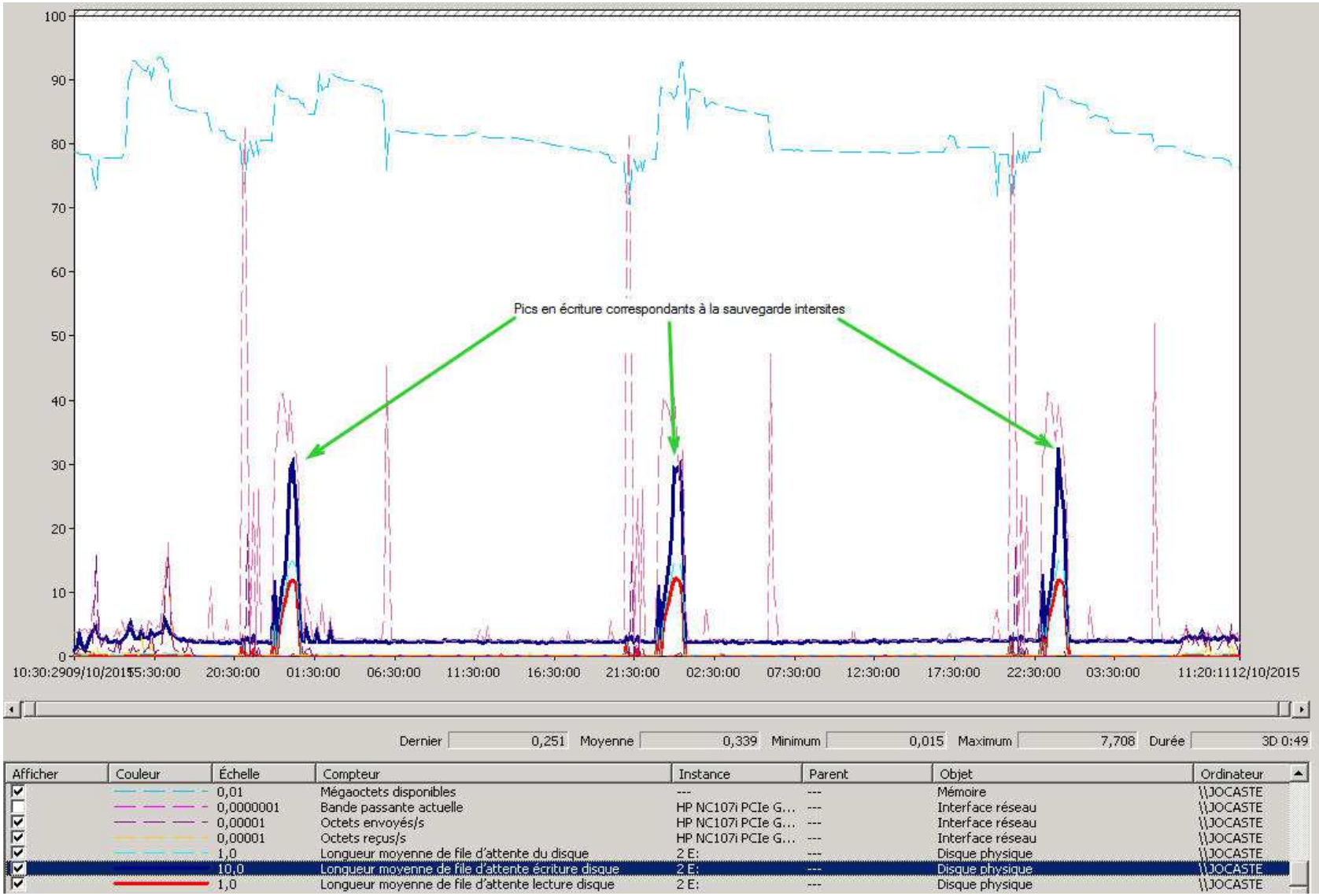


Figure 75 : collecte de données de performances Jocaste

7.3 Formation

Plusieurs modules de formation sont planifiés du mois d'avril au mois de septembre 2015 pour les personnels administratifs ainsi que pour les enseignants.

8 Réalisation de la sauvegarde des données stratégiques

Les sauvegardes des données administratives s'appuient actuellement sur le système de sauvegarde intégré à Windows Server 2008 R2 Wbadmin. Une sauvegarde quotidienne différentielle niveau bloc est déposée sur un disque dur interne dédié et nous permet de disposer d'un historique de sauvegarde annuel.

Il est demandé de pouvoir bénéficier d'une sauvegarde sécurisée quotidienne avec une durée de rétention d'une année des données stratégiques du groupe afin de disposer de ces données en cas de sinistre grave.

On demande d'étudier plusieurs solutions :

- Une solution qui s'appuiera sur l'existant pour réaliser une sauvegarde inter-sites sans autre investissement que de l'espace disque si nécessaire.
- Une solution de sauvegarde en ligne.

8.1 Planning

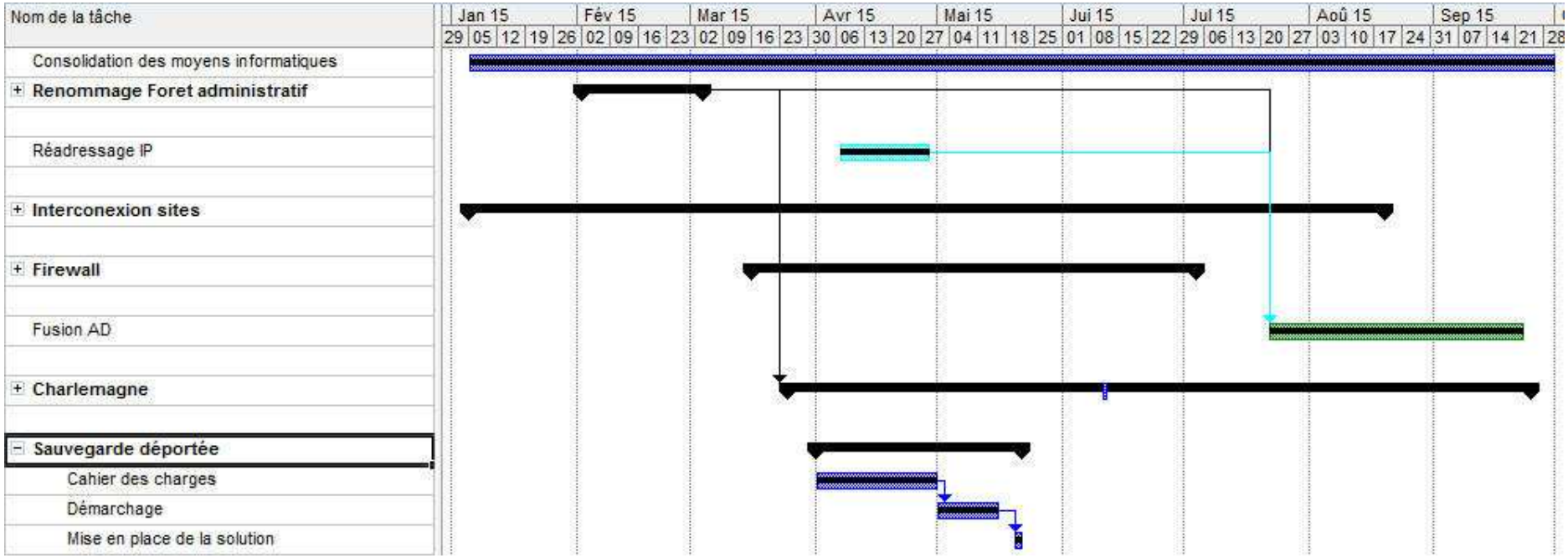


Figure 76 : planning de déploiement de la sauvegarde inter-sites

8.2 Données stratégiques et volumétrie

Il faut avant tout identifier les données stratégiques du groupe en se référant aux « métiers » exercés au sein du groupe qui doivent pouvoir établir une liste de leurs données critiques.

Au regard de ces données on établira le volume des sauvegardes à réaliser.

8.2.1 Estimation du volume des données à sauvegarder

Tableau 25 : estimation des volumes à sauvegarder

Désignation des données	Volume estimé
Charlemagne pour environ 1200 élèves	Entre 1 et 2 Go (données développeurs)
UDT	385 Mo
Gesawin	370 Mo
Total brut	**Entre 2 Go et 3 Go**

Il faudra bien entendu surveiller l'évolution du volume de ces données, de le maitriser en prenant soin de sensibiliser les utilisateurs de ce fait. Il est par exemple inutile d'importer des photos d'élèves en haute définition, et le réflexe doit être pris de traiter ces clichés avant import afin d'en réduire la taille sans nuire à leur qualité.

8.3 Sauvegarde inter-sites

La sauvegarde actuelle n'est accessible que par le biais de l'outil de sauvegarde/restauration intégré à Windows. On effectuera donc une sauvegarde quotidienne spécifique que l'on placera sur un autre site du groupe.

On s'appuie sur l'existant et l'on propose une solution sans autre achat éventuel que de l'espace disque.

Actuellement déployé sur la forêt stpaul.org, le système de sauvegarde SCDPM Microsoft permet d'effectuer la sauvegarde d'un dossier ou d'une machine située dans

une forêt liée par une relation d'approbation bidirectionnelle. Hors pour des raisons de sécurité nous avons choisi de n'établir qu'une relation unidirectionnelle entrante vers la forêt admin.priv. SCDPM ne peut donc pas être utilisé pour effectuer directement cette tâche. De plus, ce service étant situé sur le même site géographique que l'administratif, nous ne répondons que partiellement à la demande initiale.

Un système de type DFS ne passant pas non plus la « barrière » de la relation d'approbation AD, nous nous orientons donc vers la synchronisation d'une sauvegarde locale spécifique avec un dossier distant selon une rotation à définir. Cette sauvegarde sera déclenchée par une tâche planifiée et s'appuiera sur Robocopy pour la synchronisation entre le dossier local et un dossier DFS situé sur le site St Paul dans le domaine pédagogique lui-même synchronisé avec un dossier DFS situé sur le site St Joseph. On bénéficie ainsi de la synchronisation niveau bloc du système de réplication DFSR économisant de faite la bande passante du VPN. Une fois la synchronisation effectuée, une sauvegarde Wbadmin est réalisée sur le site St Joseph.

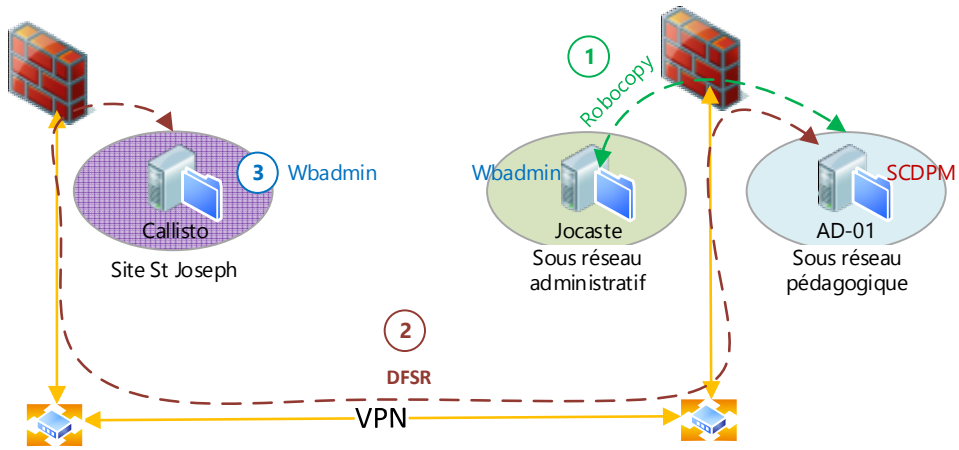


Figure 77 : schéma du système de sauvegarde inter-sites

8.3.1 Compression et sécurité des données

Les données à sauvegarder sont compressées au sein d'une archive avant transfert afin de minimiser l'utilisation de la bande passante. On utilise 7zip afin de réaliser ces

opérations. Cette application sous licence GNU LGPL permet dans son format 7z d'atteindre des taux de compression de l'ordre de 30 à 70 % meilleurs que ceux obtenus avec le format zip selon le développeur de l'application. Ces résultats sont bien entendu fonctions de la nature de ce qui est archivé et compressé.

Tableau 26 : taux de compression des données

Dossier à sauvegarder	Taille avant compression	Taille après compression	Taux de compression
Charlemagne	1 370 Mo	735 Mo	53%
UDT	385 Mo	116 Mo	70 %
Gesawin	370 Mo	65 Mo	83 %
Total	**2 125 Mo**	**916 Mo**	

Il est à noter que le processeur sera fortement sollicité lors de la compression des données. Ci-dessous, on retrouve les mesures effectuées lors de l'exécution successive des 3 scripts de création d'archive.

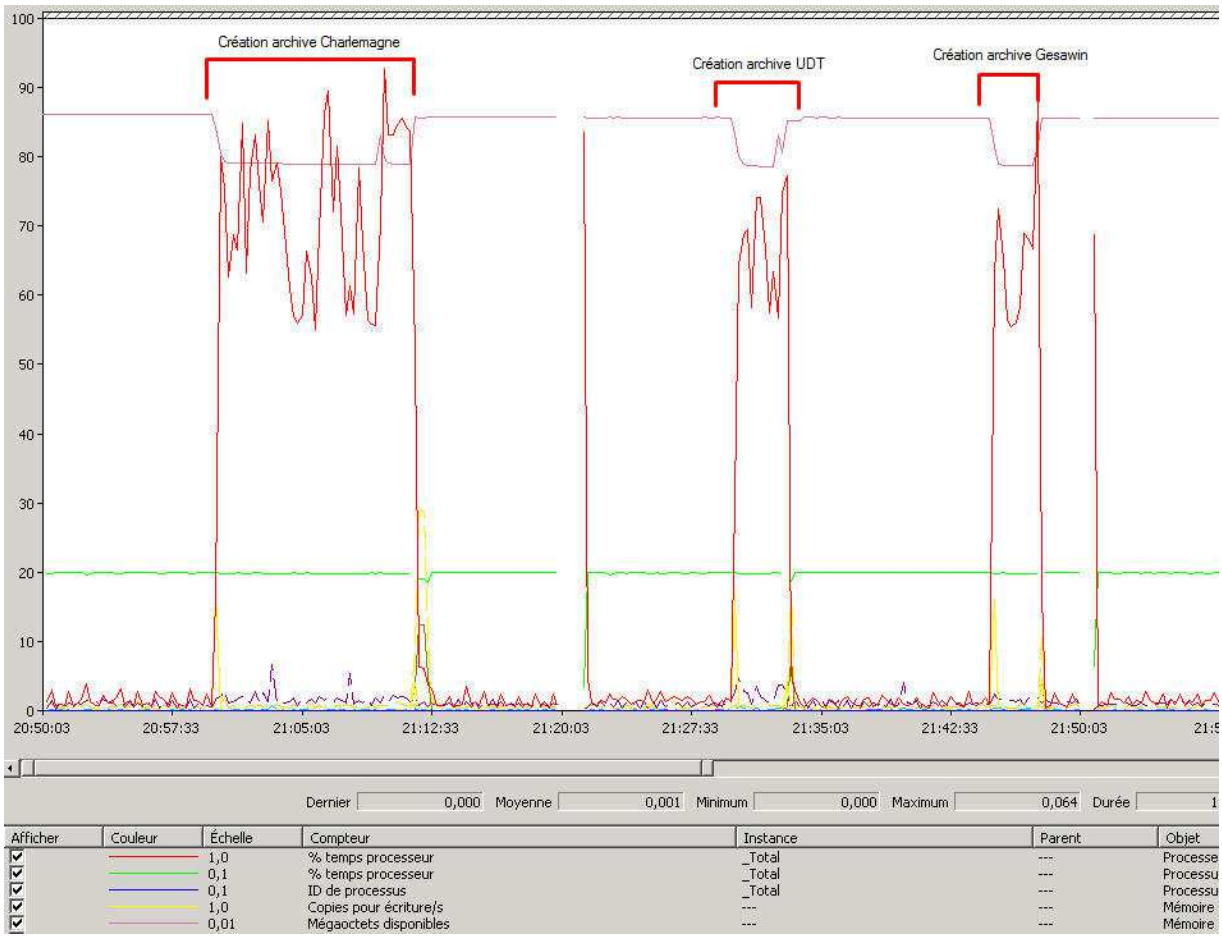


Figure 78 : Mesure du pourcentage d'occupation du processeur

Ces scripts étant déclenchés par une tâche planifiée, on veillera à choisir un créneau situé avant le début de la sauvegarde sur le serveur Callisto du site distant et ou les ressources du serveur Jocaste sont disponibles.

8.3.2 Script de sauvegarde

Le script créé l'archive dans un dossier local, et le synchronise avec un dossier distant.

On inscrit le résultat de la création de l'archive, de la synchronisation ainsi que la taille du fichier créé dans le fichier de log LogBackup.txt. La récupération de la taille de l'archive va permettre de suivre son évolution au cours du temps et d'anticiper un manque de place éventuel (cf. annexe 10.3 script de sauvegarde).

8.3.3 Evolution du volume des sauvegardes

Les données récoltées lors de chaque sauvegarde, nous permettent de calculer le taux de variation entre deux valeurs avec la formule suivante :

Taux de variation entre deux valeurs = [(valeur 2 – valeur 1)/valeur 1]*100

Bien que très empiriques, ces données vont nous permettre d'évaluer approximativement les volumes de sauvegarde et de prédire leur évolution. En effet, l'augmentation des volumes de données n'est pas linéaire, mais soumise aux réalités du terrain. Par exemple, en période de vacances scolaires, les données n'évoluent pratiquement pas. Par contre, on comprend aisément qu'en période ouvrée les modifications, les inscriptions sont légions dans les secrétariats avec un pic en période de rentrée. Les résultats suivants sont donc donnés à titre indicatifs et doivent faire l'objet d'une surveillance au fil du temps.

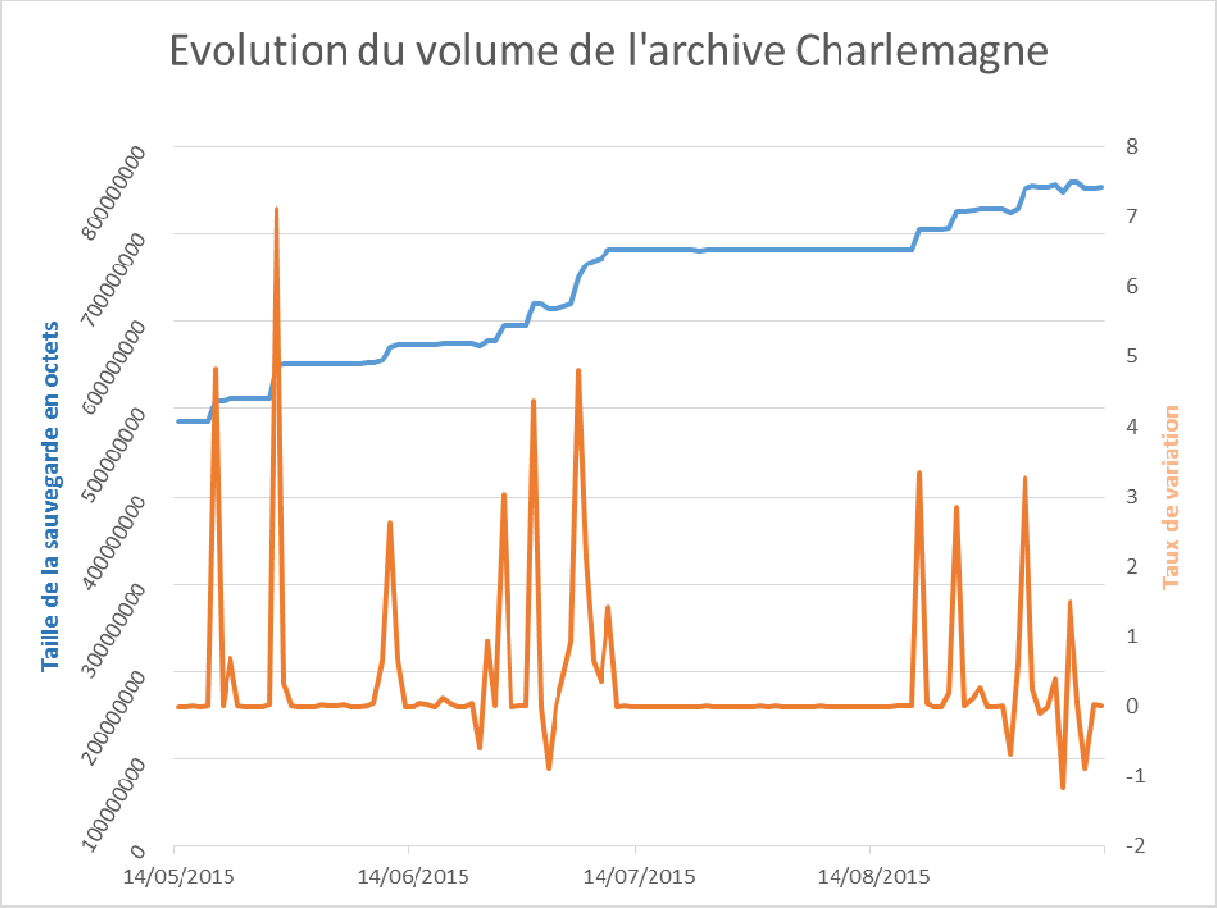


Figure 79 : graphique d'évolution du volume de l'archive Charlemagne

On en déduit un taux de variation moyen de 0.36 %. En partant de la taille de la dernière sauvegarde Charlemagne, on peut dire que l'archive augmente quotidiennement de 2 à 3 Mo et qu'au bout d'un mois la sauvegarde aura augmenté d'environ 86 Mo.

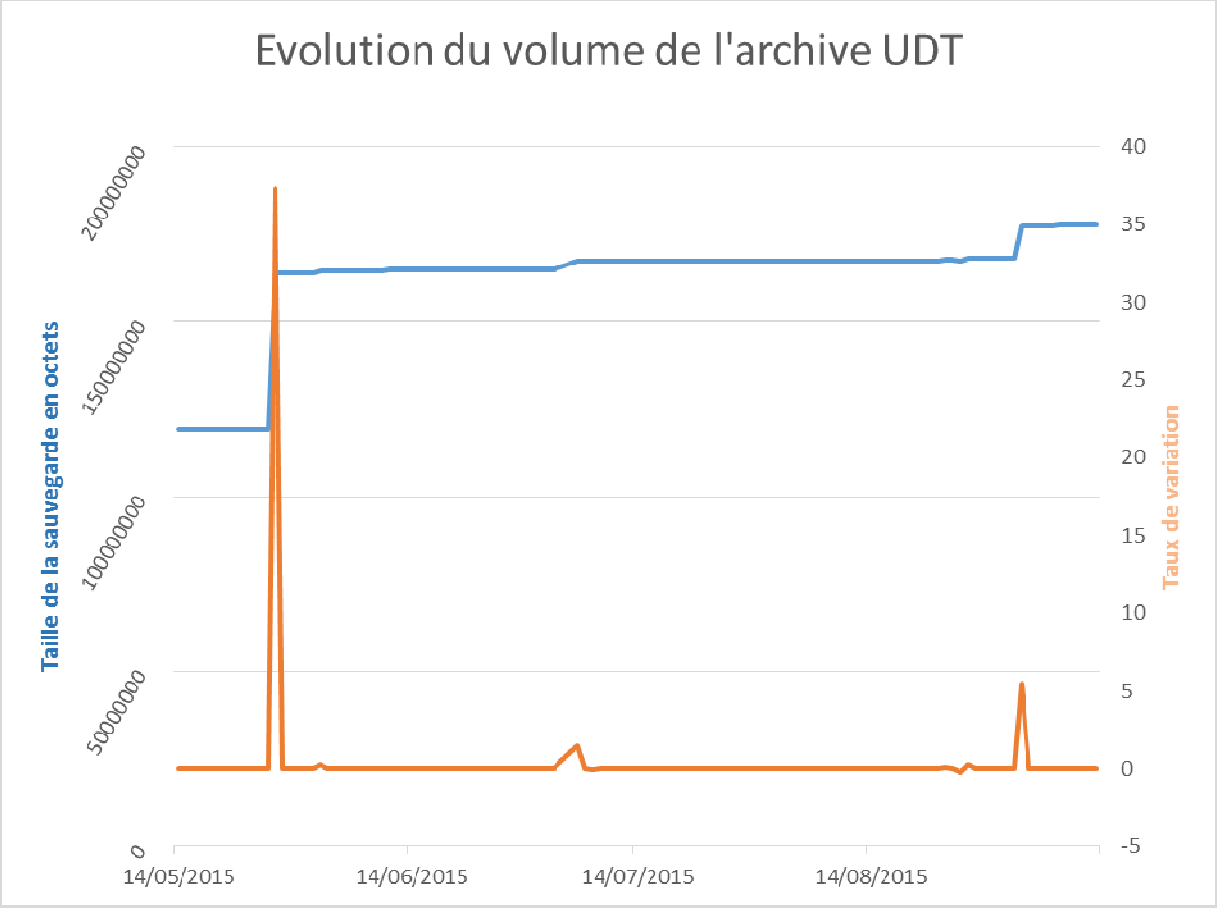


Figure 80 : graphique d'évolution du volume de l'archive UDT

On en déduit un taux de variation moyen de 0.22 %. En partant de la dernière valeur de la sauvegarde UDT, on peut dire que l'archive augmente quotidiennement d'environ 700 Ko et qu'au bout d'un mois la sauvegarde aura augmenté d'environ 20 Mo.

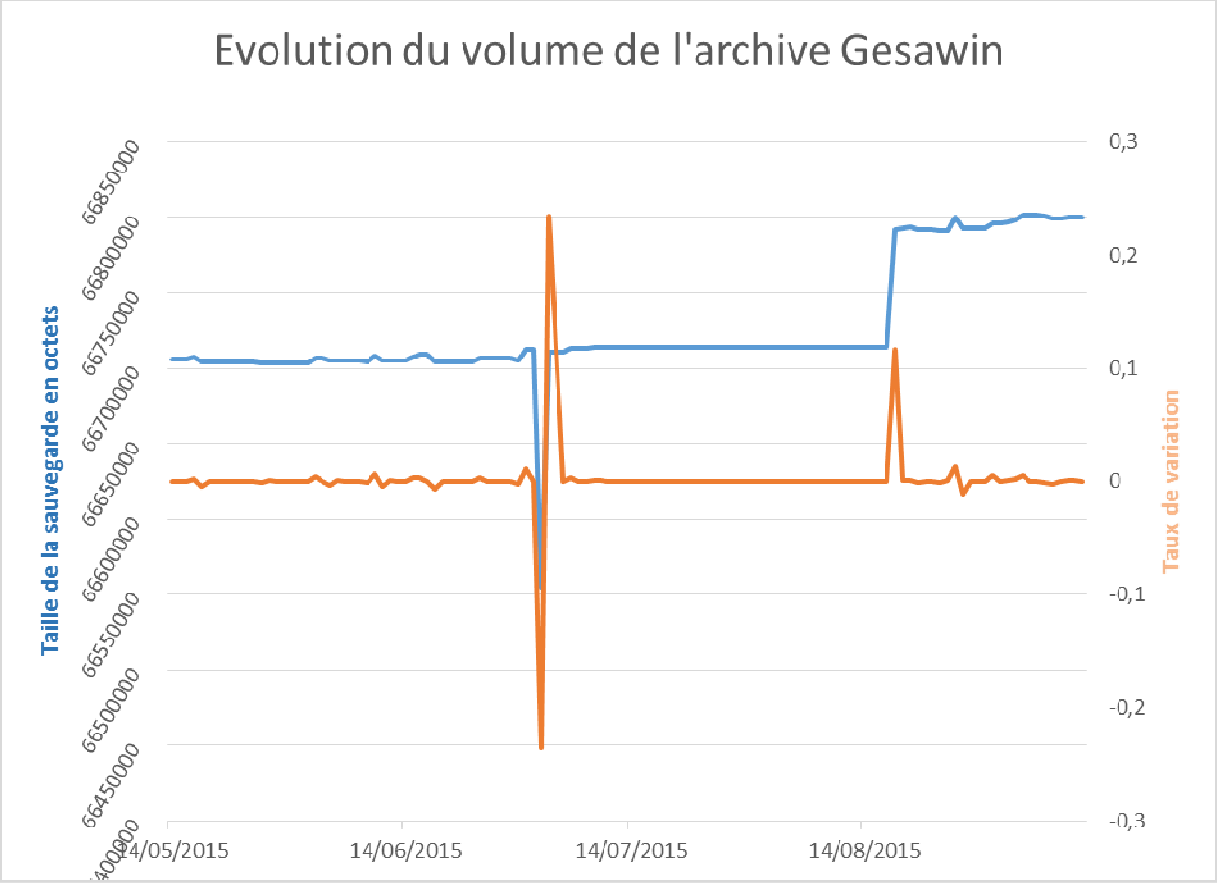


Figure 81 : graphique d'évolution du volume de l'archive Gesawin

On en déduit un taux de variation moyen de 0.0042 %. En partant de la dernière valeur de la sauvegarde Gesawin, on peut dire que l'archive augmente quotidiennement d'environ 250 Ko et qu'au bout d'un mois la sauvegarde aura augmenté d'environ 8 Mo.

Tableau 27 : récapitulatif des données d'augmentation des volumes de sauvegardes

Nom de l'archive	Taille de départ en octets	Taux de variation moyen	Augmentation quotidienne estimée en Mo	Augmentation mensuelle estimée en Mo
Charlemagne	752971479 o	0.36%	2.5 Mo	86 Mo
UDT	177609622	0.22 %	0.7 Mo	20 Mo
Gesawin	66800223	0.0042 %	0.25 Mo	8 Mo
Augmentations moyennes			**3.45 Mo**	**114 Mo**

8.3.4 Synchronisation DFSR

Un groupe de réplication DFSR est créé entre les machines AD-01 et Callisto permettant ainsi d'effectuer la sauvegarde sur cette dernière machine.

Nous avons à synchroniser environ 4 Mo de données sur un lien VPN à 10 Mbps. En réalisant cette opération de nuit, on peut allouer une bande passante d'à 1 Mbps sur les heures non ouvrées (19 :00 – 6 :00) et de 64 Kbps sinon, en sachant de plus qu'une fois la première synchronisation effectuée les échanges sont considérablement réduits puisque le moteur DFSR travaille au niveau bloc et non au niveau fichier.

8.3.5 Restauration de données à partir d'une sauvegarde

Les données sont récupérées en deux étapes :

- Restauration à une date t de l'archive souhaitée à partir de la sauvegarde WbAdmin réalisée sur le serveur Callisto site St Joseph.
- Décompression de la sauvegarde et récupération des données par copié/collé/remplacé.

8.4 Sauvegarde en ligne

La sauvegarde inter-sites ne répondant pas à toutes les exigences de sécurité et de récupération de données en cas de sinistre grave, une solution de stockage en ligne est proposée. Le choix étant pléthorique, il faudra rester vigilant sur certains points comme le respect des normes et certifications (ISO 27001), la redondance des stockages proposée par l'opérateur, les services associés, le SLA… Enfin il faudra évaluer au plus juste l'espace disque nécessaire au stockage de nos données critiques.

8.4.1 Estimation de la volumétrie

On s'appuie sur les résultats obtenus au chapitre *8.2.3 Evolution du volume des sauvegardes* précédemment à savoir un volume brut de départ d'environ 1 Go et une augmentation moyenne de ce volume de 3.45 Mo par jour.

Charlemagne est une application développée en WinDev. Ce langage s'appuie sur un système d'indexation de fichiers .fic en fichiers .ndx. Ces derniers fichiers peuvent être reconstruits et peuvent donc être exclus de la sauvegarde déportée.

Il faut également déterminer la fréquence des sauvegardes qui aura un impact sur les volumes de stockages. Au vu des données sauvegardées, on peut d'ores et déjà tabler sur une sauvegarde quotidienne.

8.4.2 Synchronisation ou sauvegarde des données ?

Suivant le principe de la synchronisation, le fonctionnement est le suivant :

- Si on ajoute un document dans le dossier synchronisé, il sera ajouté sur l'espace de stockage en ligne ;
- Si on modifie un document déjà présent, la version modifiée sera envoyée sur l'espace de stockage en ligne ;
- Si on supprime un élément, il sera supprimé de l'espace de stockage en ligne (**Attention** : cette suppression est irréversible et définitive).

La sauvegarde quant à elle permet de récupérer les données à différents moments selon la planification des sauvegardes et c'est bien cette fonctionnalité que l'on recherche. De plus, en mode delta bloc, seuls les blocs de données modifiés sont transmis vers l'espace de stockage, ce qui réduit considérablement le trafic réseau.

8.4.3 Confidentialité

- Hébergement sur le sol Français si possible.
- Flux sécurisés de bout en bout lors des transferts.
- Chiffrement des données en local avant transfert, clé de cryptage personnalisée.
- Stockage chiffré

8.4.4 Planification des sauvegardes

On souhaite pouvoir planifier le déclenchement de nos sauvegardes afin d'optimiser au mieux l'utilisation des ressources de nos machines.

8.4.5 Filtrage de fichiers

On ne souhaite pas par exemple sauvegarder les photos des élèves, ces données n'ayant pas de caractère stratégique pour l'entreprise. Des fonctionnalités de filtrage de type de fichiers peuvent effectuer automatiquement ce tri à l'échelle d'une arborescence de dossiers à sauvegarder.

8.4.6 Persistance des sauvegardes

Définir la persistance des sauvegardes revient à déterminer l'antériorité maximum d'un fichier au jour d'aujourd'hui. Ce point est important, car l'on souhaite disposer de sauvegardes ayant été réalisées il y a plusieurs mois voire une année.

8.4.7 Certifications de l'opérateur

L'opérateur doit être certifié ISO 27001:2013. Cette norme internationale est un gage de garantie sur le management de la sécurité de l'information au sein de l'entreprise.

8.4.8 Choix d'une solution

Comparatif des solutions Mozy by EMC et OoDrive, la solution Hubic est écartée d'emblée puisqu'elle ne propose pas de solution de sauvegarde stable et efficace (solution proposée très récemment et sujette à de nombreux problèmes cf. forum utilisateurs, pas d'exclusion de répertoire possible dans la sauvegarde, pas de sauvegarde possible lorsque les fichiers sont utilisés…).

Tableau 28 : comparatif des solutions de sauvegarde en ligne

Fonctionnalité	Mozy Pro by EMC	OoDrive AdBackup Pro	Commentaire
Sauvegarde en mode delta bloc	Oui	Oui	
Planification des sauvegardes	Programmable : quotidienne, hebdomadaire, mensuelle	Programmable : quotidienne, hebdomadaire, mensuelle	
Filtrage de fichiers	Oui	Oui	
Cryptage des données	AES 256 bits, Blowfish 448 bits par utilisateur	Possible par utilisateur AES 128 bits	
Sauvegarde fichiers ouverts (à chaud)	Oui	Oui	
Bande passante nécessaire	Paramétrable	Paramétrable	
Sécurisation des transferts de	SSL AES 128	SSL AES 128	

données			
Data center	Mondial	National, redondance entre 2 data centers	
Restauration	Logiciel client, en ligne, DVD	Logiciel client, en ligne, DVD	
Historique de sauvegarde	Jusqu'à 30 jours	Jusqu'à 999 jours	
Certification hébergement	ISO 27001:2013	ISO 27001:2013 ISAE 3402	
Support		7j/7, 24h/24	
Tarifs 5 Go/an		300 € HT	
Tarifs 10 Go/an	87,89 HT		
Tarifs 30 Go/an		660 € HT	
Tarifs 50 Go/an	175,89 € HT	900 € HT	

Mozy by EMC propose des tarifs très compétitifs. OoDrive bien que plus onéreuse est plus convaincante :

- OoDrive garantit contractuellement les données sauvegardées. En cas de non restauration, le préjudice sera estimé par notre assureur pour une indemnisation jusqu'à 3 000 000€.
- Historique des sauvegardes jusqu'à 999 jours
- Sauvegarde en mode service
- Sauvegarde offline en local
- Gestion portail web

La solution OoDrive 5Go est retenue.

8.4.9 Sauvegarde OoDrive

L'outil mis à disposition rassemble toutes les fonctionnalités attendues et permet d'appliquer lors de la sélection des données à sauvegarder des filtres de fichiers à exclure de la sauvegarde. Ainsi nous pouvons réduire de moitié la taille des sauvegardes Charlemagne en excluant les fichiers de type .ndx qui correspondent à l'indexation des fichiers .fic mis en œuvre par le langage WinDev. Lors de la restauration, il faudra cependant procéder à la réindexation des fichiers .fic restaurés à l'aide de l'outil mis à disposition par le développeur de la solution Charlemagne.

8.4.10 Récupération

La récupération des données s'effectue via l'outil AdBackuppro, via l'interface web connectée au cloud OoDrive ou encore à l'aide de l'application Recovery Tools. Une récupération de test est effectuée pour valider la solution de bout en bout.

8.5 Conclusion : solution globale de sauvegarde

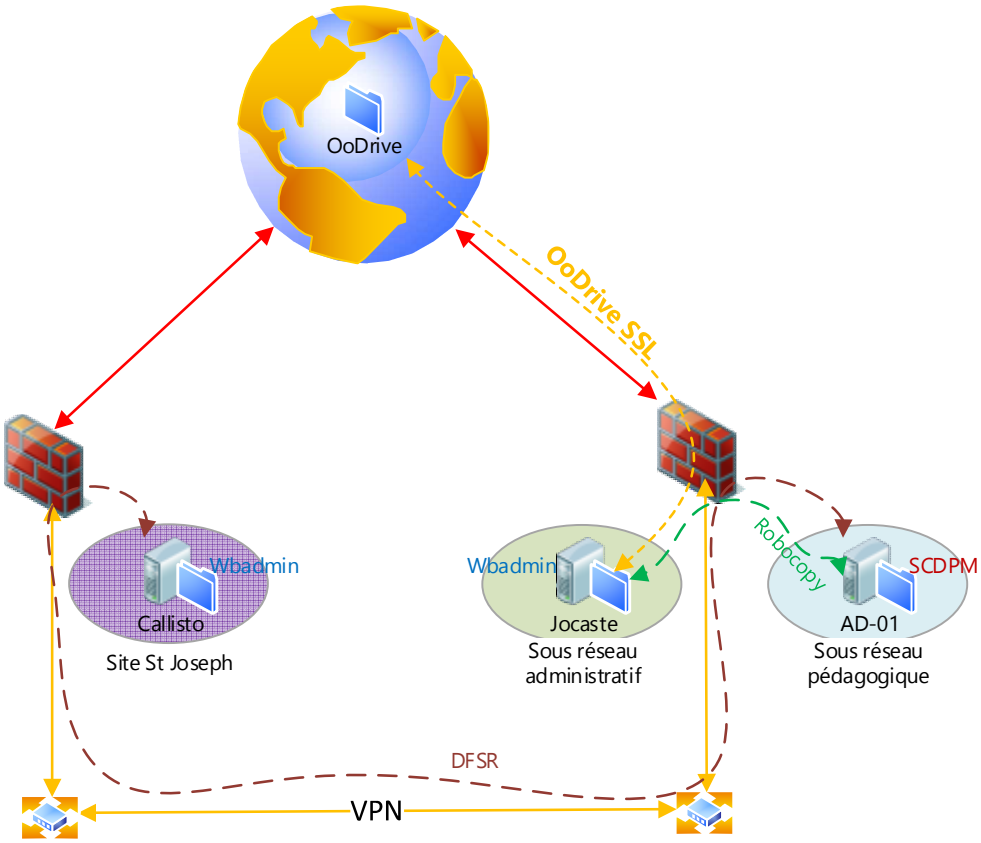


Figure 82 : Système de sauvegarde Ogec

Toutes les données administratives sont sauvegardées quotidiennement sur le serveur Jocaste avec l'outil Windows Intégré WbAdmin.

Les données stratégiques sont quant à elles sauvegardées sur un site distant par la copie d'une archive 7z sauvegardée sur le serveur Callisto avec l'outil intégré WbAdmin. Elles sont également externalisées sur l'espace de stockage OoDrive.

9 Résultats et conclusion

Le projet s'est globalement bien déroulé, le planning a pu être respecté afin de livrer début septembre un système pleinement fonctionnel répondant aux demandes exprimées par le conseil d'administration de l'OGEC.

On notera toutefois quelques difficultés rencontrées lors de la phase de déploiement de la fibre optique du lien VPN. En effet des travaux de voirie ont été nécessaires sur la zone de la copropriété. Un effondrement des gaines techniques a dû être réparé retardant de plusieurs semaines la mise en fonction du lien sur fibre optique, mais n'impactant pas le planning général puisqu'un lien cuivre temporaire avait été préalablement demandé en prévision des délais de mise en œuvre de la fibre.

9.1 Utilisation du lien VPN et dimensionnement du firewall

Les statistiques d'utilisation de la bande passante du VPN MPLS 10 Mbps du firewall site St Joseph de la *figure 81 : statistiques utilisation bande passante VPN, et consommation CPU globale du firewall sur une période d'une semaine* ci-dessous, nous permettent de constater que nos prévisions en termes de consommation de bande passante se révèlent correctes puisqu'en moyenne le besoin se situe entre 3 Mbps et 4 Mbps. On remarque également les pics attendus pendant les heures ouvrées ainsi que ceux liés à la sauvegarde inter sites.

On note en rouge les pics liés spécifiquement au flux RDS. Il s'agit principalement des éditions et impressions de documents.

Cette figure nous permet également de valider le choix du firewall. La consommation CPU moyenne se situe entre 40 % et 50 %, sachant qu'il s'agit de la ressource la plus sollicitée. La mémoire consommée plafonne à 10 %. L'espace disque permettant de stocker les logs est à 37 % du volume alloué à cet effet.

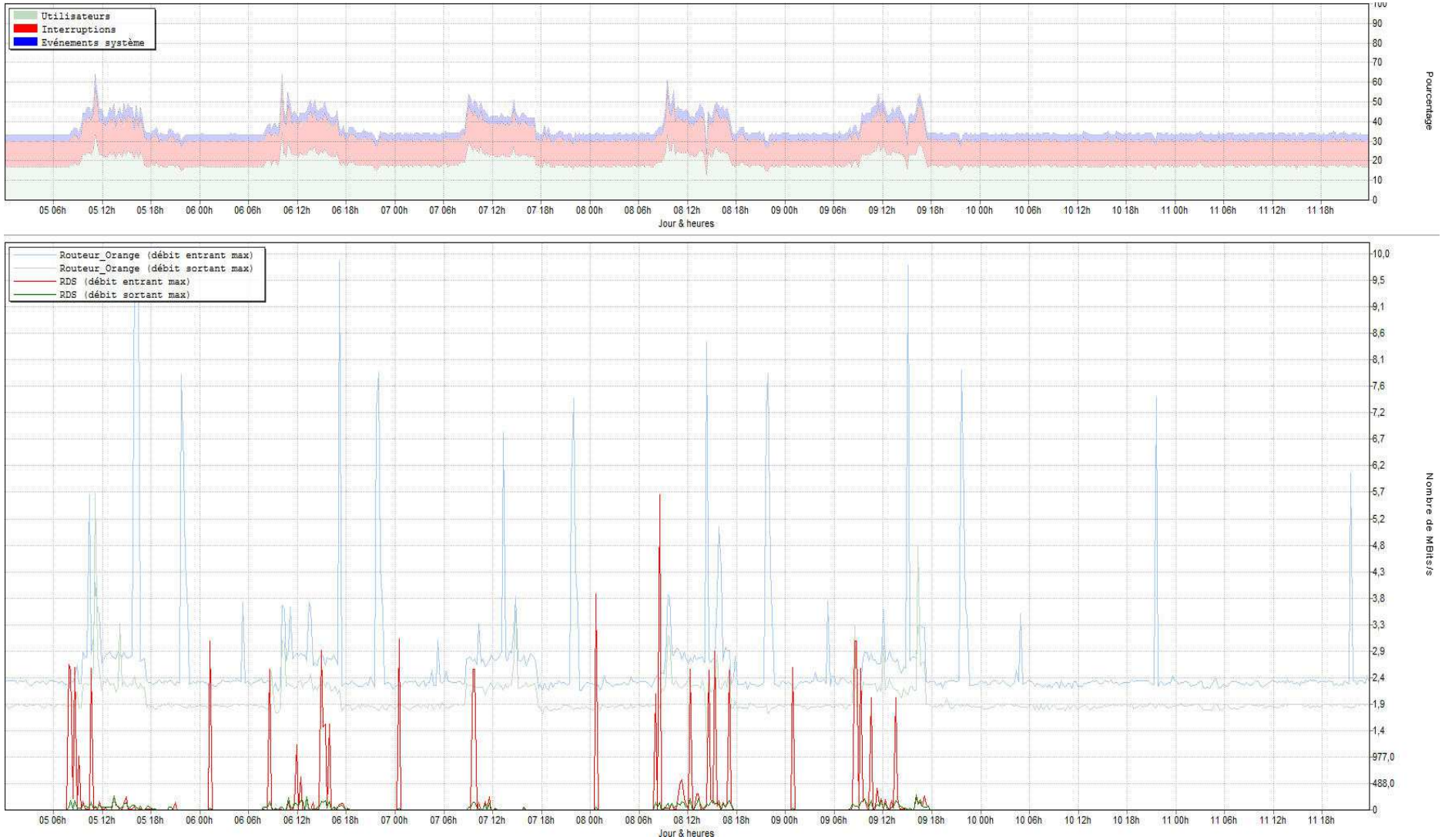


Figure 83 : statistiques utilisation bande passante VPN, et consommation CPU globale du firewall sur une période d'une semaine

9.1 Système de sauvegarde

Les volumes de données restent peu ou prou dans la fourchette estimée au chapitre *8.2.3 Evolution du volume des sauvegardes*. Après 4 mois d'utilisation, le volume occupé sur le stockage en ligne OoDrive est d'1,54 Go/5Go. La rentrée est passée, et ces valeurs ne devraient plus beaucoup évoluer dans les mois à venir.

9.2 Suite logiciel Charlemagne

La solution est aujourd'hui exploitée sans soucis particulier. Les différentes équipes (administratif, enseignants) ainsi que les parents via le portail de consultation ont totalement pris en main le logiciel. Ce déploiement a été également l'occasion de remettre à plat des pratiques et des fonctionnements anciens au bénéfice de l'entière communauté éducative.

9.3 Management du Si consolidé

Le management est aujourd'hui entièrement centralisé. Nous constatons au quotidien les améliorations apportées et leurs bénéfices. Le SI est beaucoup plus réactif et efficace. Un effet de bord est cependant à retenir. Compte tenu du caractère consolidé des stratégies en place, il est encore mal compris que toute modification dont la portée est globale, doit faire l'objet d'une concertation au niveau du groupe scolaire. L'achat, le déploiement d'un logiciel par exemple doit convenir à l'ensemble des utilisateurs et n'est plus cantonné au besoin d'un enseignement unique. Si ce dernier point n'est pas intégré, c'est l'utilité même de ce projet qui est remise en question.

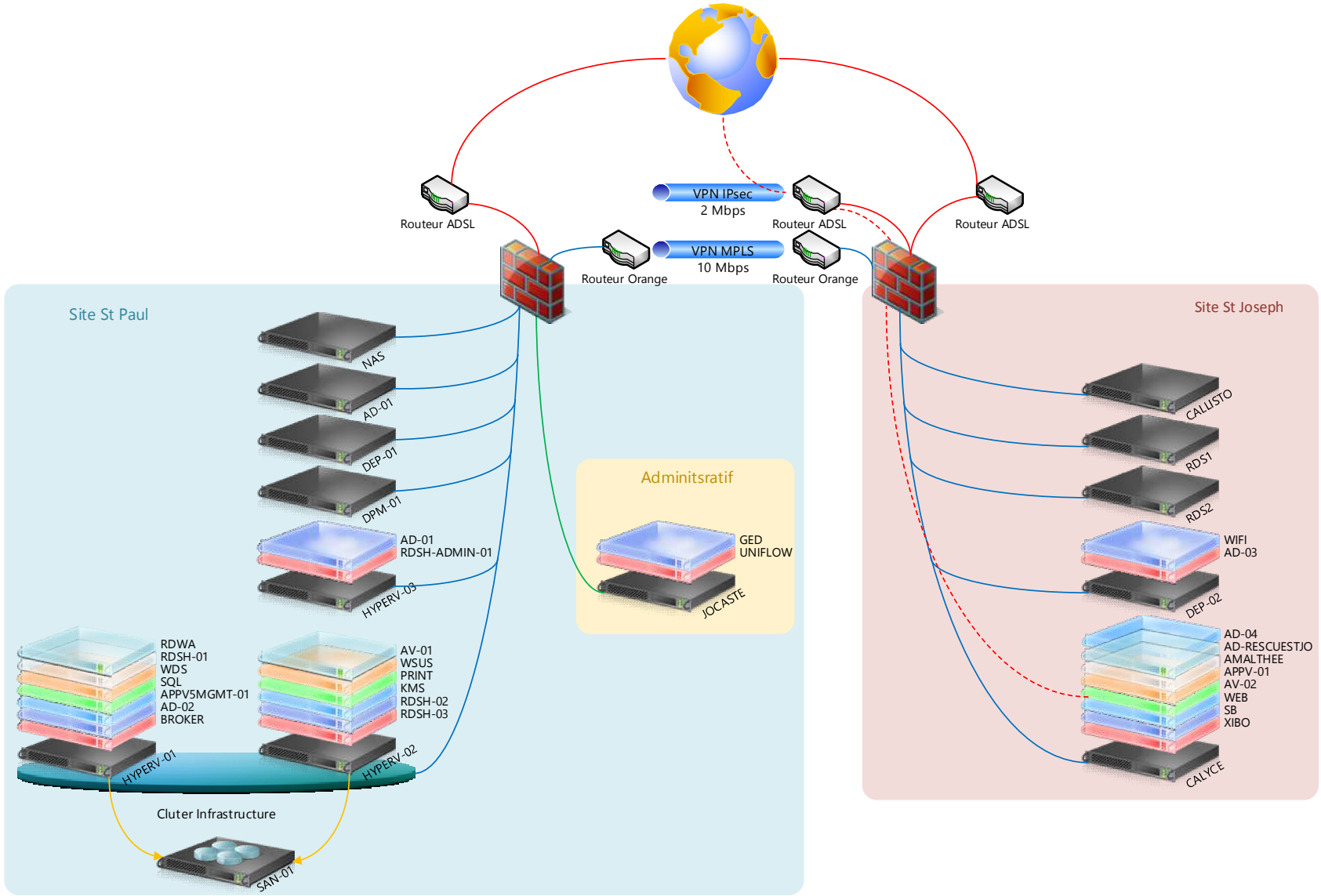


Figure 84 : architecture serveur finale

10 Annexes

10.1 Calcul du temps de téléchargement d'un profil itinérant

Sur un réseau Ethernet connecté à 1 Gbps, le temps de téléchargement d'un profil de 10 Mo est calculé ainsi :

Soit 1 Gbps = 1 000 000 000 bits/s (on est en puissance de 1000 pour les débits). Soit 1 000 000 000 / 8 / 1024 / 1024 = 119, 2092895508 Mio/s (les Méga octets Mio sont en puissance de 1024).

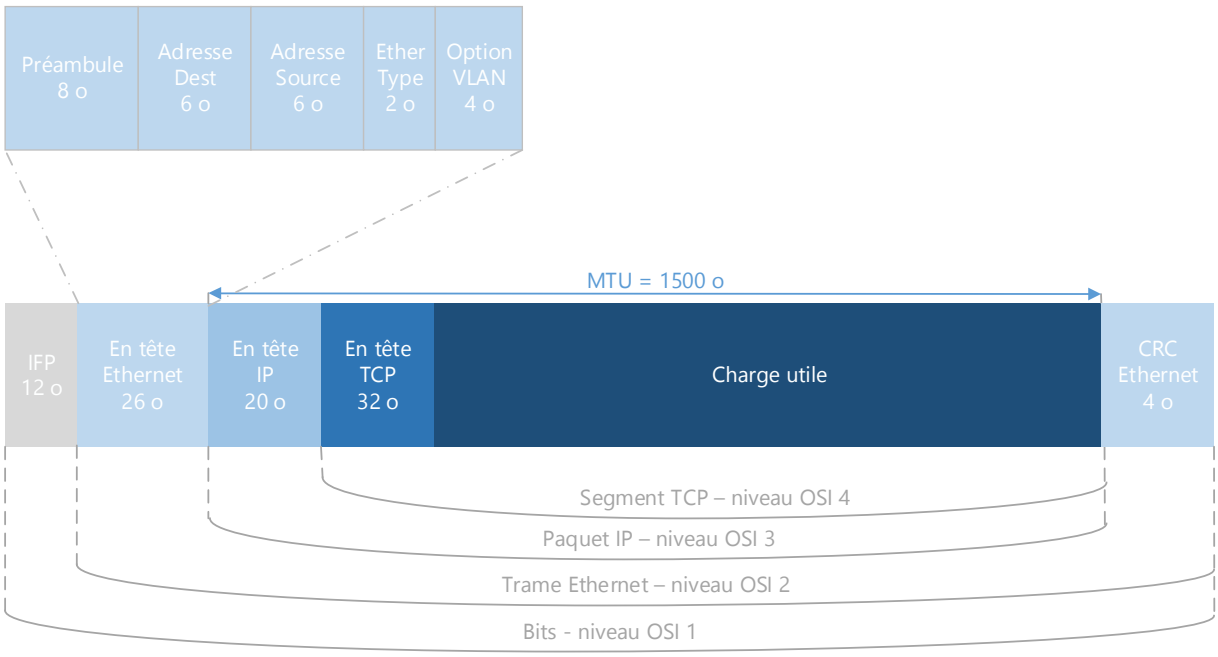


Figure 85 : imbrication des en-têtes de protocoles des différentes couches OSI

On a également un MTU (Maximum Transmit Unit, taille maximale d'un paquet IP entête comprise sur Ethernet) de 1500 octets.

Sachant que l'on ne peut transporter au maximum 1448 octets de données utilisateur en IPv4 pour 1542 octets au niveau physique, on a ratio $_{\text{Physique}\ \rightarrow\ \text{data IP}}$ = 1448/1542 = 0.9390420752.

Le ratio pour avoir simplement le débit utile IPv4 en Mio/s à partir du débit brut niveau OSI 1 en Mbps se calcul ainsi:

1 Mbps brut = 1 000 000 / (8 * 1024 * 1024 *) * ratio $_{\text{Physique → data IP}}$ = 0,1119425387 Mio/s IPv4 utile, donc le ratio $_{\text{débit IP utile Mio → débit physique Mbps}}$ = 0,1119425387. Le débit théorique d'1 Gbps physique représente donc 1 000 Mbps / ratio $_{\text{débit IP utile Mio → débit physique Mbps}}$ = 111,94 Mio/s en IPv4 charge utile (théorique car TCP n'arrive pas à utiliser 100% de la connexion sachant qu'il ne connait pas la place disponible de par son mécanisme de fenêtrage, mais il s'en approche fortement, au prix de quelques retransmissions).

Il faut donc 10 Mo / 111,94 Mio/s = 0.089 s pour télécharger un profil de 10 Mo, soit de l'ordre de la seconde sur un réseau haut débit de 1 Gbps.

10.2 Transfert des instructions et monitoring du processus de renommage

La commande *Rendom /upload* permet de créer et de transférer à un DC un script contenant les séquences de modifications nécessaires afin de traduire les changements spécifiés dans un fichier de structure cible.

Ce script contient des instructions auxquelles se réfèrent les DC lorsqu'ils reçoivent des commandes de mise à jour de la part de *rendom*. On retrouve dans ce script 3 composantes :

- Test : opération en lecture seule sur la partition de domaine du DC qui comprennent la vérification des relations d'approbations post renommage nécessaires, des pré publications des SPNs, la vérification des conflits de nommage éventuels dus à des modifications ayant eu lieu après la création du script de renommage.
- Action : les instructions de mises à jour à effectuer sur la partition de domaine
- Une signature cryptographique afin de prouver que le script a bien été généré par *rendom*.

Rendom /upload déclenche le processus de traduction et de génération ainsi que la création du fichier d'état DCList.XML.

Au fur et à mesure de l'avancée du processus de renommage, le fichier est mis à jour pour refléter l'état de chaque DC permettant ainsi de monitorer l'avancement des opérations. Ce fichier d'état permet d'enregistrer 4 états différents pour les DCs :

- Initial : état de départ de chaque DC
- Prepared : état atteint par un DC lorsque les données de renommage transmises par Renom ont été vérifiées
- Final : soit Done, ce qui signifie que le processus est terminé pour le DC, soit Error. Ce dernier état indique que des erreurs irrécupérables ont été détectées au cours du processus et que le DC en question ne peut être renommé.

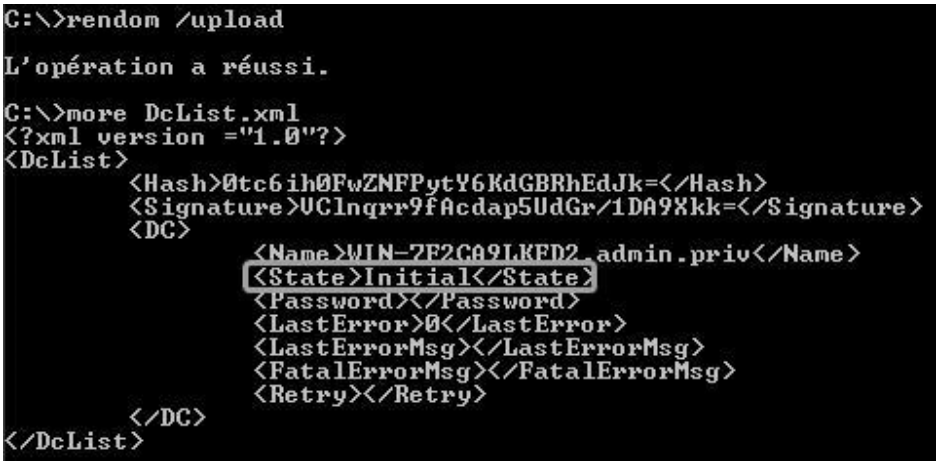


Figure 86 : commande *rendom /upload*

En sus des données d'état, le fichier contient des données des dernières erreurs rencontrées par les DCs au cours du processus de renommage.

Le script contenant les séquences de modifications de l'AD est uploadé dans la partition de configuration du DC qui possède le FSMO de maître d'attribution des noms pour la forêt, et plus précisément dans l'attribut msDS-UpdateScript de l'objet Partition de configuration cn=partitions,cn=configuration,dc=ForestRootDomain. De même, l'attribut msDS-DnsRootAlias des objets de références croisées (permet à chaque DC de connaître les partions des autres domaines de la forêt) de chaque domaine devant être renommé est rempli avec son futur nom DNS.

Ces attributs sont ensuite répliqués vers les partitions de configurations des autres DC de la forêt. Lorsque les différents DCs reçoivent les mises à jour de la partition de configuration, l'attribut msDS-DnsRootAlias déclenche la série d'opérations suivante sur les DCs :

- Pré publication des enregistrements SRV supplémentaires : Création d'enregistrements SRV DNS supplémentaires afin de prendre en compte le nouvel alias de nom de domaine.
- Pré publication des CNAME de réplication supplémentaires : Ces enregistrements DNS sont utilisés par les DCs afin de localiser leurs partenaires de réplication ADDS : <DsaGuid>._msdcs.<DnsForestName>.

  Un DC a besoin de connaitre le DsaGuid de l'objet DSA (Directory System Agent) d'un autre DC pour créer des objets de réplication NTDS, il est donc essentiel que ces données soient également pré publiées. Si elles ne l'étaient pas, la réplication s'appuierait sur des données de pré renommage obsolètes et ne pourrait aboutir, à moins d'une intervention manuelle pour mettre à jour les CNAME. On retrouve toutes ces modifications dans le fichier DNSRecords.txt créé en même temps que le fichier DcList.xml au lancement de la commande *rendom /upload*.
- Pré publication des SPNs supplémentaires : Les SPNs (Service Principal Name) sont entre autres choses utilisés par le système d'authentification mutuelle qui a lieu lors de la réplication entre deux DCs. Ainsi chaque DC dispose d'un attribut servicePrincipalName enregistré dans l'objet Computer de la partition de domaine contenant un jeu de SPNs. Des SPNs supplémentaires sont donc créés afin de ne pas interrompre la réplication ADDS. A ce stade, le fichier d'état est créé et tous les DCs sont dans l'état Initial. Il est possible de forcer les opérations de réplication entre le DC possédant le FSMO de maître d'attribution des noms et les DC de la forêt à partir de la console Sites et services AD.

10.3 Script de sauvegarde

```
- @echo off
- REM Compression d'un dossier
-
- REM Nom de la sauvegarde
- set Name=%1
- REM Taille de la sauvegarde
- REM Répertoire Source
- set dir_source=E:\DATA\%Name%
- REM Répertoire de destination local
- set dir_dest_local=E:\DATA\Backups
- REM Répertoire de destination distant
- set dir_dest_distant=\\AD-01.stpaul.org\Backup$\Backup
- REM Répertoire de log
- set LogLocation=E:\DATA\Backups
- REM Chemin de l'archive
- set FilePath=%dir_dest_local%\%Name%.7z
- REM Nombre de jours de grace (TTL)
- set dtr=1
- REM reglage de la date
- set date_today=%date:~6,4%%date:~3,2%%date:~0,2%
- REM initialisation des variables pour la gestion des dates
- REM Le fichier num.txt permet de gérer la persistance des
  sauvegardes
- REM Il se trouve dans le répertoire à sauvegarder et est
  initialisé à 0
```

```
- set /p num= < %dir_source%\num.txt
- set /a num_today=(%num%)+1
- echo %num_today% > %dir_source%\num.txt
- set /a num_dtr=%num_today%-%dtr%
- REM Chemin de 7z
- set path_7z=C:\"Program Files (x86)"\7-Zip\7z.exe
-
- REM Compression de l'archive au format 7z en utilisant la methode LZMA2 multithreaded avec un taux de compression maximal x9
- %path_7z% a -t7z -m0=LZMA2 -mmt=on -mx9 %dir_dest_local%\%Name%.7z %dir_source%
- echo Création de l'archive %Name% terminee le %date% a %time% >> %LogLocation%\logBackup.txt
-
- REM echo Suppression des sauvegardes plus vielles de %dtr% jours
- REM erase /Q %dir_dest_local%\%Name%*-N%num_dtr%.7z
-
- echo sauvegarde de %dir_source% vers %dir_dest%
- robocopy /MIR %dir_dest_local% %dir_dest_distant%
- echo Copie de l'archive %Name% terminee le %date% a %time% >> %LogLocation%\logBackup.txt
-
- echo Sauvegarde de %Name% terminee le %date% a %time% >> %LogLocation%\logBackup.txt
```

```
-
-  for %%a in (%FilePath%) do (set FileSize=%%~za)
-  echo  Taille  de  la  sauvegarde  de  %Name%  :  %FileSize%
   octets>> %LogLocation%\logBackup.txt
-  REM Enregistrement taille archive pour suivi evolution
-  echo                  %date%;%FileSize%                  >>
   %LogLocation%\EvolutionTaille%Name%.txt
-
-  echo ---------- >> %LogLocation%\logBackup.txt
```

Script de sauvegarde avec compression et synchronisation de dossier

11 Bibliographie

APREA J-F, 2011. *Configuration d'une infrastructure Active Directory [2ième édition]*.ENI, St Herblain, 829p.

ANDERSON C, GRIFFIN K, 2010. *Windows Server 2008 R2 Remote Desktop Services Resource Kit*. MICROSOFT PRESS, Redmond, 689p.

12 Liste des figures

13 Liste des tableaux

Résumé : Rationalisation des ressources informatiques d'un groupe scolaire en constituant un réseau IP étendu sécurisé au travers de la construction d'un lien VPN, puis en renommant et en fusionnant les entités de gestion Active Directory en place. Utilisation de ce lien inter-sites pour la relocalisation et la migration de l'environnement logiciel administratif et comptable ainsi que pour la mise en place d'un système de sauvegarde inter-sites des données stratégiques de l'entreprise.

Mots-clés : VPN, MPLS, Active Directory, réplication, forêt, domaine, Unité d'Organisation, GPO, migration, sauvegarde, pare-feu.

Summary : Streamlining IT resources of private schools by providing a secure expanded IP network through the construction of a VPN link, then renaming and merging Active Directory management entities in place. Use of this inter-sites link for the relocation and the migration of the administrative and accounting software environment and for the establishment of an inter-sites backup system of the company's critical data.

Keywords : VPN, MPLS, Active Directory, replication, forest, domain, Organizational Units, GPO, migration, backup, firewall.