Cah. Techn. Inra 2007, 61, pp 37-46

Construction d'un système informatique centralisé dans une unité Inra

Georges Pfeiffer[1], Nicolas Moitrier[2]

Résumé : *Nous présentons ici une démarche de mise en place d'un système informatique à partir de l'expérience menée dans notre unité. En partant des contraintes liées à notre environnement, nous nous proposons de formaliser la méthode qui nous a conduits à modifier notre système informatique. Le cahier des charges a défini une partie des objectifs qui ont été retenus par le conseil d'unité à savoir : la sauvegarde des données, la mise en place de dossiers partagés à accès exclusif pour chaque équipe de recherche, une sécurisation du système, une grande disponibilité, un système stable. Par ailleurs, grâce à de la formation sur le système dispensée aux agents et aux outils mis en place nous avons surmonté les contraintes existantes à savoir : l'infrastructure répartie sur deux bâtiments, l'hétérogénéité des systèmes d'exploitations, le niveau très inégal des compétences en informatique du personnel.*

Mots clés : Windows 2000/2003 serveur, Domaine Windows Active Directory, sauvegarde, sécurité, disponibilité, traçabilité, inventaire matériel/logiciel, gestion de parc informatique.

Introduction

La question informatique prend de plus en plus d'importance, ce qui contraint les unités de recherche à s'informer pour profiter des dernières technologies. Les besoins croissants de partager les données, les ressources et les outils, pour faciliter la communication entre les différents acteurs de la recherche conditionnent d'avoir un système informatique fiable et sécurisé. Ce document présente la démarche qui a été adoptée et qui peut servir de modèle aux personnes confrontées à ce type de problèmes.
Le début du processus a été initié par l'unité qui a recruté un gestionnaire de parc informatique à temps plein avec pour objectif d'unifier le système informatique des deux bâtiments. Nous avons établi un état des lieux et une enquête exprimant les besoins du personnel pour élaborer le futur système informatique (**figure 1**), tout en préservant la sécurité de la structure et la confidentialité des données. Le projet présenté a été validé par le conseil d'unité. Il est ensuite entré dans sa phase de planification et de réalisation.
La stratégie mise en place a nécessité un achat minimum de matériel avec la possibilité d'en améliorer les capacités au fur et à mesure de l'évolution du système. Le coût total du projet a été financé sur trois ans en faisant des investissements raisonnables du côté des serveurs tout en continuant à faire évoluer les postes de travail.
Ce nouveau système (**figure 2**) doit faciliter les interactions entre les équipes situées dans les deux bâtiments notamment en développant le partage des ressources ; il doit également uniformiser les outils et le matériel pour simplifier leur administration et pour minimiser leurs coûts.
Pour mener à bien ce projet, il faut créer une synergie entre les besoins des utilisateurs et les

1. Inra **P**lantes et **S**ystèmes de cultures **H**orticoles, Domaine St Paul – Site Agroparc 84914 Avignon cedex 09
☎ 04 32 72 24 78 georges.pfeiffer@avignon.inra.fr
2 nicolas.moitrier@avignon.inra.fr

contraintes de l'administrateur. Les besoins qui ont été définis par les utilisateurs lors de l'enquête préliminaire sont : la sauvegarde des données, la sécurité/fiabilité du poste de travail et le partage de fichiers. Les contraintes de l'administrateur du parc sont : la sécurité, les coûts humains et financiers, la facilité d'installation, la centralisation du système et une harmonisation des systèmes d'exploitations des postes de travail.
Le travail de l'informaticien a été de résoudre les contraintes techniques pour répondre aux demandes des utilisateurs.

Le contexte initial et stratégie d'évolution
L'unité PSH (Plantes et Systèmes de cultures Horticoles) est née, en 2001, de la fusion de deux unités situées sur deux bâtiments. La difficulté de gérer le système informatique relevait davantage de la diversité de son fonctionnement hétéroclite que de la répartition sur plusieurs bâtiments. L'absence de responsable informatique à part entière ne permettait pas de résoudre de manière globale les problèmes résultant des stratégies organisationnelles propres à chaque unité d'origine.
Ainsi la gestion de deux parcs informatiques et l'utilisation parallèle de différents systèmes d'exploitation sont pénalisantes pour une gestion efficace des problèmes. Cette difficulté de communication initiale entre les systèmes existants a favorisé la naissance d'un système commun propre à satisfaire nos attentes.
Nous avons choisi d'évoquer d'abord le matériel informatique retenu (justificatif des choix, caractéristiques et application), nous évoquerons ensuite les stratégies mises en place et enfin le mode de fonctionnement global du système.

1. Le matériel

L'essentiel des informations suivantes concernent l'acquisition et les caractéristiques techniques du serveur qui est le point central de notre dispositif.
La première étape est de sélectionner un fournisseur qui maîtrise les architectures serveurs et qui nous oriente vers le matériel qui correspond au mieux à nos besoins. Il faut privilégier un fabricant reconnu dans le monde des serveurs. La raison principale est le suivi de la gamme du matériel sur de nombreuses années. Pour des structures telles que les unités de recherche, les serveurs doivent offrir des garanties de stabilité, d'évolutions et de pérennité.
Outre le serveur il faut acheter un onduleur pour éteindre proprement les serveurs en cas de coupure prolongée du courant.

1.1 Les sections suivantes décrivent le matériel choisi

1.1.a Carte SCSI (Small Computer System Interface***)***
Cette technologie est sélectionnée pour le nombre possible de périphériques branchés sur le même contrôleur, jusqu'à 15. Une connexion SCSI est multi-sessions, elle est capable d'exécuter plusieurs requêtes lecture/écriture en parallèle, contrairement à l'IDE ATA. Le système inclus le contrôle d'erreurs sur les données. De plus, réservés aux serveurs, les disques SCSI sont plus rapides et plus fiables. Les périphériques peuvent être internes ou externes ; cette option est intéressante puisque les disques sont internes et le lecteur de sauvegarde externe.
1.1.b RAID (Redondant Array of Inexpensive Disk), que l'on traduit par « ensemble redondant de disques indépendants ». L'intérêt du RAID est d'agglomérer plusieurs disques durs pour fabriquer une entité de stockage fiable et rapide. Il existe plusieurs niveaux qui ont chacun leurs avantages et inconvénients. Le niveau de RAID ici choisi est le 5. Ce niveau

présente, comme tous les niveaux, une tolérance aux pannes élevée. Deux autres avantages offerts sont la possibilité de rajouter « facilement » de la capacité supplémentaire avec l'ajout de nouveaux disques et une grande vitesse de transferts des données.
1.1.c Double carte réseau **: I**'intérêt d'une double carte réseau est un taux de transfert multiplié par deux et la tolérance de panne.
1.1.d Double alimentation : toujours en terme de fiabilité du système, la double alimentation permet la tolérance de panne. L'une d'elle est branchée sur onduleur, l'autre sur le réseau électrique « normal ».
1.1.e Onduleur **:** l'onduleur permet aux serveurs de s'éteindre normalement en cas de coupure de courant prolongée. Il peut supporter au moins 20 minutes de coupure. Mais au bout de 5 minutes, il commence à éteindre les serveurs dans un ordre pré-établi. D'abord les moins importants, comme ceux qui gèrent la redondance. Il termine par ceux nécessaires au fonctionnement « de base », authentification, impression, partages. Cet ordre de traitement permet de « couper » d'abord les serveurs secondaires pour prolonger l'autonomie des serveurs les plus « importants ».
1.1.f La sauvegarde (matériel) : pour choisir la méthode de sauvegarde la plus appropriée, il faut avoir une idée de la quantité de données à conserver « en ligne » par les utilisateurs et du rythme des opérations. Il existe 3 manières de sauvegarder ces données : la sauvegarde totale concerne la totalité des données ; la sauvegarde différentielle concerne toutes les données modifiées depuis la dernière totale et la sauvegarde incrémentale concerne les données modifiées depuis la précédente, à défaut la dernière sauvegarde totale.
Pour évaluer la quantité de données à sauvegarder, nous avons établi un questionnaire diffusé à l'ensemble des agents de l'unité, leur demandant la quantité, ainsi que le rythme, des données qu'ils souhaitent sauvegarder. A partir de ces informations nous avons évalué la quantité de données à conserver « en ligne » et nous avons sélectionné les matériels adéquats.
Les choix du matériel et du processus de sauvegarde doivent tenir compte de tous les risques pouvant provoquer la perte des données, que ce soit sur les disques sources ou sur les supports de destination. Ces risques peuvent être nombreux et leur fréquence estimée très différente : crash disque, virus, attaque de pirate informatique, erreur système, vol, inondation, foudre...
Après avoir étudié les différents systèmes disponibles et les coûts de ces appareils, le choix s'est porté sur un lecteur de bande DLT SCSI d'une capacité de 200/400 Go. Il correspond bien sûr à la capacité actuelle des besoins exprimés, mais aussi à la prévision de leurs accroissements dans les années à venir.

1.2. Système d'exploitation

Le choix du système d'exploitation pour les serveurs fût guidé dans la mesure où l'unité possédait déjà des licences Windows 2000 serveur. Le rapport « coût d'achat de nouvelles licences / intérêt des nouveautés » n'était pas intéressant. Il n'y a en effet pas de grandes différences entre Windows 2000 et 2003 serveur. Le premier permet d'ailleurs de satisfaire complètement les exigences requises. De plus, une grande partie des postes de travail étaient déjà équipés de Windows 2000 qui est le client « poste de travail » classiquement associé à Windows 2000 serveur.
L'intérêt de l'installation en Domaine Windows Active Directory est de profiter des stratégies de groupe, de l'impression centralisée, du partage de fichiers et de remplir des exigences de sécurité nécessaires en conformité avec la charte informatique de l'Inra.

2. Mise en place des stratégies de groupe

Les stratégies de groupe sont un ensemble de paramètres centralisés sur les serveurs. Ils sont applicables aux ordinateurs ou aux utilisateurs, selon leur nature ; il représente un gain de temps considérable pour l'administrateur du réseau qui n'a plus à intervenir sur chaque machine du parc. Le nombre important de paramètres applicables demande de faire des choix opportuns propres à son domaine, c'est-à-dire réellement utiles, pour ne pas alourdir leur gestion. Surtout si l'administrateur n'est pas seul à s'occuper du domaine. Les stratégies peuvent se répartir en deux groupes (qui ne contiennent pas les mêmes paramètres) qui sont les stratégies ordinateurs et les stratégies utilisateurs. Par exemple, le premier groupe est appliqué au démarrage de l'ordinateur et le second groupe à la connexion de l'utilisateur au domaine. Celles retenues sont décrites ci-dessous.

2.1. Les stratégies utilisateurs

2.1.a La redirection du « Mes Documents ». Tous les utilisateurs ont un « Mes Documents » qui est redirigé sur les disques d'un serveur possédant un système RAID. L'accès en est exclusif. Ceci présente un avantage important pour la sauvegarde des données des utilisateurs. Pour être confortable, ce système doit fonctionner sur un réseau au minimum 100 Mbits/s commuté. L'autre avantage est que tout utilisateur peut retrouver instantanément ses données quel que soit l'ordinateur du domaine qu'il utilise. Pour cela, il faut autoriser l'utilisation des fichiers hors connexion. Ceci a pour conséquence de mettre les fichiers les plus fréquemment utilisés en mémoire cache sur le disque local de la machine de l'utilisateur. Si le serveur devient indisponible, l'utilisateur pourra toujours travailler de manière transparente sur ses fichiers. Une synchronisation sera réalisée lors de sa prochaine fermeture de session. Celle-ci peut-être forcée par l'utilisateur ou planifiée à intervalles réguliers. Pour un ordinateur portable, il est alors naturellement possible de travailler « normalement » à la maison. La synchronisation se déroule à la prochaine ouverture de session à l'Inra.

2.1.b. Attribution des imprimante**s.** Cette stratégie permet de publier automatiquement les imprimantes en fonction de la situation géographique ou/et de l'équipe à laquelle l'utilisateur appartient. Celle-ci étant défini préalablement par l'appartenance à des groupes. A la première connexion de l'utilisateur, les imprimantes s'installent sur sa machine sans aucune intervention humaine. L'administrateur n'a plus besoin d'installer individuellement les imprimantes sur chaque poste de travail. Ce déploiement se fait grâce à un script WMI générique adapté à notre environnement.

2.1.c Partage. Cette stratégie installe dans le menu « favoris » de l'exploreur de fichiers de Windows les liens vers les ressources partagées, cela peut concerner les données partagées par les membres des équipes ou bien des sites Web internes.

2.1.d Economiseur d'écran. En cas d'inactivité prolongée (ici 30 minutes), cette stratégie permet de forcer la machine cliente à mettre en fonction l'économiseur d'écran avec réactivation de la session par mot de passe. Les utilisateurs ne pensent pas toujours à fermer leur session en cas d'absence, surtout pour la pause déjeuner. L'ordinateur reste alors pleinement accessible à tout individu passant par-là, un manquement à la sécurité de l'ensemble du parc. Remarque : un délai trop court du déclenchement de l'économiseur gêne les utilisateurs et rend la démarche impopulaire, même si elle est justifiée.

2.2. Les stratégies ordinateurs

2.2.a Les mots de passe. Cette stratégie permet d'être en harmonisation avec la charte informatique de l'Inra. Les mots de passe doivent respecter des exigences de complexité : minuscules, majuscules, chiffres, caractères spéciaux, longueur minimale...

2.2.b WSUS. Installer les mises à jour officielles Microsoft de Windows et Office à l'ensemble des postes clients. Ce système permet, à travers un serveur Web local, de configurer le rapatriement sur un serveur en local et le déploiement des mises à jour. Cette stratégie assure que les mises à jour sont effectuées sur tous les postes clients. De plus ce serveur local génère un moindre trafic réseau sur l'Internet puisqu'il n'y a qu'une machine qui se connecte au serveur de Microsoft. La désactivation des mises à jour sur les postes de travail est impossible par l'utilisateur.

2.2.c OCS Inventory. Ce logiciel permet de faire l'inventaire complet des machines du domaine (matériels et logiciels) via un script exécuté au démarrage. L'exploitation des données recueillies peut se faire directement avec OCSInventory ou avec le logiciel de gestion de parc GLPI.

2.2.d Système d'authentification LAN manager (NTLM)**.** Avec Windows, il y a 3 niveaux de négociation pour l'authentification entre le client et le serveur, à choisir en fonction des systèmes d'exploitations installés sur le domaine. Les deux premiers sont historiques, ils datent de Windows 95/98 et de Windows NT. Avec les systèmes 2000/XP, le niveau d'authentification maximum est possible. Ce paramètre renforce la sécurité au niveau du domaine.

2.2.e Restrictions supplémentaires pour les connexions anonymes (anonymous logon)**.** Ce paramètre interdit les connexions anonymes au domaine, c'est-à-dire qui ne sont pas explicitement authentifié par le serveur.

2.2.f Installation de logiciels**.** OpenOffice et Java sont installés automatiquement lors du démarrage des ordinateurs, offrant un socle de logiciels de base communs à tous les utilisateurs.

2.2.g Tâches planifiées**.** Les ordinateurs doivent effectuer, à intervalles réguliers, des opérations de maintenance. Les deux retenues sont la synchronisation de l'horloge, (importante dans la mesure où il ne faut pas qu'il y est un décalage entre les serveurs et les stations de travail pour garantir le bon fonctionnement du système d'authentification Kerberos 5) et la défragmentation des disques locaux, exécutée le dimanche, sur tous les postes du domaine c'est-à-dire sur l'ensemble des machines de l'unité connectées au serveur.

3. Stratégie de sauvegarde

Une fois le matériel choisi, il reste à définir la procédure à utiliser. Le fait que le « Mes Documents » soit redirigé sur un disque unique permet de n'utiliser qu'une seule machine à sauvegarder. De ce fait, une seule licence serveur suffit, ce qui permet une économie en temps d'administration et en coût de licence. Afin d'éviter au maximum la perte de données, celles-ci sont sauvegardées quotidiennement. De plus, pour éviter une gêne aux utilisateurs, les sauvegardes sont programmées la nuit.

Pour parer aux risques décrits dans la première partie, la sauvegarde va se diviser en trois étapes, avec des rythmes différents :

- Sur bande, sur un cycle de cinq mois avec une bande par mois. En début de mois, une sauvegarde totale du système et des données utilisateurs est réalisée. En cas de « crash »

violent du serveur, une installation minimum de Windows et du logiciel de sauvegarde permet de rétablir le système dans l'état précédent le crash. Elle est suivie de cinq sauvegardes différentielles régulières, avec uniquement les données utilisateurs. Les données système évoluant peu, sauf pour les mises à jour de sécurité lourdes, une sauvegarde par mois est suffisante. La dernière sauvegarde différentielle éjecte la bande. Les bandes ainsi récupérées sont stockées dans un endroit fermé à clé.
- Régulièrement, une sauvegarde totale est réalisée, la bande est mise en sécurité dans un lieu distant, pour éviter de tout perdre par exemple en cas de feu.
- Sur disque, sur un cycle d'un mois. Une sauvegarde totale en début de mois suivi de sauvegardes différentielles journalières. Il n'y a donc pas un long historique comme la solution précédente, la sauvegarde suivante écrase tout. Les données sont très rapidement accessibles dans un espace disque équivalent en taille à celui prévu pour les données des utilisateurs.
Avec ce double système de sauvegarde on pare aux éventualités décrites plus haut. Suivant les avaries, la procédure de restauration des données n'est pas identique. Elle est rapide et simple pour les pertes de données les plus courantes, sans hypothéquer la possibilité de tout restaurer en cas de gros problème, c'est un compromis acceptable entre le coût, la facilité d'installation du système et le service rendu.

3.1. La disponibilité et la fiabilité

Le bon fonctionnement du système doit être vérifié à plusieurs niveaux. Tout d'abord, la typologie du réseau doit être commutée : « une prise, un ordinateur », pour ainsi s'assurer qu'un problème vient d'une coupure réseau ou non.
Une certaine redondance est assurée par le choix d'un matériel de type serveur. Mais pour garantir au mieux la disponibilité du système, il est important de le doubler. Ce matériel « de secours » est généralement moins puissant et en cas de « crash » violent du serveur principal, le travail continue dans des conditions proches de la normale.
Ces serveurs redondants sont aussi utilisés pour décharger les serveurs principaux de certains services dits « secondaires ». C'est-à-dire dont la non disponibilité immédiate ne porte pas préjudice à l'utilisation du système et dont la charge (mémoire, CPU, disque) est faible : serveur anti-virus, serveur WSUS (mise à jour Windows et Office), inventaire des machines, gestion du parc... La répartition des services réseaux entre les serveurs permet un rétablissement du système, en cas d'avarie grave, plus rapide. Le basculement des services réseaux d'un serveur à l'autre est plus facile.
Une fois installé, le système est stable. Cependant lors des mises à jour de sécurité il est souvent nécessaire de redémarrer le système. La fréquence généralement observée est d'une à deux fois par mois. Les logiciels que nous utilisons, notamment pour la messagerie électronique, la navigation Internet et la bureautique intègrent les mises à jour automatiques. La sécurité et la stabilité sont encore améliorées (correction de bug notamment).
Un pare-feu (firewall) est installé au niveau du centre Inra d'Avignon. Les attaques extérieures sont donc limitées. Un anti-virus centralisé est installé, déployé automatiquement sur tous les postes de travail du domaine.
L'avantage de la centralisation est d'être sûr que tous les ordinateurs en sont équipés et que les mises à jour de la base virale sont bien effectuées. Pour limiter le trafic réseau sur l'Internet, seul le serveur anti-virus va chercher les mises à jour chez l'éditeur, puis les redistribue de façon programmée à tous les postes clients.
La défragmentation du fichier d'échange et des disques est programmée pour s'exécuter (sous forme de script) automatiquement sur l'ensemble des ordinateurs du domaine. Cela accélère

les accès disques et en même temps réduit le travail des disques (déplacement de la tête de lecture).
Pour appliquer les stratégies de groupe correctement, il faut empêcher les horloges des ordinateurs d'être décalées entre elles. Une synchronisation est réalisée quotidiennement avec un serveur de temps (NTP) via un script et déployé par les stratégies de groupe.
Les mises à jour système, logiciels et anti-virus assurent une sécurité et une bonne harmonisation du système. En effet, l'utilisation de mêmes logiciels dans l'unité en favorise la maîtrise et permet de mieux solutionner les problèmes.

3.2. Traçabilité et vue centralisée du système :

L'efficacité du système peut se mesurer par la rapidité de détection des pannes. Grâce àne vue centralisée des services et des outils mis en oeuvre on intervient rapidement sur l'état défectueux d'un matériel ou d'un logiciel. Les remontées d'alertes programmables livrées avec les logiciels qui exploitent les matériels ou inclus dans les outils centralisés (anti-virus, gestion de parc...) avertissent dès qu'un problème survient. Ci-dessous une liste des principaux éléments surveillés :
- l'onduleur, avec entre autre son pourcentage de charge et le temps qui lui reste en cas de coupure de courant ;
- les disques de la baie RAID,
- l'état des systèmes et des logiciels, avec pour toutes les machines du domaine, les numéros de versions et les mises à jours effectuées ;
- l'anti-virus centralisé : l'inventaire du matériel se fait avec le logiciel libre OCS Inventory. Celui-ci permet d'inventorier l'ensemble du parc matériel et logiciel du domaine. Il peut être couplé au logiciel de gestion de parc GLPI (Gestionnaire Libre de Parc Informatique). A noter que l'inventaire est réalisé automatiquement via les stratégies de groupe de Windows. Deux possibilités sont offertes : soit l'inventaire se fait à l'allumage de l'ordinateur, soit à l'ouverture de session. La solution choisie est à la mise en route de l'ordinateur. En effet, la fréquence de renouvellement de l'inventaire étant considérée comme faible, ce choix permet une sollicitation moindre du réseau. GLPI permet l'importation des données contenues dans OCS Inventory.
GLPI permet aussi de faire de la réservation en ligne. La liste du matériel peut provenir des importations d'OCS Inventory ou en rajoutant individuellement du matériel non informatique, tel que les salles de réunion, les véhicules, les appareils photo... De plus, GLPI autorise l'alimentation d'une base de connaissance en ligne permettant aux utilisateurs de résoudre des problèmes courants.

Conclusion

La démarche employée est imprégnée du système Windows. Mais la plupart des concepts et techniques sont génériques, transposables et adaptables facilement. On aurait pu, par exemple, mettre un système Linux avec des fonctions identiques. L'idée principale est d'avoir une vision globale du système pour une mise en place progressive et qui tient compte des besoins futurs.
L'unité a ouvert un poste de gestionnaire de parc et a instauré un système informatique fiable et efficace en peu de temps. Les données sont en sécurité et le système offre une grande disponibilité, de par son faible taux de panne et par sa stabilité. Tout ceci participe à un gain de temps non négligeable pour l'administrateur et pour tous les utilisateurs.
Nous avons pu tester la montée en charge et la stabilité du système avec l'arrivée d'une équipe

de recherche qui a intégré le domaine sans difficulté et qui a profité des stratégies, des partages et de la sauvegarde en les joignant simplement au domaine.
L'automatisation du système permet de gagner un temps précieux utilisé pour faire de la veille technologique. Cette veille sert à améliorer le système existant et à anticiper les évolutions futures. Ces changements technologiques des systèmes d'exploitations depuis Windows 2000 (tant au niveau serveur que poste de travail) ne justifient pas pour l'instant une migration. Surtout si l'on considère les surcoûts des logiciels et des matériels que cela engendre. Toutefois, il apparaît nécessaire « de garder un oeil »sur les derniers systèmes (Windows Vista) pour éviter les écueils. Ceci est nécessaire par l'achat quasi obligatoire des PC dernières générations.

Liens utiles :

http://www.glpi-project.org/

http://ocsinventory.sourceforge.net/index.php?page=French

http://www.microsoft.com/france/windows/previous/server/default.asp

Cahier des charges → Les moyens matériels

✓La sécurité des données

- sauvegarde (système + données utilisateurs)
- stabilité du système (mise à jour système et logiciels)
- anti intrusion (anti-virus + mise à jour système et logiciels)

✓La fiabilité et la disponibilité

- des ordinateurs (poste de travail, serveurs de terminaux applicatifs ou calculs)
- des services réseaux (disques partagés, impression...)
- des données
- empêcher ou limiter la piraterie
- empêcher ou limiter les pannes matériels ou logicielles
- rétablir rapidement un fonctionnement normal du système quelle que soit l'avarie

✓L'efficacité

- **Vue centralisée du système** ➔ vérification de l'état du système
  - état onduleur
  - état des disques
  - état des mises à jour système / logicielles
  - état anti-virus
- **automatisation du système**
  - défragmentation des disques
  - synchronisation des horloges
  - mise à jour système / logicielles
  - mise à jour anti-virus
- **harmoniser le matériel et les logiciels pour mieux les maîtriser**

- postes de travail, terminaux
- disques partagés, espace de stockage utilisateurs
- imprimantes, scanners partagés
- serveur applicatif, serveur de calcul

Autres moyens minima requis

- Financier : 5k € - 10k €
- Infrastructure : réseau 100 Mbits commuté
- Humain : 1 personne à temps plein

Figure 1 : *Schéma du processus d'élaboration du système informatique de l'unité*

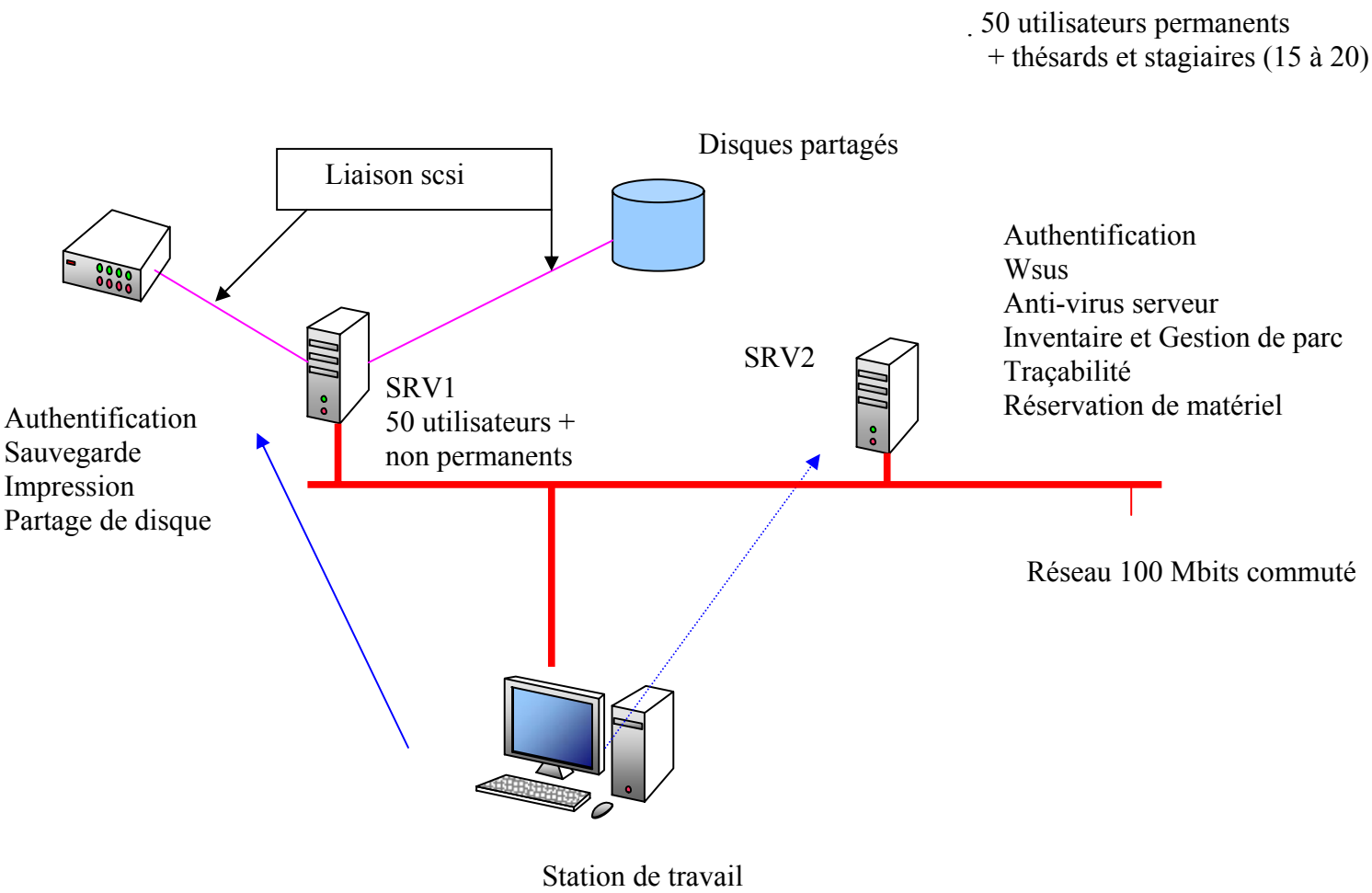

Figure 2 : *Schéma du nouveau système mis en place dans l'unité*