Retour d'expérience:

le déploiement d'un NAS en environnement LDAP pur,

dans le cadre de l'ENT de Rennes 1

Pierre-Antoine Angelini
CRI – Campus de Beaulieu
Université de Rennes 1 – Avenue du General Leclerc – 35042 Rennes Cedex
pierre-antoine.angelini*univ-rennes1.fr

Résumé

L'article expose la démarche du Centre de Ressources Informatiques (CRI) de l'Université de Rennes 1 dans le choix et l'intégration d'un NAS[1] dans son système d'informations. Cette action s'inscrit dans les actions d'homogénéisation des environnements informatiques des étudiants et personnels.

Rennes 1, après s'être doté d'un annuaire global pour les personnels et étudiants (LDAP Iplanet SUN), pouvait envisager le déploiement de services communs homogènes, parmi lesquels un E.N.T[2].

Parmi de nombreuses briques (agenda partagé, emplois du temps, ressources documentaires, assistance en ligne, dossier administratif, etc), les espaces de stockage (personnels, partagés, collaboratifs) représentaient un défi dans un contexte très hétérogène et face à une population très demandeuse de solutions. Ils devaient s'appuyer sur une solution souple, fiable et évolutive.

On découvrira ci-dessous le contexte technique et organisationnel, les attentes du projet, les fonctionnalités réellement disponibles et les améliorations possibles.

Mots clefs

NAS, LDAP, NFS, CIFS, pGina, quotas, snapshot, NDMP, TiNa, RAID,

1 Le contexte

L'université de Rennes 1 est implantée sur cinq campus rennais auxquels s'ajoutent plusieurs sites délocalisés (St Malo, St Brieuc, Lannion, Paimpont, Fougères). Dans un premier temps, seuls les campus de Rennes étaient concernés à court terme par le projet. Une partie des personnels des sites éloignés pourrait l'utiliser dès l'origine. L'objectif était d'étendre, à terme, le dispositif à l'ensemble de l'établissement, en fonction de l'amélioration de la connectivité inter-sites, via le réseau régional.

1.1 Les données des utilisateurs

Avec l'abandon des systèmes centralisés au cours des années quatre-vingt, les solutions informatiques individuelles s'étaient multipliées au sein de l'université, comme dans beaucoup d'autres structures et avaient fragilisé les informations et leur manipulation.

Les données des utilisateurs étaient, pour partie éclatées sur des serveurs disséminés sur tout le territoire de l'établissement et pour le reste conservées sur des postes individuels. La gestion des serveurs était assurée soit par le CRI, soit par des personnels de composantes, de laboratoires ou d'équipes dont ce n'était pas, le plus souvent, l'activité principale. La qualité des services ainsi rendus variait considérablement d'une situation à l'autre. Pour ce qui concerne les données conservées sur les postes utilisateurs, les pertes étaient fréquentes (vol, panne).

1.2 Une accessibilité réduite

Bien que toutes connectées au réseau, de nombreuses machines restaient indépendantes et autonomes. Les utilisateurs ne pouvaient donc accéder à leurs données que depuis des postes de travail spécifiques, voire depuis un seul poste de travail. En conséquence, dans l'enceinte même de l'université, l'accès à ces informations pouvait être impossible pour les utilisateurs nomades.

1.3 Une disponibilité incertaine et un partage difficile

En fonctionnement normal, les informations n'étaient accessibles que lorsque les machines qui les hébergeaient fonctionnaient. Le stockage sur des postes individuels rendait leur disponibilité aléatoire. De plus, le partage de données exigeait des manipulations compliquées pour les

[1]NAS: Network Attached Storage

[2]ENT: Environnement de Travail Numérique. Voit http://www.esup-portail.org

utilisateurs, notamment en raison des règles de sécurité inter-vlan[3] en vigueur à l'université.

1.4 Une confidentialité à améliorer

Alors que la confidentialité des informations est assurée sur les serveurs qui dépendent du CRI ou qui sont gérés par lui, elle ne l'est pas toujours de la même façon sur les serveurs gérés par les composantes elles-même. Quant aux données stockées sur des postes individuels, elles sont extrêmement exposées.

1.5 Une sécurité à renforcer

Les machines qui ne sont pas administrées par le CRI sont souvent peu ou pas sauvegardées. Il est donc malheureusement fréquent qu'il soit impossible de restaurer des données perdues (erreurs de manipulations, pannes, vols …). Ces pertes peuvent s'avérer catastrophiques pour les utilisateurs autant que pour l'établissement. La sécurité est une priorité de l'université en même temps qu'elle devient une demande forte de la part des utilisateurs, notamment dans les laboratoires.

1.6 En conclusion

C'est pourquoi l'université de Rennes 1 a décidé de mettre à disposition de tous ses utilisateurs (étudiants et personnels enseignants, administratifs et techniques), un espace de stockage qui pallie tous les défauts évoqués ci-dessus et qui assure l'accessibilité, la disponibilité, la fiabilité et la sécurité des données.

2 Les utilisateurs dans le détail

Les utilisateurs potentiels du service de stockage sont au nombre de 3000 pour les personnels de l'université (administratifs, enseignants, chercheurs, IATOS) et de 25 000 pour les étudiants.

2.1 Les personnels

Les personnels stockaient leurs informations sur :

- des serveurs Novell : ces serveurs hébergeaient les données des personnels de services administratifs et de quelques enseignants (données gérées par le CRI et sauvegardées tous les jours);
- des serveurs Windows : ces serveurs hébergeaient des populations hétérogènes (données gérées par le CRI sauvegardées, situation plus floue pour les autres);
- des serveurs Unix : une partie des utilisateurs voyaient leurs données hébergées sur les serveurs Unix ou Linux (notamment le CRI). On rencontrait toutes sortes de situations pour ce qui concerne la sauvegarde;
- des postes de travail individuels : beaucoup de personnels se contentaient de stocker leurs informations sur leur poste de travail personnel sans jamais les sauvegarder.

Certains agents, rattachés à plusieurs structures de l'établissement et qui pouvaient travailler dans autant d'endroits, n'avaient pas de lieu de stockage unique pour leurs données.

2.2 Les étudiants

Les étudiants avaient quant à eux accès à des salles pédagogiques, des salles libre service, des salles de documentation, les bibliothèques, les laboratoires de langue. Ils disposaient :

- d'un compte utilisateur et d'un espace de stockage, en général personnel, sur les serveurs de certaines salles pédagogiques, soit autant de répertoires personnels que de salles de ce type dans lesquelles ils sont accueillis, sans lien entre eux. Ces répertoires pouvaient être réinitialisés au début de chaque année universitaire ;
- d'un espace de stockage personnel pour les salles libre-service. Les étudiants migraient quand ils accédaient au second cycle mais ne conservaient pas leurs données ;
- d'accès dans des salles de documentation, bibliothèques ou laboratoires de langue ainsi que dans certaines salles pédagogiques, sans espace privé ; ils ne pouvaient transférer les données que par disquettes ou messagerie ;
- d'un compte de messagerie accessible par le Web.

2.3 Quelle authentification ?

Rennes 1 a engagé en 1999 le projet d'annuaire LDAP global.

Toutes les applications développées convergent vers ce projet avec la volonté de fédérer composantes et services autour de cet annuaire.

Parallèlement, nous voulions nous affranchir de toute synchronisation avec d'autres annuaires (*NIS, Active Directory, Samba*) et développer l'usage du SSO (*Single Sign On*).

Il en découlait naturellement la contrainte d'une authentification basée uniquement sur LDAP.

Cette démarche a été accompagnée d'une réflexion longue et très discutée sur le nommage des répertoires d'accueil (homedir) des utilisateurs. Il a été décidé :

- d'attribuer à un utilisateur un répertoire fixe et unique pour toute la durée de son passage à Rennes 1. Ceci évite notamment les transferts de données d'une année sur l'autre, pour la population étudiante;

[3]VLAN: Virtual Local Area Network ou réseau logique virtuel

- de ne pas gérer les droits d'accès aux homedir en utilisant les groupes, en raison de la multi-appartenance des étudiants , comme des personnels, à de multiples entités. Ceci se révélerait rapidement ingérable;
- de résoudre le transfert de données entre groupes d'utilisateurs, soit à travers des espaces spécifiques (espaces de partages), gérés par les utilisateurs ou soit avec des applications spécifiques (application de rendu de TP, par exemple).

3 L'appel d'offre

3.1 Pourquoi un NAS ?

L'expérience et les compétences acquises dans l'exploitation de petits NAS, par différentes équipes informatiques de Rennes 1, montraient que ce type de solutions :

- tenait bien la charge;
- était stable et fiable, avec une très bonne disponibilité;
- apportait une grande souplesse de configuration, notamment dans la gestion des volumes et des quotas;
- gardait un coût d'administration extrêmement faible;
- apportait des fonctionnalités supplémentaires, par rapport aux solutions basées sur des systèmes d'exploitation (OS) plus traditionnels.

Les OS spécifiques de ce type de machines, moins répandus, rendent ces matériels, de fait, moins faciles à attaquer et moins susceptibles d'intéresser des attaquants.

L'administration est facile à prendre en main pour une équipe, du moins dans des configurations simples.

Un des reproches majeurs vis à vis des NAS est leur coût d'acquisition et de maintenance.

3.2 SAN[4] versus NAS

On a l'habitude d'opposer NAS et SAN. Dans notre contexte, la nécessité d'apporter d'abord des services (NFS ,CIFS, WebDAV) militait pour une solution de type NAS.

Les SAN étaient également stables et fiables, souples en termes de gestion de volume, mais :

- plus coûteux en terme d'administration,
- plus difficiles à prendre en main,
- ne se chargeaient pas de la gestion des quotas, reportées vers les OS des serveurs.

Enfin, si la tenue en charge de solutions NFS ne faisait aucun doute face à un grand nombre d'utilisateurs, des doutes subsistaient vis à vis des services CIFS, via Samba.

Par ailleurs, les SAN exploités par le CRI (bases de données, messagerie) ne pouvaient être étendus facilement vers les capacités demandées. Il fallait, dans ce cas, envisager une nouvelle acquisition.

Rennes 1 a donc décidé d'orienter son appel d'offres vers un NAS.

3.3 La procédure

Après une consultation des divers acteurs du domaine, la procédure dite « de dialogue compétitif » a été retenue, pour plusieurs raisons:

- Le secteur des NAS est en pleine évolution et un CCTP[5] trop rigide, par méconnaissance des fonctionnalités nouvelles ou en développement, pouvait priver Rennes 1 d'une solution viable;
- Les attentes du dossier, en termes de fonctionnalités, étaient ambitieuses. Il convenait de les ajuster au mieux à la réalité du marché.

3.4 Les candidats

Les 14 candidats nous proposaient des solutions de type NAS (EMC, Network Appliances, Dell, IBM), des *cluster* Linux ou Solaris.

En finale, l'université de Rennes 1 a confronté les solutions de 4 candidats qui proposaient tous une solution à base Network Appliances, plus ou moins aboutie, plus ou moins intégrée.

3.5 Le choix

Le choix s'est porté sur un FAS 940, mieux adapté pour supporter les volumétries demandées et la charge potentielle.

Nous visions un espace de 100 Mo par étudiant et de 500 Mo par personnel, soit environ 4To utiles. Les projections faisaient apparaître un besoin d'environ 1TO pour un espace supplémentaire dédié aux espaces partagés et collaboratifs. Le FAS 940 supportant à l'époque 6TO, il est apparu judicieux de l'équiper totalement, en prévision de l'évolution de la demande.

La machine a été équipée de :

- 9TO brut avec 70 disques *Fiber Channel,* soit 6TO utiles;
- double alimentation;
- 6 interfaces gigabit cuivre permettant la redondance de liens vers les VLAN recherche et enseignement, une liaison dédiée aux sauvegardes;

[4]SAN: Storage Area Network

[5]CCTP: le Cahier des Clauses Techniques Particulières rassemble les détails techniques d'un appel d'offres, donnant lieu à un marché.

- DataOnTap version 6.3.

4 L'intégration

4.1 La première année

La machine a été installée durant l'été 2004. Nous avons défini 3 volumes RAID4, occupant respectivement deux fois 2,5To et une fois 1.2To.

Très vite des difficultés d'intégration sont apparues, notamment sur l'authentification LDAP, durant le mois d'août 2004. Les difficultés à trouver un interlocuteur technique, en raison des vacances, une documentation LDAP indigente, ont retardé le déploiement et empêché sa mise en service pour la rentrée 2004-2005.

Celui-ci a commencé effectivement en janvier 2005, de manière progressive. Plusieurs populations d'étudiants et de personnels ont utilisé la machine durant l'année 2005 :

- 2000 répertoires personnels (étudiants et personnels) pour environ 300 GO cumulés;
- 100 répertoires partagés pour les services administratifs, regroupant 1200 personnes, pour environ 200 GO cumulés;
- des laboratoires et entités connexes ayant demandé en urgence un espace de stockage, soit environ 1TO, pour 300 personnes.

Durant cette période la charge moyenne de la machine (mesure sysstat pondérée) a été de 17%, pour environ 500 utilisateurs simultanés. L'utilisation a été plus faible qu'escomptée, en raison du retard de déploiement.

L'intégration à l'ENT et la nouvelle rentrée devraient faire monter ces chiffres de manière conséquente durant le dernier trimestre 2005.

Plus de 800 machines clientes ont été modifiées pour utiliser le NAS à la rentrée 2005-2006. Par ailleurs de très nombreuses formations ont migré durant l'été depuis des serveurs Novell, NT ou Unix pour converger vers le NAS.

4.2 Les fonctionnalités attendues et la réalité

Parmi les fonctionnalités attendues, certaines avaient été validées par le constructeur et se sont révélées soit inutilisables, soit décevantes. D'autres sont aujourd'hui des points forts de cette solution et méritent qu'on leur porte attention lors d'un dossier similaire.

NFS

Ce type de machine propose du partage de fichiers via NFS V2, V3 UDP et TCP, voire V4. Seule la version V3 est utilisée à Rennes 1, en raison du peu de clients NFS V4.

Le montage de machines Unix, Linux s'opère sans difficultés et les mécanismes traditionnels d'*exports*, de *netgroup* sont utilisés, sur la base de fichiers locaux au NAS.

Pour des raisons évidentes de sécurité, l'export est réservé à des machines dont le CRI a la maîtrise.

CIFS

La volonté de Rennes1 d'utiliser exclusivement une authentification LDAP a révélé très vite, et en dépit des affirmations de l'appel d'offres, les limitations de cette solution.

La configuration « CIFS + authentification LDAP pure» fonctionne dans un *workgroup*, et non pas un domaine Microsoft. Ceci a des conséquences.

La gestion des droits d'accès n'a pas la souplesse des ACL NT. On doit se contenter des droits d'accès traditionnels Unix.

Un autre point nous a échappé lors des entretiens de l'appel d'offres : ce mode « LDAP pur » impose, comme décrit dans la documentation DataOnTap[6], une authentification du client via un mot de passe en clair. Ce point préoccupant fait partie de nos demandes réitérées d'amélioration auprès de Network Appliances.

Il empêche également le montage automatique de lecteurs sur des clients Windows XP originaux, puisque XP envoie toujours un mot de passe chiffré par défaut. Les clients dont le *logon* a été modifié avec pGina (http://pGina.xpasystems.org),sans permettre de s'affranchir de la contrainte évoquée ci-dessus pour les mots de passe, ne présentent pas ce problème

Les clients Mac OS X, à partir de la 10.4, présentent le même comportement, en plus grave, puisque l'on ne sait pas envoyer un mot de passe convenant à cette configuration. Le montage via CIFS est donc impossible. Cette situation est préoccupante.

Le montage de lecteurs via les clients Samba Linux se fait sans difficultés.

WebDAV

Ce protocole, présent dans DataOnTap, a fait l'objet de questions précises durant l'appel d'offres et de réponses tout aussi précises du fournisseur, confirmant la disponibilité et l'adéquation à notre environnement.

Tous les doutes étaient permis, en l'absence de ACP[7], sur la capacité de cette machine à offrir un partage de fichiers,

[6]Voir annexe en fin de document.

à travers ce protocole, dans des conditions de sécurité et de contrôle d'accès conformes aux souhaits de Rennes 1.

En dépit des affirmations de Network Appliances, nous avons pu constater que WebDAV est, dans son implémentation en version 6.X, un protocole basique qui fonctionne, mais sans aucun contrôle d'accès. Il est donc inutilisable dans notre contexte à ce jour.

Gestion des droits d'accès

Les droits d'accès gérés dans cette configuration suivant les standards Unix sont disponibles à la fois dans l'environnement NFS et CIFS. Les partages visibles dans les deux environnements (nommés « *shares* » dans la terminologie DataOnTap) sont alors de type « *mixed* ».

Un utilisateur Windows peut changer les droits d'accès de ses données via un utilitaire : SecureShare. Celui-ci est fourni avec le NAS.

Par ailleurs, les partages miment les droits obtenus avec un bit S sous Unix.

Par exemple, le bit S appliqué sur le groupe d'un répertoire provoque l'appartenance à ce groupe de tout fichier créé dans ce répertoire. Ceci correspond à l'option « *forcegroup* » de création des partages CIFS.

La disponibilité de droits d'accès aussi fins que ceux disponibles avec un domaine NT fait partie des requêtes de Rennes 1 auprès du fournisseur.

Quotas

Une gestion de quotas performante, étant données les populations en jeu, devait pouvoir traiter toutes les configurations présentes à Rennes 1. Les spécifications laissaient à penser que nous aurions un environnement très riche : nous ne fûmes pas déçus.

Gestion par personne (uid), par groupe(gid), par défaut, par volume logique, par *quota tree* (volume logique limité par un quota spécifique), par groupe dans un *quota tree*, etc.

La mise en place est souple (un fichier de configuration) et la commande de mise à jour simple (quota on/quota off par volume logique).

Le recalcul des quotas (après chaque modification) peut cependant s'avérer long sur des gros volumes. C'est pourquoi il est automatisé et effectué durant la nuit.

Snapshot

Ce mot décrit la possibilité de programmer le stockage d'images du système de fichiers à un instant t.

L'utilisateur trouvera ces images dans un répertoire nommé *.snapshot* ou *~snapshot* (suivant l'OS) dans le point de montage du NAS. Elles contiendront une copie en lecture seule de ses fichiers au moment de la création de l'image. Il y accède seul, exploite ses fichiers par recopie. Les *snapshot* ne font pas partie des quotas de l'utilisateur.

Les images ont une durée de vie programmable, et l'algorithme employé minimise beaucoup l'espace occupé par ces images. Ils représentent au plus 10% du volume réel des données utilisateurs, dans notre contexte.

Nous avons choisi des snapshot étalés sur 3 jours consécutifs, en boucle, complétés par un snapshot du dimanche précédent.

Cette fonctionnalité élimine à 95% les demandes de restauration de fichiers par les utilisateurs.

4.3 Administration

L'administration se fait soit à travers un site web, soit à travers une connexion directe (telnet en standard, SSH en option), soit à travers des commandes rsh depuis une machine autorisée.

Le serveur web intégré au NAS permet d'effectuer 90% des tâches de configuration.

L'accès telnet est réservé aux tâches spécifiques, en face d'un problème spécifique.

La commande rsh est le moyen d'automatiser toutes les tâches récurrentes : gestion des *homedir*, des *snapshot*, des accès partagés. Quelques exemples sont donnés en annexe.

4.4 Sauvegardes via NDMP

NDMP (Network Data Management Protocol) est un standard aujourd'hui disponible sur de nombreuses plates-formes. Ce protocole définit un format de données lues ou écrites à travers les pilotes de disque ou de bande. Il permet également le contrôle de librairies.

Il est natif dans DataOnTap et l 'intégration NDMP se fait sans difficultés avec le logiciel TiNa (Time Navigator de Atempo).

Un lien gigabit dédié, sur adresse privée, permet d'éviter l'utilisation des liens dédiés aux utilisateurs.

Il faut prendre la précaution d'exclure les *snapshot* des sauvegardes.

5 Les difficultés

5.1 Patch et solutions de contournement

L'intégration LDAP a montré des dysfonctionnements divers, résolus (ou non) par des solutions de contournement ou des *patch*.

[7]ACP (Access Control Protocol) permet de gérer les droits d'accès à des ressources de type WebDAV,au travers des ACL (Access Control List).

- pas de prises en compte des groupes dans LDAP (*backport patch* sur version 6.3, puis contournement sur 6.5, intégration dans la 7.0);

- *reboot* intempestifs lors du *login* d'utilisateurs possédant un mot de passe chiffré suivant la méthode « *advanced crypt* ». Si la chaîne chiffrée commence par le caractère _ , elle plante un processus vital et provoque un *kernel* panic. Les solutions de contournement proposées ne fonctionnent pas. Solution temporaire: ne pas utiliser « *advanced crypt* »;

- accès sans contrôle à toutes les données : effet de bord désagréable du contournement proposé pour résoudre le problème des mot de passe chiffrés « *advanced crypt* ».

- mot de passe non chiffré sur le réseau: nous sommes en attente d'informations sur le sujet.

L'origine de ses difficultés découle d'un fait découvert en Janvier 2005 : Rennes 1 est, à ce jour, et d'après la base de connaissances de Network Appliances, le seul site au monde à utiliser un NAS dans ce type d'authentification. L'expérience accumulée par le fournisseur en ce domaine est donc limitée.

L'ensemble des problèmes présentés ci-dessus sont issus de DataOnTap, et donc susceptibles de se présenter sur toute la gamme NAS Network Appliances.

- abus de ressources : ce point n'est pas spécifique du NAS, mais mérite attention lorsque l'on partage une machine à grande échelle. Les outils de surveillance du NAS permettent l'identification précise et rapide d'un client NFS gourmand. Le CRU[8] utilise actuellement 300 GO pour héberger son serveur miroir FTP, via un lien gigabit dédié. Lors de la publication sur le site de la Mandrake 10.1, la charge imposée au NAS a frôlé les 100% CPU. Il a suffi de changer la taille des requêtes NFS (32K au lieu de 8k) émises par ce client pour revenir à des valeurs très acceptables.

5.2 Les pannes

Depuis la mise en service 4 disques FC ont présenté des défauts. Détectés par le système, ils ont été mis hors service et remplacés par le disque de « spare » présents dans chaque bloc RAID4 de 12 disques. L'envoi automatique d'un disque neuf permet de réparer dans les plus brefs délais (moins de 24 heures).

5.3 Les limitations de LDAP client

Les implémentations de LDAP pour les clients ne sont pas toujours de même qualité.

- L'intégration PAM LDAP Solaris représente , avant la version 9.0, une course d'obstacle,

- La notion de filtre LDAP, destiné à restreindre l'accès aux machines clientes, repose sur un fichier local (aussi bien sous Unix qu'avec pGina). Il peut devenir complexe de gérer l'accès à une salle lorsque des étudiants issus de multiples entités l'utilisent. Le filtre peut également devenir trop long.

6 Les améliorations en cours ou prévues

6.1 Gestion déléguée des quotas

Si la gestion des quotas est très souple et fine, elle souffre cependant d'une faiblesse en terme d'administration.

Tout repose sur un seul fichier local du NAS (/etc/quotas) administré de manière centralisée. S'agissant d'une machine partagée entre de multiples entités, une gestion centralisée est lourde et ne peut perdurer.

L'année 2006 verra le développement au CRI d'une interface web autour de MySQL. Elle permettra de déléguer l'administration des quotas d'un espace de partage à un responsable de service, par exemple.

6.2 Gestion déléguée des accès aux espaces partagés

Si la gestion des accès à un espace partagé est très souple et fine, elle souffre cependant d'une faiblesse en terme d'administration.

Tout repose sur un seul fichier (/etc/groups) administré de manière centralisée. De manière encore plus aiguë que la gestion des quotas, cette gestion centralisée est inadaptée.

Si l'annuaire LDAP est capable de fabriquer automatiquement les groupes, les responsables de ces services sont malgré tout les plus indiqués pour gérer la liste de leur personnel et surtout les exceptions.

Les évolution de l'ENT pour 2006 devraient permettre d'offrir une gestion des accès plus souple. Le NAS deviendra dans ce cas précis un simple serveur de fichiers adossé à un frontal.

[8]CRU: Comité Réseau des Universités. Le CRU co-organise une grande manifestation tous les deux ans, avec un certain succès. Tous les détails sur http://www.jres.org et http://www.cru.fr. :-)

7 Les évolutions prévues

7.1 Sécurisation du NAS

Le NAS est devenu un élément vital de l'infrastructure. Malgré son architecture très redondante, on peut penser que lorsque la capacité nominale sera atteinte, nous risquons d'avoir des difficultés en cas de perte complète d'un volume.

Même avec des lecteurs performants, la restauration d'un volume conséquent peut prendre des heures.

Plusieurs hypothèses sont envisagées, dont, par ordre de coût décroissant :

- la mise en *cluster* (très coûteuse);
- la duplication sur un autre NAS moins performant;
- la sauvegarde sur disques.

7.2 Un autre NAS

Lors de son déploiement, nous avons été amenés à utiliser des volumes encore inutilisés du NAS pour répondre à la demande d'espace émise par des laboratoires.

A ce jour ils occupent 1 TO sur la machine. Un recensement effectué sur les mois de mai à juillet 2005 a permis d'identifier un besoin initial de 12 TO pour la seule communauté rennaise.

Un appel d'offres pour un NAS de nouvelle génération (disques SATA) devra venir répondre à cette demande fin 2005.

8 Conclusions

Le bilan de cette opération est positif pour Rennes 1. Le service est au rendez-vous et nous pouvons espérer obtenir rapidement une solution pour les quelques points sombres du dossier.

- la machine nous apporte le service attendu en termes de fiabilité et de disponibilité;
- malgré un démarrage difficile et un point actuellement préoccupant concernant la sécurité, l'intégration LDAP est correcte. Elle reste perfectible et la nouvelle version de DataOnTap (7.0) devrait apporter quelques nouveautés (LDAPS entre autres);
- le FAS 940 répond sans difficultés à une charge conséquente. Lors de la présentation des JRES, après un trimestre sous régime soutenu, des données plus précises seront diffusées.

Annexe

DataOnTap[9]

Cet OS spécifique aux matériels Network Appliances est basé sur un noyau Unix. Optimisé pour les services de fichiers, il s'appuie sur un système de fichiers propriétaire (WAFL[10]), et sur une architecture de type RAID4 (1 disque de parité par groupe RAID) ou RAID-DP (deux disques du groupe RAID 4 peuvent tomber en panne simultanément). Outre sa fiabilité, il permet l'intégration du NAS dans un SAN et dispose de fonctionnalités originales, mais qui ne sont plus toujours exclusives. Le site http://www.netapp.com vous donnera de nombreuses informations sur ce produit.

La concurrence (notamment EMC) est très présente. Voir http://www.emc.com

Exemples de commandes rsh

Ci-dessous, des extraits du script perl qui crée les *homedir* et *shares* CIFS, en fonction d'informations collectées journellement dans l'annuaire LDAP, via un mécanisme de notifications. Les volumes contenant les *homedir* sont montés via NFS sur la machine d'administration.

```
#!/usr/local/bin/perl
# Création d'un homedir sur le serveur de stockage
#en fonction des 5 paramètres passés en entrée
.....
my ($uid)=shift;
my ($uidnum)=shift;
my ($gidnumber)=shift;
my ($hd)=shift;
my ($type)=shift; #type = pers ou etu
print LOG "Traitement de $uid\n";

#determination des points de montage root sur la machine d'administration
my ($root, $root2, $rootvol);
if ($type =~ /pers/i) {
  $root = "/sf1vol2";
  $rootvol = "/vol/vol2";
  $root2 = "staff";
}
else {# type = etu
  $root = "/sf1vol1";
  $root2 = "student";
  $rootvol = "/vol/vol1";
```

[9] http://www.netapp.com/products/software/ontap.html

[10] WAFL: Write Anywhere Filesystem Layout

```
}
.....
       print LOG ("création du home dir de$uid ---> /
$root/private/$root2/$p1/$p2$p1/$uid \n");
   unless (-d "$root/private/$root2/$p1") {
     unless (mkdir("$root/private/$root2/$p1", 0755)) {
                        print LOG ("Impossible de creer /
$root/private/$root2/$p1 ($!) \n\n");
            close LOG;
            exit;
      }
   }
   unless (-d ("/$root/private/$root2/$p1/$p2$p1")) {
          unless (mkdir("/$root/private/$root2/$p1/$p2$p1",
0755)) {
                      print LOG ("Impossible de creer /
$root/private/$root2/$p1/$p2$p1 ($!) \n\n");
       close LOG;
       exit;
     }
   }
    unless (mkdir("/$root/private/$root2/$p1/$p2$p1/$uid",
0700)) {
                   print LOG ("Impossible de créer /
$root/private/$root2/$p1/$p2$p1/$uid ($!) \n\n");
     close LOG;
     exit;
   }
.....
    print LOG ("Création du share $uid... \n");
    my$rootsf1="$rootvol/private/$root2/$p1/$p2$p1/$uid"
;
   `rsh sf1staff cifs shares -add $uid $rootsf1`;
    print LOG ("Droit d'acces $uid\n");
    `rsh sf1staff cifs access $uid $uid 'Full Control'`;
    print LOG ("Retrait droit everyone\n");
    `rsh sf1staff cifs access -delete $uid everyone"`;
        print LOG ("Environnement $uid, $uidnumber de
$gidnumber, avec homedir $homedirectory fini \n\n");

} #fin unless roothd
else {
print "Homedir deja existant \n\n";
print LOG "Homedir deja existant \n\n";
}

} # fin unless ARVG =4
close LOG;
exit;
```