Des services authentifiés pour une communauté de 50 000 utilisateurs dans 17 établissements

Alain Zamboni
Centre Réseau Communication, Université Louis Pasteur
Alain.Zamboni@crc.u-strasbg.fr

Pierre David
Centre Réseau Communication,Université Louis Pasteur
Pierre.David@crc.u-strasbg.fr

Jean Benoit
Centre Réseau Communication, Université Louis Pasteur
Jean.Benoit@crc.u-strasbg.fr

Résumé

Le CRC, gestionnaire du réseau métropolitain Osiris pour le compte de 17 établissements, offre de nouveaux services très fortement mutualisés pour l'ensemble de la communauté d'enseignement supérieur et de la recherche à Strasbourg.

Ces services sont l'accès VPN, qui permet aux utilisateurs d'arriver directement dans le sous-réseau de leur composante, le réseau sans-fil accessible à tous sans frontière d'établissement, et la messagerie pour une vaste partie de la communauté, comprenant entre autres les étudiants des 3 universités et des écoles d'ingénieurs.

Tous ces services sont authentifiés, pour une population d'environ 50 000 utilisateurs. Nous présentons dans cette contribution l'infrastructure d'authentification et son interaction avec les annuaires d'établissements et les Environnements Numériques de Travail.

Mots clefs

Authentification, services, LDAP, messagerie, annuaire, réseau sans-fil, VPN.

1 Introduction

La plupart des sites universitaires mettent de nouveaux services à disposition de leurs utilisateurs. Par exemple, un nombre croissant d'universités se dotent de serveurs VPN pour remplacer leurs vieux accès RTC et permettre à leurs utilisateurs de bénéficier des offres des fournisseurs d'accès à l'Internet. De même, une forte incitation du Ministère a amené la plupart des universités à offrir des accès au réseau sans-fil sur les campus.

Les populations concernées par ces nouveaux services sont de plus en plus importantes. Ainsi, il n'est pas rare de voir un serveur de messagerie pour une université héberger des dizaines de milliers de comptes. Cette démarche de démocratisation des services est poussée en avant par la mise en place d'Environnements Numériques de Travail (ENT) dans un nombre croissant d'établissements.

Le réseau Osiris regroupe la quasi-totalité de la communauté de l'Enseignement Supérieur et de la Recherche à Strasbourg : 17 établissements sont connectés au réseau et ont confié au Centre Réseau Communication (CRC) de l'Université Louis Pasteur la mission d'exploiter et d'opérer le réseau, y compris un nombre croissant de services.

L'offre de services du CRC, initialement composée de l'hébergement de la messagerie, s'est récemment enrichie de l'accès VPN et de la gestion du réseau sans-fil transversal à une majorité d'établissements. Les caractéristiques de cette offre sont les suivantes :

- une très grande population concernée : initialement prévus pour 50 000 utilisateurs, les services sont maintenant proposés à près de 75 000 utilisateurs (en incluant les anciens étudiants qui ont encore un compte pendant une période transitoire) ;
- le service VPN offert à tous les utilisateurs permet à chaque établissement, laboratoire ou service, de disposer d'un serveur VPN virtuel qui amène ses utilisateurs dans son propre sous-réseau ;
- le réseau sans-fil est géré de manière transversale par le CRC pour le compte de l'ensemble de la communauté, ce qui permet à n'importe quel utilisateur reconnu de s'authentifier sur tout point d'accès de manière transparente, même s'il est situé dans un autre établissement, laboratoire ou service que le sien.

Pour proposer aux utilisateurs un accès cohérent, nous avons été amenés à unifier l'authentification et à développer des outils permettant de gérer une très grande masse d'utilisateurs.

Après une présentation sommaire des différents services proposés à la communauté strasbourgeoise, nous détaillons l'unification des bases d'authentification sous la forme de l'annuaire Osiris, puis nous décrivons l'intégration de cet annuaire avec les services. Enfin, nous terminons en évoquant la démarche que nous avons suivie pour aller vers cette unification et le premier bilan que nous pouvons tirer de la mise en exploitation.

2 Les services proposés par le CRC

2.1 Accès VPN

Le VPN (Virtual Private Network) est un service permettant à un poste client distant de se connecter, via un réseau public, à un réseau privé tel qu'Osiris et ainsi d'obtenir une adresse IP dans ce dernier. La communication est sécurisée par la mise en place d'un tunnel chiffré entre le poste client et le serveur VPN.

Concrètement, cette technologie permet aux utilisateurs d'accéder aux ressources privées de leur réseau quel que soit leur lieu de connexion : domicile, campus extérieur, depuis l'étranger, etc. Depuis mars 2005, le CRC offre ce service aux utilisateurs d'Osiris, décliné sous 3 formes différentes, selon les besoins des laboratoires ou établissements.

VPN standard

L'accès VPN standard permet aux utilisateurs nomades d'arriver dans un sous-réseau d'Osiris commun, comme illustré sur la Figure 1. Les utilisateurs peuvent dès lors accèder aux données à accès restreint, comme par exemple les publications scientifiques mises à disposition par les Services Communs de Documentation.

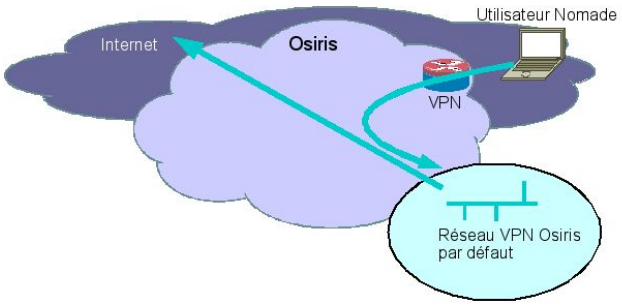

Figure 1 - *Fonctionnement du VPN Standard*

VPN Lab

L'accès VPN-Lab permet aux utilisateurs nomades d'arriver dans un sous-réseau VPN dédié à leur composante (laboratoire, service, voire établissement tout entier). Cette plage d'adresses IP étant réservée à ses utilisateurs, l'administrateur de la composante peut autoriser l'accès à des ressources internes, comme des serveurs de fichiers.

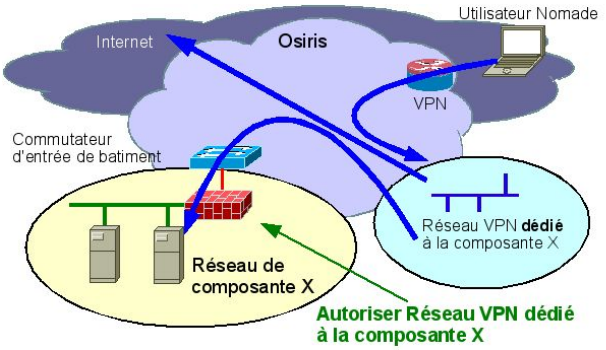

Figure 2 - *Fonctionnement du VPN Lab*

VPN Lab+

L'accès VPN-Lab+ permet aux utilisateurs nomades d'arriver directement dans le sous-réseau de leur composante. La différence par rapport à l'offre précédente est que le trafic des postes nomades est amené par le CRC sur un port spécifique du commutateur d'entrée de bâtiment, permettant à l'administrateur de connecter les domaines de diffusion Ethernet du réseau principal et du réseau nomade, et de mettre un pare-feu (bridgé par exemple) pour implémenter une politique de sécurité plus fine. Pour l'utilisateur nomade, le bénéfice est qu'il est protégé par cette politique de sécurité, et qu'il peut de plus accéder aux fonctionnalités nécessitant le mécanisme de « broadcast » (partages Windows par exemple). Pour l'administrateur, la politique de sécurité est aussi simplifiée car le réseau des nomades est distingué sur une interface particulière..

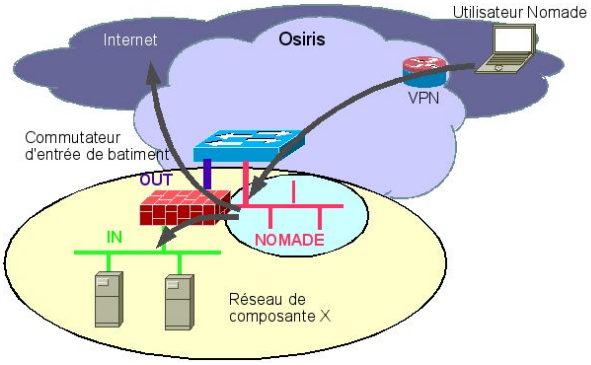

Figure 3 - *Fonctionnement du VPN Lab+*

La conception des différentes offres VPN du CRC a été réalisée par Laurence Moindrot.

2.2 Accès réseau sans-fil

L'Université Louis Pasteur s'est engagée dès 2001 dans le déploiement du réseau sans-fil. Après avoir pris conscience des problèmes que pose le développement non maîtrisé de tels réseaux, le Conseil d'Administration a confié la construction d'un réseau sans-fil commun, et sa gestion exclusive par le CRC. Cette politique a été par la suite reprise par d'autres établissements sur Osiris. Actuellement, 200 points d'accès sont déployés et gérés par le CRC, pour une perspective à terme d'un millier de bornes pour couvrir l'ensemble de la population d'enseignement supérieur et de recherche strasbourgeoise.

Cette gestion mutualisée par le CRC offre de nombreux avantages :

- accès uniforme : les utilisateurs nomades doivent pouvoir accéder au réseau sans fil de manière identique quel que soit le bâtiment, d'où un besoin de cohérence pour les technologies et matériels employés ;
- niveau de sécurité élevé : le réseau sans-fil est naturellement plus vulnérable aux problèmes de sécurité, ce qui nous a amenés à offrir un niveau de sécurité élevé passant par une authentification commune ; ces principes sont uniformément appliqués : un utilisateur doit avoir le même compte dans tous les bâtiments ;

– économie de ressources : le CRC a initié un groupement de commandes entre établissements pour obtenir de meilleures conditions financières et des conditions techniques homogènes ; de même, la réalisation d'une architecture d'authentification unique offre aussi une économie substantielle de temps et d'argent pour chaque établissement ;

L'expérience acquise par le CRC sur les premiers déploiements a permis aux établissements de gagner un temps précieux par la suite. De plus, afin d'avoir une couverture optimale, le CRC propose la réalisation de la cartographie. Cette étape était auparavant confiée à un prestataire externe, mais nous avons préféré par la suite la réaliser en interne. En effet, l'accompagnement du prestataire ne nous faisait pas gagner de temps, et les résultats se sont avérés décevants.

Actuellement, la connexion au réseau sans fil place l'utilisateur dans un réseau commun transversal. À terme, l'objectif est d'amener l'utilisateur dans le réseau de sa composante, à l'instar de l'offre VPN. Malheureusement, en raison de limitations matérielles (les bornes utilisées, Cisco AP 1100, n'autorisent pas plus de 16 Vlans), ceci est actuellement impossible à réaliser facilement.

Initialement, il était prévu de proposer un accès authentifié via le protocole IEEE 802.1X [1,2] au réseau sans-fil. À l'usage, nous avons constaté que le niveau de support de ce protocole était assez variable et compliquait considérablement la connexion des personnes de passage (par exemple lors des conférences). Nous avons donc complété notre offre par un accès, baptisé « non sécurisé », offrant une authentification via un portail captif.

Accès sans-fil sécurisé

L'accès sécurisé au réseau sans-fil implique la sécurisation des échanges transitant sur les ondes, effectuée par chiffrement des données entre le poste client et la borne à laquelle il s'associe. L'authentification est réalisée par le protocole 802.1X, et les données sont ensuite chiffrées en WPA/TKIP, WPA/AES ou WEP selon les capacités de la carte du client, avec une renégociation de la clé de chiffrement toute les deux minutes. La mise en place de cette connexion sécurisée nécessite, pour certaines plate-formes, l'installation et la configuration d'un client particulier (Aegeis, puis SecureW2 pour les plates-formes Windows).

Avec ce mode de connexion, tous les protocoles sont accessibles sans filtrage, et toutes les données sont chiffrées dans des conditions de sécurité satisfaisantes.

En revanche, le support de multiples plate-formes est complexe du fait de l'ampleur et de la diversité de la population concernée. De plus, nous rencontrons quelques problèmes d'incompatibilité de WPA avec certains pilotes de cartes sans-fil.

Accès sans-fil non sécurisé : le portail captif

Le portail captif est un portail Web couplé à un garde-barrière qui gère les accès au réseau sans-fil Osiris en mode non sécurisé. Il permet de donner aux utilisateurs, après authentification, un accès limité (essentiellement le Web et les protocoles chiffrés comme SSH, IMAPS, etc.) à Osiris et Internet de la manière la plus simple possible, via l'ouverture d'un simple navigateur Web.

Cette simplicité implique l'association aux points d'accès sans chiffrement de niveau 2. Aucun logiciel d'authentification n'est donc à installer sur le poste client. En revanche, la sécurité doit être assurée au niveau applicatif.

Les avantages du portail captif sont donc une connexion simple, facile et rapide, sans logiciel client à installer. En revanche, les données transitent en clair, ce qui nous contraint à restreindre les accès aux seuls protocoles de niveaux supérieurs chiffrant les données.

Ce portail captif est un développement logiciel du CRC car, à l'époque de nos tests, aucun logiciel disponible ne savait gérer complètement le protocole IPv6 [4]. Nous avons donc développé un portail simple, hébergé sur un système FreeBSD, et utilisant le serveur Web Apache ainsi que le pare-feu « pf » pour le filtrage.

Après une année d'exploitation, nous constatons qu'environ 36 % des connexions se font en mode sécurisé et 64 % des connexions se font avec le portail captif.

La conception du réseau sans-fil a été réalisée par Christophe Saillard et Sébastien Boggia.

2.3 Messagerie

Le service d'hébergement des boîtes aux lettres est offert par le CRC depuis les débuts d'Osiris. Jusqu'au début 2005, environ 2 700 boîtes étaient ainsi hébergées pour une demi-douzaine d'établissements.

Les établissements réalisant les avantages de la mutualisation des ressources, le CRC s'est vu confier pour la rentrée 2005 l'hébergement des boîtes aux lettres des étudiants des 3 universités et des écoles d'ingénieurs strasbourgeoises. C'est ainsi que nous hébergeons aujourd'hui environ 75 000 boîtes aux lettres. Ce nombre continue d'augmenter car de nouvelles composantes disposant de leur propre système de messagerie souhaitent profiter de l'offre du CRC.

Un tel nombre d'utilisateurs a nécessité le redimensionnement du serveur de messagerie en terme d'espace disque pour offrir un espace de stockage adapté, et en terme de puissance pour supporter le surcroît de charge. Pour sécuriser les données, nous avons également mis en place un système de sauvegarde.

Grâce à cette nouvelle architecture d'hébergement de messagerie, le CRC offre de nouvelles fonctionnalités aux utilisateurs comme la mise en place de répondeurs automatiques, de transfert[1], un filtrage anti-spam, la possibilité d'avoir des alias ou des « mini-listes » de diffusion, et bien sûr la lecture par les protocoles classiques (IMAP et POP3, avec version sécurisée) et un Webmail robuste (IMP).

[1]Ce qu'on appelait autrefois un « .forward »...

De plus, nous avons délégué certaines fonctions de paramétrage vers nos correspondants réseau (gestion des listes et des aliases, gestion des comptes, modification des répondeurs et des transferts des utilisateurs, etc.), ce qui permet une meilleure gestion des domaines de messagerie.

Nous avons pris l'option de gérer l'ensemble de la messagerie sur trois serveurs :

- un serveur confortablement doté en ressources (4 processeurs, 2 Go de mémoire, 1,7 To d'espace disque) pour l'hébergement des boîtes, la réception et la lecture ;
- un deuxième serveur de secours (moins puissant, mais avec 6 To d'espace disque pour disposer d'une fonction d'archivage), afin de basculer le plus rapidement possible en cas de problème sur le premier serveur ;
- un dernier pour le Webmail, pour diminuer la surcharge due au chiffrement sur le premier serveur ;

Gérant traditionnellement des volumes de données de quelques centaines de giga-octets, le passage à un volume de données beaucoup plus important nous a fait rencontrer des problèmes inattendus : nous avons atteint les limitations des systèmes et des applications. Par exemple, le système UFS de FreeBSD, même avec les « soft-updates », s'est avéré inexploitable avec un temps de démarrage minimum de 40 minutes, la synchronisation entre les deux serveurs avec GEOM nous semblait séduisante, mais toute perte de connectivité réseau entraînait une synchronisation qui pouvait durer plusieurs jours, et l'utilitaire « rsync » se terminait prématurément[2] lorsque nous simulions la synchronisation de notre espace bien rempli, du fait du trop grand nombre de fichiers.

Compte-tenu des délais, nous avons dû migrer vers ReiserFS sous Linux et nous avons adopté une stratégie plus simple de synchronisation avec le serveur de secours, basée sur l'utilitaire « rdiff-backup » qui permet de conserver un historique des modifications sur plusieurs jours. Cependant, le coût de la restauration est élevé, et un basculement sur le serveur de secours doit être évalué en fonction de la durée prévisible de la panne du serveur principal, car la restauration des données sur celui-ci après son redémarrage peut durer jusqu'à 3 jours (toujours pour des disques pleins). Heureusement, cette restauration peut se faire alors que l'activité est reprise, les messages restaurés s'ajoutant aux messages dans les boîtes.

Une évolution prévisible de cette situation consiste en la mise en place d'un SAN, en collaboration avec un autre service de l'ULP. L'évolution vers des volumes de données importants pose en tous cas des problèmes inhabituels.

La conception de l'infrastructure système de la messagerie (gestion du volume de données, synchronisation, système de secours) a bénéficié du concours de Philippe Pegon.

[2]... avec le message bien connu « bus error. Core dumped » !

2.4 Applications web

Le CRC propose également à ses utilisateurs, et notamment aux correpondants réseaux, un intranet et des applications Web authentifiés [3].

3 L'annuaire Osiris

L'énumération des services authentifiés et des populations concernées fait apparaître le besoin d'une base d'authentification unique pour tous les services du CRC.

De plus, les établissements se sont souvent engagés dans des démarches de mise en place d'annuaire d'établissement, voire de développement d'environnement numérique de travail (ENT). Il paraît alors évident que l'accès aux services du CRC doit se faire avec le même couple login/mot de passe que celui de l'ENT ou de l'annuaire d'établissement lorsqu'il existe. Ainsi est né l'annuaire Osiris.

3.1 Architecture globale

Gérer une base de comptes par service ou par application se révèlerait bien trop fastidieux et coûteux en temps pour l'administrateur, du fait de la multiplication des opérations de gestion et de l'incohérence des données qui en résulterait. Pour l'utilisateur également, la présence de nombreux comptes différents est très contraignante : plusieurs logins, plusieurs mots de passe à changer.

Cela dit, le besoin ne porte pas uniquement sur l'authentification des utilisateurs, mais aussi sur l'ajout de données applicatives propres à chaque utilisateur : groupe VPN, adresses électroniques supplémentaires , etc.

Deux options étaient possibles :

- la première consiste à consulter directement les annuaires d'établissement lorsqu'ils existent ;
- la deuxième consiste à regrouper les données en provenance des annuaires d'établissement dans une base de comptes unique et dédiée aux applications du CRC.

La première option aurait demandé d'imposer à tous les établissements un format d'annuaire utilisable par le CRC, comprenant en particulier les attributs spécifiques de nos applications. De plus, les services que nous proposons auraient été tributaires d'une architecture tierce, n'ayant pas forcément les mêmes objectifs de disponibilité que ceux fixés au CRC (99,9 %) par les instances politiques.

Nous avons donc bâti une base d'authentification centralisée et hébergée au CRC, uniquement accessible en lecture par nos applications, mais alimentée par les différents annuaires d'établissements. Il est bien sûr nécessaire d'intégrer la possibilité de gérer manuellement les comptes, d'une part pour permettre aux établissements sans annuaire propre de profiter du service, et d'autre part pour permettre à tous d'éditer les informations spécifiques de nos applications (groupe VPN, filtres de messagerie; etc.).

La figure 1 présente de manière simplifiée l'architecture générale de l'annuaire Osiris. Au centre de ce schéma figure l'annuaire Osiris. Sur sa gauche figurent les annuaires des

établissements, généralement sous forme d'annuaires LDAP, alimentant l'annuaire Osiris avec des comptes utilisateurs. La possibilité d'intéger des annuaires sous d'autres formes (fichiers csv, base de données) est envisagée, mais le cas ne s'est pas encore présenté. Le CRC met à disposition des correspondants informatiques des établissements une application Web pour gérer manuellement les comptes utilisateurs et les données applicatives. Enfin, à droite de l'annuaire Osiris sont présentées les applications initiales qui y accèderont.

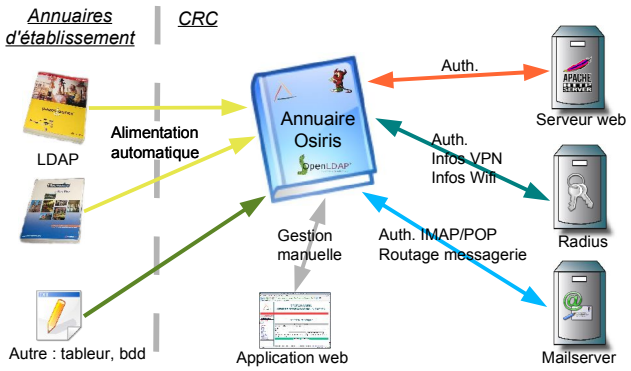

Figure 4 - *Principe de l'annuaire Osiris*

Le protocole LDAP s'est rapidement imposé comme protocole de communication global, pour trois raisons. Tout d'abord, ce protocole est universel : il est indépendant des systèmes d'exploitation ou du codage des informations. Ensuite, ce protocole est, de fait, la norme des annuaires d'établissements, ce qui facilite grandement l'interfaçage. Enfin, l'accès via LDAP est déjà implémenté par de nombreuses applications, et plus particulièrement toutes celles nous concernant.

3.2 Structure générale

La figure 3 présente l'arborescence de l'annuaire Osiris que nous avons définie. Les informations contenues dans chaque branche sont les suivantes :

- « *ou=personnes* »
  C'est dans cette branche que sont stockés les comptes utilisateurs, leurs informations administratives, ainsi que les informations applicatives (groupes sans-fil et vpn, adresses de messagerie...). Ce nœud est lui même subdivisé : il contient une sous-branche par établissement, plus une sous-branche « *ou=autres* » contenant les utilisateurs issus d'une création manuelle ;
- « *ou=profilsWifi* » et « *ou=profilsVPN* »
  Ces branches contiennent respectivement les différents groupes Wifi et VPN, et les informations qui leur sont associées (numéro de Vlan...) ;
- « *ou=aliases* »
  Cette branche applicative contient les aliases de messagerie, typiquement utilisés pour faire des « mini-listes » de diffusion[3] ; ces dernières étant utilisés pour gérer de petites listes de quelques adresses (comme un secrétariat), pour lesquelles une liste « Sympa » serait trop compliquée à gérer ;
- « *ou=domaines* »
  Cette branche contient les différents domaines de messagerie gérés au CRC et, pour chacun, les groupes d'utilisateurs autorisés à les gérer ;
- « *ou=logins-expires* »
  Cette branche contient les enregistrements des utilisateurs supprimés, dans le but de ne pas réutiliser leur logins ou adresses mails.

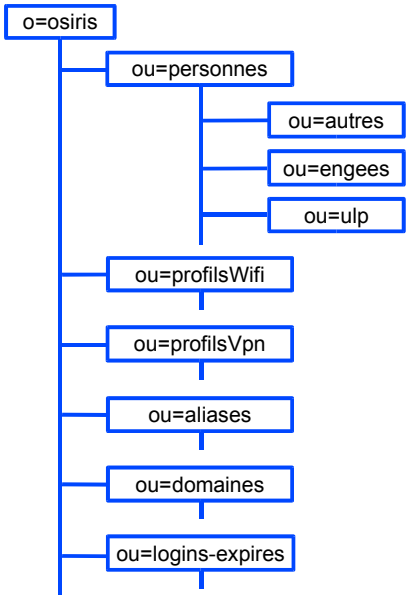

Figure 5 - *Nœuds de l'annuaire Osiris*

Les correspondants de messagerie, (administrateurs réseaux ou autres personnes désignées) sont identifiés par le fait que leur login figure dans un groupe de la base de données du système d'information Osiris [3]. Ils ont ainsi accès, via l'interface Web, à la gestion des comptes de l'annuaire Osiris.

3.3 Alimentation de l'annuaire

Contrairement au choix du protocole de communication, le choix du support de stockage de l'annuaire Osiris était moins évident et a donc donné lieu à une étude plus poussée. En effet, une base de données relationelle (de type PostgreSQL) semblait être un support plus adapté à la gestion d'une base de 50 000 utilisateurs : meilleure stabilité, simplicité de gestion et plus grande puissance expressive de SQL pour des requêtes complexes. Malheureusement, les performances d'un serveur OpenLDAP avec un « backend » de type SQL auraient été bien moindres qu'un classique « BDB », et la complexité résultante aurait posé des problèmes de fiabilité. Nous avons finalement retenu la solution traditionnelle d'un « backend BDB », tout en étant conscients que des difficultés de gestion apparaîtraient avec la croissance du nombre d'utilisateurs.

Pour assurer la mise à jour des données, deux méthodes étaient possibles : récupération des modifications par le CRC, ou envoi des modifications par l'établissement. Pour éviter à l'utilisateur tout désagrément d'authentification, la répercussion des modifications, et en particulier du mot de passe, doit être effectuée en temps réel. Nous avons donc

[3]Les « vraies » listes de diffusion étant bien sûr gérées par Sympa.

privilégié la méthode du « push », c'est à dire une réplication des informations initiée par l'annuaire source.

Une fois le mode de transmission des informations décidé, il restait à gérer ces informations au CRC. Là aussi, deux options étaient possibles : construire un vrai réplicat de l'annuaire d'établissement utilisé ensuite pour mettre à jour l'annuaire Osiris, ou alors utiliser un « backend » de type « perl » ou « tcl » permettant de déclencher des procédures de mise à jour immédiate de l'annuaire Osiris. Après maquettage, nous avons retenu la première solution, qui impose un processus intermédiaire mais qui offre plus de traçabilité, notamment pendant les phases de développement et de mise au point des réplications.

Comme l'illustre la figure 6, l'annuaire réplicat ainsi obtenu (annuaire esclave) est configuré pour générer un fichier de log (appelé « replog ») contenant toutes les modifications envoyées par l'annuaire d'établissement (annuaire maître), au format LDIF. Ce fichier est périodiquement analysé par un démon nommé « *repd* » pour en déduire les répercussions nécessaires sur l'annuaire Osiris.

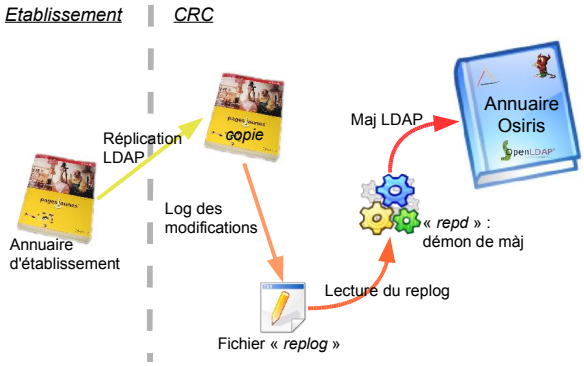

Figure 6 - *Synchronisation avec un annuaire d'établissement*

La figure 7 détaille le fonctionnement du démon « repd » : il découpe le fichier « *replog* » en plusieurs fichiers contenant chacun une seule opération, qui sont ensuite traités un par un. Chaque opération est analysée : type d'opération, type de modification, attributs concernés, etc, puis les modifications s'il y a lieu sont répercutées dans l'annuaire Osiris. Ce peut être une simple mise à jour du même attribut dans l'annuaire Osiris, mais aussi une opération plus complexe comme par exemple la génération d'une nouvelle adresse électronique suite à un changement de nom.

Les annuaires d'établissements n'ont pas forcément la même structure, même s'ils se basent généralement sur le schéma SupAnn. C'est pourquoi chaque instance du démon « *repd* » fait appel à une librairie de fonctions propre à l'établissement, qui permet l'adaptation à la structure de l'annuaire source, de définir des informations particulières à chaque établissement (domaine de messagerie, correspondants réseau autorisés, etc.), mais aussi d'effectuer aussi des actions supplémentaires en fonction des choix politiques de chaque établissement : format de l'adresse électronique, autorisation d'accès VPN, etc. C'est pourquoi nous avons donné à ces librairies le nom de « politiques d'établissements ».

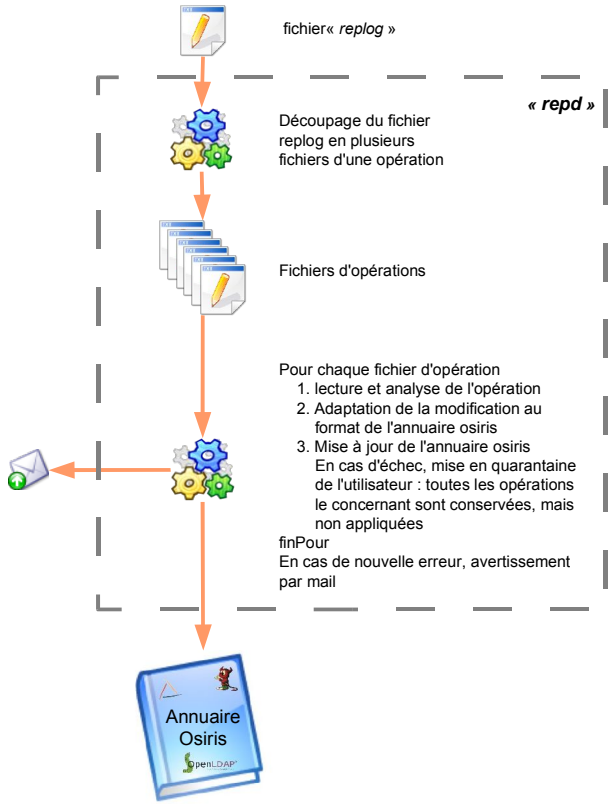

Figure 7 - *Fonctionnement du démon repd*

3.4 Architecture matérielle

L'annuaire Osiris ainsi construit devient la clé de voûte de l'architecture des services offerts par le CRC. Sa fiabilisation, surtout compte-tenu de l'objectif de disponibilité rappelé précédemment, est donc indispensable ; elle est réalisée en rendant l'annaire Osiris redondant : la base LDAP de l'annuaire Osiris est dupliquée, via le mécanisme de réplication d'OpenLDAP, sur un autre serveur.

Afin de rendre rapide et transparent le basculement sur le serveur de secours, nous avons utilisé le protocole CARP[4]. Les deux serveurs possèdent tous deux une interface virtuelle, configurée avec une adresse IP identique « *ldaposiris.u-strasbg.fr* ». Si l'interface CARP du serveur maître ne répond plus, le serveur esclave le détecte et active la sienne. L'adresse « *ldaposiris* » est donc l'adresse utilisée par toutes les applications accédant en lecture à l'annuaire. Les services s'appuyant sur l'annuaire Osiris ne sont donc pas impactés par une panne du serveur principal, hormis les connexions LDAP déjà entamées bien sûr.

En revanche, les tentatives d'écriture dans l'annuaire se feront non pas sur l'adresse virtuelle, mais sur l'adresse réelle du serveur primaire, car la réplication est unidirectionnelle : le serveur maître transmet les modifications à ses esclaves. Dans notre cas, lors du passage sur le serveur esclave, les modifications de l'annuaire LDAP ne sont donc plus possibles. Ce mode de fonctionnement est

[4]http://www.openbsd.org/faq/pf/carp.html

donc légèrement dégradé, mais reste supportable : tous les services d'authentification continuent de fonctionner, et il n'y a aucune perte d'information en provenance des annuaires d'établissement.

L'annuaire Osiris, ainsi que les réplicats des annuaires d'établissement, sont hébergés sur un serveur sous FreeBSD avec 2 Go de mémoire. Ce serveur supporte également toutes les instances du démon « repd », avec les politiques d'établissement associées, ainsi que tous les scripts de maintenance de l'annuaire (expiration des comptes, vérification de la cohérence des réplicats, etc.). Le serveur de secours, dans la même configuration matérielle et logicielle, ne supporte quant à lui que le réplicat de l'annuaire Osiris.

4 Intégration des services

Cette section décrit la mise en œuvre de l'annuaire Osiris dans les différents services proposés par le CRC.

4.1 Authentification radius : VPN & sans-fil

Les accès VPN et réseau sans-fil sont tous deux authentifiés via un serveur Radius, qui doit bien évidemment puiser ses données dans l'annuaire Osiris. Les deux types d'accès sont très proches au niveau du principe.

Le schéma de l'annuaire contient deux attributs (radiusProfileWifi et radiusProfileVpn) qui contrôlent l'accès aux ressources correspondantes. L'absence d'un attribut interdit l'accès à la ressource au titulaire du compte. Si cet attribut est présent, il indique le DN du profil attribué à ce compte (dans la branche « ou=profilsWifi » ou « ou=profilsVpn »), ce qui permet par exemple aux utilisateurs de VPN-Lab ou VPN-Lab+ d'arriver dans leur sous-réseau.

Le serveur Radius devient lui aussi un élément critique de l'infrastructure d'authentification. C'est la raison pour laquelle il a été dédoublé, et la redondance est assurée de manière transparente pour les clients Radius (en particulier ceux qui sont hébergés dans les points d'accès et dans le serveur VPN) grâce au protocole CARP.

4.2 Hébergement des boîtes aux lettres

L'interfaçage de la messagerie avec le protocole LDAP est sans doute le service qui a demandé le plus d'efforts. L'acheminement des messages et la lecture de ces derniers par l'utilisateur nécessitent plusieurs applicatifs. La première étape est le routage de messagerie, effectué ici par *Sendmail*, qui a pour but d'acheminer le courrier vers le bon utilisateur. C'est ensuite l'agent de remise local, *Maildrop*, qui prend le relais pour déposer le courrier dans la boîte adéquate. Enfin, *Courier-imap* met les messages à disposition de l'utilisateur.

Routage de messagerie : Sendmail

Toutes les informations nécessaires au routage de messagerie pour les boîtes aux lettres hébergées au CRC sont contenues dans l'annuaire Osiris. Sendmail effectue donc des requêtes LDAP pour obtenir le login en fonction de l'adresse électronique. Les messages sont ensuite transmis à l'agent de dépôt local.

Pour répondre au besoins de routage, chaque compte utilisateur peut comporter les informations suivantes :

- *« canonicalAddress »* : adresse électronique principale de l'utilisateur ;
- « *alternateAddress* » : adresse électronique secondaire (attribut multivalué) ;
- « *forwardAddress* » : adresse de transfert de messagerie (attribut multivalué).

Les « aliases », stockés dans la branche du même nom de l'annuaire LDAP, sont en fait constitués d'une succession de forwardAddress. Il sont analogues au fichier des aliases de sendmail.

Dépôt local : maildrop

L'agent de dépôt local reçoit en paramètre de la part de sendmail un courrier à remettre ainsi que le destinaire sous la forme du login. Il interroge l'annuaire Osiris pour récupérer les quotas et le répertoire des boîtes aux lettres de l'utilisateur. Le courrier est alors déposé dans la boîte aux lettres, au format Maildir, si les quotas ne sont pas atteints.

Les attributs applicatifs supplémentaires nécessaires pour l'application sont donc :

- « *quotas* » : espace disque alloué à l'utilisateur ;
- « *mailDirectory* » : répertoire spécifique de l'utilisateur sur le serveur de messagerie, contenant la boîte aux lettres et diverses informations tels que les filtres.

Authentification et lecture des messages : Courier-imap

Courier-imap interroge l'annuaire Osiris pour authentifier l'utilisateur et pour obtenir le répertoire de l'utilisateur.

L'attribut mailFilter

Les nouvelles fonctionnalités offertes par l'hébergement de la messagerie au CRC sont :

- le transfert vers une autre adresse ;
- le répondeur simple ou répondeur enregistreur ;
- le filtrage anti-spam.

Chaque utilisateur peut gérer ces fonctionnalités via une interface Web simple d'emploi.

Notre souhait étant de centraliser toutes les informations applicatives dans l'annuaire, nous avons donc créé un attribut « *mailFilter* » pour regrouper les paramètrages de ces options de messagerie. Ils sont d'un niveau d'abstraction supérieur à ce qui est utilisé directement par les agents de messagerie, dans le double but de les rendre facilement éditables via l'interface Web et de pouvoir changer de logiciels sous-jacents si le besoin s'en fait sentir dans le futur.

Aujoud'hui, cet attribut multivalué peut prendre les valeurs suivantes :

- `forward` *adresse-de-destination*

– `vacation` *message*

– `localdelivery`

– `spam`

Il est prévu d'enrichir ce format à l'avenir pour mettre à la disposition des utilisateurs une interface de gestion de filtres sur le serveur.

Les informations sont interprétées par un démon (présenté ci-dessous), qui actualise la configuration du serveur de messagerie en fonction des données de l'annuaire Osiris.

Synchronisation du serveur de messagerie

La manipulation des comptes des utilisateurs est effectuée via l'annuaire LDAP. Cependant, de nombreuses actions doivent être effectuées sur le serveur d'hébergement des boîtes aux lettres.

Dans un système classique, comme celui qui existait auparavant, la création d'un compte passe par l'édition plus ou moins automatique de fichiers comme `passwd`, `aliases`, `revaliases`, etc. Le passage à l'annuaire LDAP a permis d'éliminer ces fichiers : les aliases et les revaliases sont remplacés par une consultation LDAP directe par sendmail, et toutes les boîtes aux lettres appartiennent à un utilisateur unique (le facteur), les utilisateurs n'ayant pas de compte Unix sur le serveur d'hébergement. Il reste toutefois des actions à effectuer dans le système de fichiers du serveur de messagerie :

– création du répertoire spécifique par utilisateur, comprenant à la fois la configuration de messagerie de cet utilisateur (filtres, répondeur, etc.) et la boîte aux lettres (répertoire Maildir et descendance) ;

– constitution des filtres et répondeurs suite à une modification dans l'annuaire LDAP ;

– archivage et suppression des comptes.

Le démon « *monitorldap* », dont l'algorithme est détaillé en figure 8, gère les répercussions de l'annuaire LDAP vers le serveur de messagerie. À intervalles réguliers, « *monitorldap* » recherche les comptes de messagerie de l'annuaire Osiris récemment modifiés. Pour chaque compte modifié, il vérifie l'existence du répertoire spécifique du compte et le crée si nécessaire. Le programme génère ensuite la configuration des options de messagerie : un fichier « .mailfilter » (utilisé par maildrop) est généré pour le répondeur et l'anti-spam, et l'attribut multivalué « *forwardAddress* » est mis à jour dans l'annuaire Osiris pour un transfert. La date de vérification est sauvegardée dans un fichier, pour servir en cas de redémarrage du démon.

La disponibilité du démon « *monitorldap* » a représenté une très grande simplification du dispositif : en effet, la création d'un compte de messagerie suppose maintenant uniquement l'ajout d'une entrée dans l'annuaire LDAP. Le reste, c'est à dire la création effective des informations sur le serveur d'hébergement des boîtes, est fait automatiquement, et de manière asynchrone. C'est, pour nous, un fardeau en moins.

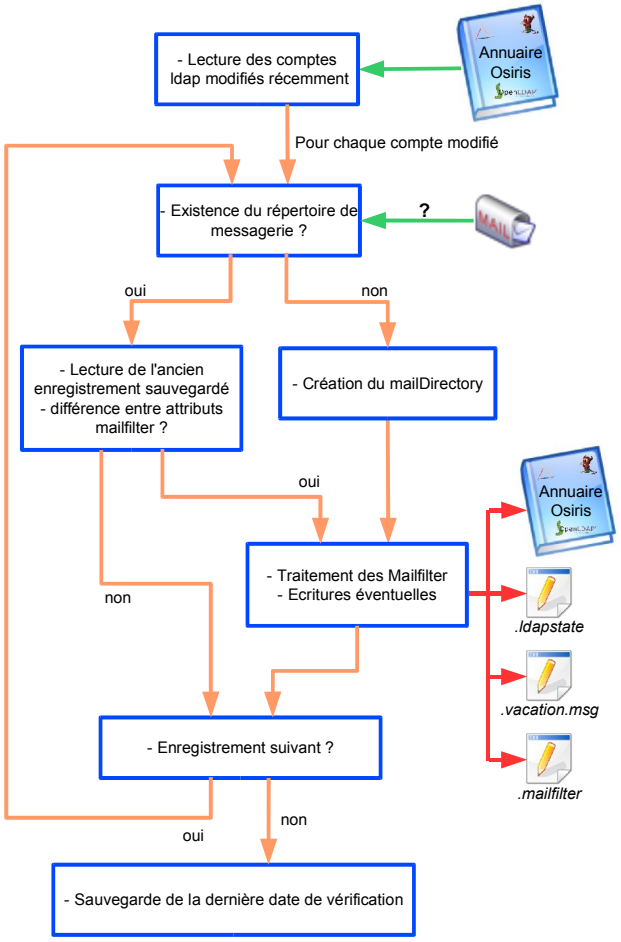

Figure 8 - *Fonctionnement de monitorldap*

De manière symétrique, le script « expiremboxes » surveille l'annuaire LDAP pour y détecter les comptes dont la date d'archivage est atteinte, et archive dans ce cas la boîte dans un répertoire spécifique accessible seulement aux administrateurs de la messagerie. Ce script détruit également les boîtes des comptes archivés, ou des comptes ayant disparu de l'annuaire.

4.3 Authiris

La mise en place du l'annuaire Osiris a permis de développer une nouvelle interface de gestion des comptes pour nos correspondants réseau et nos utilisateurs. L'application « Authiris » est une interface Web dont l'accès est bien sûr authentifié sur l'annuaire Osiris. Elle permet la gestion des données des utilisateurs, qu'elles soient informatives (adresse, téléphone...) ou applicatives (groupes VPN, options de messagerie). Il est aussi possible de gérer les mini-listes de diffusion (les listes de diffusion étant gérées par WWSympa).

Suivant leur profil, certains utilisateurs ont la possibilité de modifier leur mot de passe (typiquement ceux dont le compte ne provient pas d'un annuaire d'établissement), et ceux dont la boîte aux lettres est hébergée au CRC peuvent paramètrer leur boîte (transfert, répondeur et anti-spam).

Les correspondants réseau ont les mêmes possibilités. Ils peuvent de plus éditer les comptes des utilisateurs dont ils ont la responsabilité, par l'intermédiaire d'un formulaire de recherche, et en modifier les paramètres : réinitialisation du mot de passe, configuration des accès VPN et sans-fil, paramétrage de la messagerie (adresses secondaires, répondeur...). Les correspondants ont également la possibilité de gérer les mini-listes des domaines les concernant.

5 Migrations et bilan

Le passage à l'authentification unifiée que nous avons présentée apparaît aujourd'hui comme une évidence. C'est pourtant le résultat d'un long projet de migration, dont la caractéristique est qu'elle devait être transparente pour les utilisateurs. Cette section décrit le projet de migration, ainsi que le premier bilan que nous pouvons dresser à l'issue de la mise en production en vraie grandeur.

5.1 Les migrations

Lorsque les projets de développement des services VPN et réseau sans-fil ont débuté, le serveur de messagerie fournissait l'hébergement pour environ 2 700 boîtes aux lettres. Le système d'authentification de ce dernier reposait sur des fichiers traditionnels Unix. Tout naturellement, l'authentification des services VPN et réseau sans-fil s'est faite dans un premier temps sur des bases d'authentification autonomes. Lorsque le développement des nouveaux services fut suffisamment avancé pour connaître les besoins en terme d'annuaire, nous avons adopté une démarche de migration progressive :

- phase 0 : cette phase correspond à l'état initial décrit ci-dessus. L'authentification des accès réseau est réalisée par des fichiers « plats », et la messagerie reposait sur les fichiers « passwd », « aliases », etc. ; de plus, une ancienne application Web de gestion des comptes utilisait un fichier « passwd » spécifique pour Apache.
- phase 1 : cette phase correspond à la mise en place de la première version de l'annuaire Osiris, le 3 mars 2005, alors consulté pour les accès VPN et réseau sans-fil. Les étudiants n'étant pas encore dans cet annuaire, l'authentification de ceux-ci est réalisée via un annuaire tiers (hébergé dans un autre service). De plus, la création d'un compte de messagerie (qui se fait toujours par l'intermédiaire des fichiers « passwd », « aliases », etc.) implique la création d'une entrée dans l'annuaire Osiris, donnant ainsi l'accès au VPN et au réseau sans-fil ;
- phase 2 : cette phase a débuté le 8 juillet 2005, lors du basculement vers le nouveau serveur de messagerie, qui a entraîné le basculement de l'authentification ainsi que du routage via l'annuaire Osiris. Cette phase a permis la mise en service de l'application Authiris.
- phase 3 : toutes les applications utilisant maintenant l'annuaire Osiris, la synchronisation de celui-ci via les annuaires d'établissements est progressivement mise en place à partir du 12 septembre 2005 ; cette synchronisation a constitué le point de départ de l'hébergement des boîtes aux lettres des étudiants des 3 universités et des écoles d'ingénieurs.

5.2 Bilan d'exploitation

À l'heure actuelle, 4 annuaires sources sont répliqués, représentant 6 établissements (un des annuaires source comprend les 3 universités). Au total, les services authentifiés concernent à l'heure où nous rédigeons ces lignes 73 697 utilisateurs pour la messagerie et l'accès réseau sans-fil ; les accès VPN étant restreints aux personnels des établissements et aux doctorants, ils ne concernent que 5 615 utilisateurs.

Bien que la montée en charge de l'annuaire Osiris soit relativement récente, il a fallu affiner les réglages du serveur LDAP pour faire face au surcroît de requêtes.

Par ailleurs, comme nous le craignons, le dispositif de stockage d'OpenLDAP manque de souplesse pour la taille de la population concernée, les requêtes complexes sont beaucoup plus difficiles à spécifier qu'avec SQL, il n'y a pas de contraintes d'intégrité, et les opérations réalisables sont de trop bas niveau, manquant par exemple de transactions. Le changement du dispositif de stockage est une des pistes que nous allons devoir creuser.

Du côté positif, la faculté d'avoir une gestion de compte unifiée, ainsi que l'interface Web « Authiris », ont largement simplifié les tâches quotidiennes d'administration. La délégation de la gestion vers les correspondants réseau a également éliminé une charge de travail fastidieuse et sans valeur ajoutée de la part du CRC.

Enfin, la synchronisation de l'annuaire Osiris par les annuaires d'établissement se révèle très pratique et efficace. Même si elle reste relativement sensible, car certaines suites d'opérations LDAP (modrdn par exemple) peuvent provoquer des incohérences heureusement limitées, il s'agit d'un mécanisme indispensable pour gérer de grandes populations d'utilisateurs à partir de sources diverses. Les « politiques d'établissement » écrites peuvent être améliorées pour tenir compte de plus de cas afin d'éliminer totalement les problèmes posés par certaines opérations LDAP.

6 Conclusion

Le CRC offre à présent de nouveaux services à l'ensemble des utilisateurs de la communauté strasbourgeoise de l'Enseignement Supérieur et de la Recherche.

Les premiers bilans de la mise en exploitation sont très encourageants. Le nombre d'utilisateurs intéressés par les nouveaux services proposés (accès VPN leur permettant d'accéder aux ressources de leur laboratoire, ou accès au réseau sans-fil sans contrainte de frontière de bâtiment ou d'établissement) ne fait que croître.

La population concernée étant très importante, nous avons apporté un soin particulier à la fiabilité des dispositifs proposés, mais également à l'automatisation de la gestion d'une telle population, répartie dans plusieurs établissements. Notre démarche a consisté à intégrer les annuaires et les Environnements Numériques de Travail des

établissements, lorsqu'ils existent, tout en s'adaptant aux spécificités de chacun d'entre eux..

Les étapes les plus difficiles ont été effectuées, comme la conception de l'annuaire, les migrations successives, etc. Un tel projet n'étant par nature jamais terminé, il reste des actions à mener.

Tout d'abord, un certains nombre d'applications Web utilisent encore l'ancienne base d'authentification. L'utilisation de l'annuaire Osiris va donc demander le redéveloppement du module d'authentification commun à ces applications.

Ensuite, plusieurs fonctionnalités doivent être encore ajoutées à l'application Authiris comme la création des mini-listes de diffusion ou de comptes génériques à durée déterminée pour les invités ou les conférences. Sur le plan de la messagerie, la prochaine étape est la création d'un système de filtrage fin offrant à chaque utilisateur la possibilité de spécifier des filtres de messagerie interprétés par le serveur de messagerie.

Enfin, l'intégration du dispositif CAS de SSO (Single Sign-On) compatible avec les environnements numériques de travail a été momentanément repoussée compte-tenu des délais impératifs posés par une rentrée universitaire avancée pour prendre en compte le LMD. L'intégration des certificats compatibles avec ceux du CNRS est également prévue.

Le lecteur a pu se rendre compte du caractère collectif de la démarche retracée ici. La richesse des services offerts et leur mise en exploitation opérationnelle pour une telle population en un délai aussi court n'ont été rendus possibles que grâce à la motivation d'une équipe soudée autour de ce projet.

Bibliographie

[1] L. Saccavini. 802.1X et sécurisation de l'accès au réseau local. JRES 2003.

[2] C. Saillard. 802.1X : Solution d'authentification sécurisée pour le futur réseau sans fil de l'Université Louis Pasteur. JRES 2003.

[3] P. David, J. Benoit. Le système d'information Osiris : de la fibre optique jusqu'aux services. JRES 2005.

[4] P. Pegon. Un exemple de généralisation opérationnelle à grande échelle d'IPv6 sur un réseau métropolitain. JRES 2005