



CAHIER DES CHARGES TECHNIQUES

L'intégration de l'annuaire OpenLDAP avec Samba/Free Radius/Postfix

SEVRES - FRANCE

B.I.P.M.

Pavillon de Breteuil
92312 Sèvres
FRANCE



TABLE DES MATIERES

1	Introduction	3
1.1	Contexte	3
1.2	Organisation du document	3
2	Le BIPM.....	3
2.1	Activités	3
2.2	Le système d'information du BIPM.....	3
3	Description du système actuel.....	5
3.1	SAMBA.....	5
3.2	Serveur MTA : postfix	5
3.2.1	Réception des messages	5
3.2.2	Emission des messages.....	5
3.2.3	Vacancy.....	5
3.2.4	Forward	5
3.3	Serveur MDA : Qpopper	6
3.4	Serveur AAA : Freeradius.....	6
4	Description des besoins	7
4.1	OpenLDAP.....	7
4.2	Samba	7
4.3	Postfix.....	7
4.4	FreeRadius.....	7
5	Travail demandé.....	8
5.1	OpenLDAP.....	8
5.2	Samba	8
5.3	FreeRadius.....	8
5.4	Postfix/pop3	8
6	Organisation de l'intégration et transfert de compétences	9
7	Maintenance	9



1 Introduction

1.1 Contexte

Le BIPM souhaite procéder à la réalisation de l'intégration de l'annuaire openLDAP avec les toutes dernières versions de Samba/Free Radius/Postfix et d'un logiciel assurant le service de POP3.

1.2 Organisation du document

Après une courte description du BIPM, nous étudierons son système de communication mis en place au BIPM, à travers ses réseaux locaux et son accès à Internet. Nous préciserons ensuite les besoins fonctionnels et techniques.

2 Le BIPM

2.1 Activités

Le BIPM est une organisation intergouvernementale qui a pour mission d'assurer l'uniformité mondiale des mesures et de leur traçabilité au Système international d'unités (SI).

Son traité constitutif est la Convention du Mètre, qui est un traité auquel sont parties cinquante et quatre Etats. Il exerce son activité par son travail de laboratoire et avec l'aide d'un certain nombre de Comités consultatifs, dont les membres sont des laboratoires nationaux de métrologie des États membres de la Convention du Mètre.

Le BIPM effectue des recherches liées à la métrologie. Il organise ou participe à des comparaisons internationales d'étalons nationaux de mesure et effectue des étalonnages pour les États membres.

Le BIPM entretient des relations étroites avec d'autres organisations internationales telles que l'Agence internationale de l'énergie atomique (AIEA), l'International Laboratory Accreditation Cooperation (ILAC), l'Organisation internationale de normalisation (ISO), l'Organisation mondiale de la santé (OMS), l'Organisation météorologique mondiale (OMM).

2.2 Le système d'information du BIPM

La cellule informatique du BIPM gère l'ensemble des outils informatiques et réseaux mis à la disposition du personnel (serveurs, centre de calcul, postes de travail, sécurité, réseaux), contribue aux développements d'application Intranet/Internet (avec ou sans partenaire externe), et agit en tant que coordinateur et/ou réalisateur de projets de collaborations internationales. Elle est composée d'un responsable fonctionnel et technique et d'un ingénieur système/réseau.

Le parc informatique est constitué :

- d'un serveur de données équipé du système d'exploitation Sun/Sparc/Solaris 9 (serveur Samba/Postfix/Free Radius) ;
- d'un système de stockage en réseau Netapp ;
- d'un serveur de sauvegarde équipé du système d'exploitation Sun/Solaris ;
- d'un serveur de clients légers ;
- de deux serveurs de bases de données équipés du système d'exploitation Windows 2003 ;
- de multiples serveurs applicatifs sous Linux et Windows.



Les postes clients sont équipés du système d'exploitation Windows (2000 et XP) et sont au nombre de 170 (80 ordinateurs de bureau, 30 portables et 60 de laboratoires).

Un centre de calcul est à disposition des utilisateurs de l'Organisation et est constitué de douze serveurs sous Linux.

Une plateforme de pré-production est disponible et contient une image du serveur SUN synchronisée mensuellement.



3 Description du système actuel

3.1 SAMBA

Le logiciel SAMBA assure le service de partage de fichiers et de gestion de noms à travers les processus `smbd` et `nmbd` pour le domaine BIPM.ORG. La version 3.0.10 a été installée en 2005 et sert aujourd'hui une centaine de connexion d'ordinateurs de bureau sous Windows XP. La gestion des comptes et des mots de passe est effectuée à travers le fichier `smbpasswd` et les fichiers Unix du serveur SI (`/etc/passwd`, `/etc/group`, `/etc/shadow`) qui servent donc de base de comptes.

3.2 Serveur MTA : postfix

Le serveur MTA est le logiciel postfix dans sa version 2.0.18. Il est hébergé sur un serveur SUN V880 sous Solaris 9. Les messages reçus sont stockés au format Mbox dans le répertoire `/var/mail` du serveur `si.bipm.org`). Aucun système de filtre antispam n'est installé. Seuls des règles d'anti-relaying ont été définies, ce serveur n'étant pas directement atteignable depuis l'Internet.

La base d'authentification de la centaine d'utilisateurs du BIPM est le fichier `/etc/passwd` du serveur `si.bipm.org` et les alias au nombre d'une centaine sont définis dans le fichier `/etc/aliases`.

3.2.1 Réception des messages

Les messages à destination du domaine `bipm.org` sont envoyés aux passerelles IronPort (situés en DMZ) pour un filtre RBS, anti-spam, anti-virus et à travers des règles définies par la cellule informatique du BIPM. Seuls les accès SMTP à destination de ces passerelles sont autorisés au niveau de nos pare-feux. Une fois les messages validés par ces passerelles, ils sont redirigés vers le serveur MTA postfix sur `si.bipm.org`.

3.2.2 Emission des messages

Seuls les clients des réseaux LAN gérés par la cellule informatique (INTRANET, clients VPN, ...) peuvent envoyer leurs messages via le protocole SMTP au serveur `si.bipm.org` sans authentification de l'utilisateur. Aucun filtre en sortie n'est appliqué aux messages sortants (pas d'ajout de *disclaimer* par exemple). Le serveur MTA sur `si.bipm.org` assure la gestion des messages sortants.

3.2.3 Vacancy

Une interface Web permet d'activer la fonctionnalité d'envoi d'un message automatique informant de l'absence de l'utilisateur (fonction vacation sous Unix).

3.2.4 Forward

Une interface Web permet d'activer la fonctionnalité de renvoi des messages à destination d'une adresse vers une ou plusieurs adresses internes ou externes.



3.3 Serveur MDA : Qpopper

Le serveur MDA utilisé par les clients MUA du BIPM est le logiciel Qpopper dans sa version 4.0.5. Il est hébergé sur le serveur si.bipm.org Les clients accèdent selon le protocole POP3 dans sa version non sécurisée au serveur POP.

Une liste d'alias (/etc/aliases) est disponible sur le serveur MTA.

3.4 Serveur AAA : Freeradius

Le logiciel Freeradius dans sa version 1.1.7 assure les services AAA pour les connexions VPN et pour des applications Web « maisons ». Il s'appuie sur la base de compte et de mot de passe du serveur SI.



4 Description des besoins

4.1 OpenLDAP

Le BIPM souhaite disposer d'un annuaire électronique d'entreprise OpenLDAP (2.4.X) permettant de centraliser l'ensemble des informations relatives à ces utilisateurs (nom, prénom, mot de passe, compte e-mail, alias, ...). L'ensemble des logiciels (samba, postfix/pop, freeRadius) s'appuiera sur cet annuaire pour l'authentification des utilisateurs du BIPM.

Le schéma LDAP à intégrer comprendra des informations standard héritées de la précédente gestion de compte (nom, login, password, aliases, groupes,...). Ce schéma devra être évolutif pour pouvoir intégrer d'autres informations (fax, mobile,...) mais aussi les informations propres à Samba, Postfix et FreeRadius.

4.2 Samba

Le BIPM souhaite intégrer de la version de SAMBA supportant Windows XP et Windows 7 ainsi que la gestion des authentifications et des droits via le serveur OpenLDAP.

4.3 Postfix

Le logiciel Postfix et son pendant pop3 (pop et spop) devront utiliser l'annuaire OpenLDAP pour l'émission et la réception des messages.

4.4 FreeRadius

Le service d'authentification du serveur Radius devra s'appuyer sur l'annuaire openLDAP.



5 Travail demandé

Le prestataire choisi devra répondre à l'ensemble des besoins indiqués ci-dessus en s'assurant pour chaque élément de l'architecture du BIPM :

5.1 OpenLDAP

- De la fiabilité de la solution (sécurisation du serveur LDAP, réplication, sauvegarde) ;
- De la migration de l'ensemble des données des comptes utilisateurs du BIPM vers l'annuaire ;
- De la possibilité d'intégrer un schéma pour une messagerie collaborative (type Zimbra ou équivalent) ;
- De la mise à disposition d'une interface intuitive et personnalisable en fonction des rôles du BIPM (cellule informatique ; Ressources humaines, utilisateurs, etc.) de gestion de l'annuaire.

5.2 Samba

- Que l'ensemble des systèmes Windows du BIPM soit correctement géré par le service de partage de fichiers avec reprise de l'existant ;
- Que l'ensemble des groupes du BIPM associés à l'utilisateur soit correctement géré ;
- Que l'utilisateur du BIPM puisse mettre à jour son mot de passe via l'interface Windows.

5.3 FreeRadius

- Que le processus d'authentification réponde correctement aux demandes effectuées par les NAS du BIPM.

5.4 Postfix/pop3

- Que l'ensemble des informations relatives à la gestion des e-mails (alias, groupes) soient correctement gérées par l'annuaire ;
- De la possibilité d'ajouter un « disclaimer » pour chaque message émis par le serveur Postfix du BIPM.



6 Organisation de l'intégration et transfert de compétences

La mission devra être réalisée sur site afin d'effectuer un transfert de compétence tout au long de la mission. Une plateforme de pré-production est à disposition. Elle comprend un serveur SUN UE450 sous Solaris 9 dont le système d'exploitation est une copie du serveur de production SI et des clients sous Windows XP, Windows 7 et un serveur sous Linux Redat peut être installé si besoin est.

Le prestataire devra procéder à la mise en production de l'ensemble de l'architecture logicielle après validation par le BIPM de son bon fonctionnement sur la plateforme de pré-production. Cette recette fera l'objet d'un document de couverture de tests permettant lors de la mise en production d'effectuer des tests de bon fonctionnement.

Lors de cette mise en production, le temps d'indisponibilité des services associés (partage de fichiers, messagerie, authentification) ne devra pas excéder la demi-journée. Un arrêt/redémarrage du serveur SUN sera aussi planifié afin de tester la procédure de démarrage de l'ensemble des logiciels.

Il est demandé au prestataire de rédiger un plan de migration avant la mise en production ainsi que tous documents et scripts nécessaires à l'administration et à la gestion de la solution.

7 Maintenance

Le prestataire devra proposer une maintenance de 6 mois après l'intégration.

* * *