Mandriva Directory Server : une gestion collaborative d'annuaire

François Clémence
Centre de Ressources Informatiques - Université Paul Verlaine - Metz
UFR Sciences Humaines & Arts
Ile du Saulcy, BP 30309, 57006 METZ cedex 1

Résumé

Nous connaissons tous la société Mandriva dont la nouvelle distribution *Mandriva 2011*, est sortie cet été. Cette société édite également des solutions de gestion de parcs informatiques. Nous allons détailler dans cette présentation le logiciel libre *Mandriva Directory Server* (MDS).

L'objectif de ce système est ambitieux : fournir une solution complète de gestion d'annuaire facile à exploiter. *Mandriva Directory Server* permet une gestion des identités des utilisateurs, de l'administration du service d'annuaire et du pilotage des services réseaux.

MDS est conçu de façon modulaire et s'articule autour d'un annuaire OpenLDAP. Chaque module activé fournit des fonctionnalités supplémentaires à l'interface centrale. Cette dernière est accessible en ligne, avec un simple navigateur Web. Dans un premier temps, nous détaillerons donc le fonctionnement de ce système.

Dans un second temps, nous ferons un retour d'expérience sur cette solution que nous avons adoptée pour gérer une structure de plus de 25 salles informatiques, 80 postes fixes administratifs et plus de 6000 comptes utilisateurs.

Mots clefs

OpenLDAP, parcs hétérogènes, travail collaboratif, samba, gestion d'identités, infrastructure informatique

1 Introduction

L'entreprise Mandriva est un acteur majeur dans le monde libre et son dernier système d'exploitation *Mandriva 2011* est sorti il y quelques mois. Elle édite également diverses solutions de gestion de parcs informatiques comme *Pulse 2* et *Mandriva Directory Server* (MDS) [1]. C'est cette dernière que nous allons présenter ici.

Anciennement connu sous le nom *Linbox Directory Server*, le projet a changé d'appellation en 2007, après le rachat de Linbox par Mandriva. La finalité du produit n'a pas varié depuis son origine : gérer efficacement les comptes des utilisateurs et administrer de façon collaborative les parcs informatiques hétérogènes. Destinées avant tout aux petites et moyennes entreprises, ces multiples fonctionnalités s'intègrent-elles bien dans notre environnement de travail universitaire ?

2 MDS : vue d'ensemble

Nous allons présenter tout d'abord le logiciel puis son fonctionnement.

2.1 Fonctionnalités

Mandriva Directory Server se propose d'intégrer tous les aspects de la gestion d'annuaire OpenLDAP dans une seule interface Web. Elle couvre la création, le suivi et l'authentification des usagers, la définition d'une politique de sécurité, ainsi que l'intégration de services réseaux comme DHCP, DNS et Postfix. Afin de fournir un logiciel s'adaptant à tous les contextes d'exploitation, chaque fonction est proposée sous la forme d'un module à activer. L'administrateur peut donc déployer une solution répondant véritablement à ses besoins, tout en préservant l'infrastructure précédemment mise en place.

De nombreuses options sont déjà disponibles, développées par l'équipe MDS ou par la communauté [2]:

- Module Base : c'est le composant principal du produit. Il communique directement avec l'annuaire et va permettre la création et la gestion des identités, des groupes, ainsi que l'authentification des usagers. Nous pouvons également y définir une politique de gestion des mots de passe des utilisateurs, que ce soit pour les systèmes Linux ou les domaines Windows avec Samba. Enfin, nous avons la possibilité d'activer un mode d'audit qui s'appuie sur une base MySql. Tous les changements effectués par les administrateurs de *Mandriva Directory Server* seront alors affichés dans l'interface.
- Module Quotas : il permet de fixer les quotas des disques pour les utilisateurs ou les groupes. Ces informations sont stockées dans l'annuaire.
- Module Import CVS : on peut ajouter ou mettre à jour massivement la liste des comptes des usagers.
- Module Samba : ce module est intéressant car il offre aux postes Windows des fonctionnalités de partages de ressources et d'authentification. Une fois Samba correctement configuré et cette option paramétrée, nous disposons d'un domaine du type contrôleur de domaine primaire Windows, nous permettant de gérer des postes informatiques dans un environnement hétérogène Windows/Linux/Mac. L'interface d'administration va nous permettre d'agir directement sur les réglages Samba, de définir des partages de documents et de gérer les différents types de comptes.
- Module Messagerie : MDS peut être couplé à un système de messagerie comme Postfix. Il va s'appuyer sur la partie Base pour communiquer avec l'annuaire, délivrer correctement les messages et identifier les utilisateurs.
- Module Réseau : cette fonctionnalité est particulièrement utile car elle permet de stocker la configuration et les enregistrements des services DHCP et DNS directement dans l'annuaire. On peut donc accéder facilement à la déclaration des zones DNS et aux entrées s'y rapportant ainsi qu'aux sous réseaux DHCP, aux plages d'adresses dynamiques et aux réservations des hôtes.
- Modules Clefs SSH : ce service permet de gérer la liste des clefs publiques des utilisateurs. Il communique avec le composant Base pour dialoguer avec OpenLDAP.

2.2 Fonctionnement

La clef de voûte de MDS est un annuaire OpenLDAP. Il va stocker toutes les informations relatives aux identités et aux services utilisés.

L'interface du produit s'appelle Mandriva Management Console (MMC). C'est le chef d'orchestre de l'application. Elle est formée de deux parties :

- Un agent « MMC Agent » qu'on va mettre en place sur un ou plusieurs serveurs. Grâce à lui, on va pouvoir interroger les modules (développés en Python) qui sont installés localement. On peut par exemple imaginer un serveur dédié à la messagerie et intégrer un MMC Agent avec le module de messagerie. En parallèle une machine différente pourvue d'un autre MMC Agent et de modules adaptés, serait déployée pour héberger les autres fonctionnalités.
- Une interface Web « MMC Web Interface » qui se connecte aux multiples agents en utilisant XML-RPC. L'interface est écrite en PHP et intègre Ajax pour améliorer la navigation. La figure 1, inspirée du site officiel de Mandriva, illustre le fonctionnement du programme.

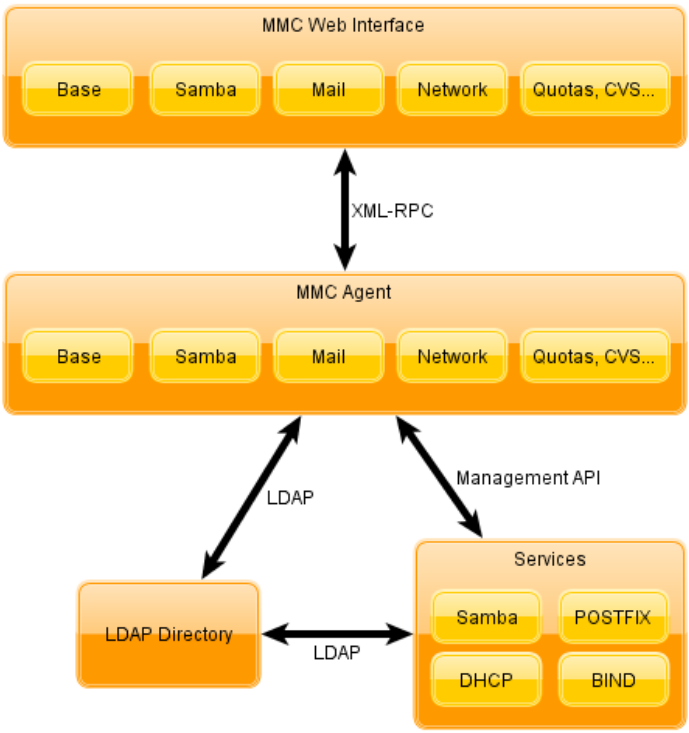

Figure 1 - *Architecture de Mandriva Directory Server avec un unique MMC Agent*

Après cette vue d'ensemble du produit, nous allons vous faire partager notre retour d'expérience.

3 Notre utilisation de MDS à Metz

Nous parlerons du déploiement du logiciel dans cette partie puis de son intégration dans un environnement universitaire.

3.1 Installation

La dernière version en date, la 2.4.2 est facilement accessible :

- Elle est incorporée à *Mandriva Entreprise Server 5*, la distribution orientée serveurs
- Elle est également disponible dans *Pulse 2*, la solution complète de gestion de parcs informatiques de Mandriva
- Les sources et des paquets .rpm et .deb sont téléchargeables sur le site officiel : http://mds.mandriva.org

Un assistant d'installation est disponible pour les deux premières alternatives et permet de mettre en production rapidement l'annuaire OpenLDAP ainsi que MDS et ses options. Une image virtuelle est aussi disponible afin de tester le programme [3].

Si l'on télécharge les sources ou les paquets sur une distribution autre que Mandriva, la mise en place est plus ardue. En effet, il faut s'assurer au préalable du bon paramétrage d'OpenLDAP et importer les schémas nécessaires au fonctionnement des modules. De même, une bonne configuration de Samba est critique avant d'installer les paquets de Mandriva. Une fois le déploiement terminé et le site Apache créé, on se connecte simplement à l'interface « MMC Web Interface » en HTTPS.

3.2 Retour d'expérience

Quelques chiffres tout d'abord : notre cellule informatique comprend quatre techniciens et un ingénieur d'études. Elle gère 800 postes dont 25 salles pédagogiques, 80 ordinateurs administratifs, répartis sur deux sites. Notre portion d'annuaire compte plus de 6000 entrées d'utilisateurs, étudiants, enseignants ou intervenants, alimentées par un système central.

Pour gérer ce parc informatique, nous avions installé dès l'origine un domaine Samba s'appuyant sur un annuaire OpenLDAP pour la gestion des comptes. Il nous paraissait en effet peu judicieux de déployer une base de données du type tdbsam non seulement pour des raisons de performances mais également pour des raisons d'évolutivité [4].

Nous utilisions des scripts Shell pour alimenter et modifier les comptes informatiques ainsi que PhpLdapAdmin pour naviguer dans l'arborescence de l'annuaire et modifier les attributs des entrées. Divers serveurs dont un DHCP et un DNS sous Linux complétaient cette infrastructure, accédée par tous les membres de l'équipe. Cette solution était fonctionnelle mais nous avons constaté les limites suivantes :

- Le point le plus visible était la difficulté de piloter de façon collaborative les services et les configurations de différents serveurs. Il faut en effet garder un historique des changements lorsque plusieurs personnes interviennent sur une même ressource afin d'éviter d'éventuels conflits de paramétrage. La présence d'un wiki semblait essentielle mais il fallait penser à le compléter à chaque intervention. Nous avons alors essayé différents outils permettant de suivre les versions des fichiers ainsi que le module auditlog d'OpenLDAP qui enregistre les changements de l'annuaire au format LDIF. Cependant, cette approche augmentait la complexité de l'administration en introduisant de nouveaux programmes à un socle déjà bien fourni.
- La prise en main du système demandait plusieurs séances de formation interne afin de se familiariser avec la syntaxe et le fonctionnement des différents fichiers de configuration. En effet, une simple erreur de saisie pouvait rendre indisponible l'accès à plus de 25 salles informatiques. Nous souhaitions également qu'un personnel administratif puisse créer un compte en cas d'urgence, ce qui n'était pas possible sans une délégation fine des permissions et une interface adaptée.

Découvert en consultant les présentations Solutions Linux 2008 [5], nous avons rapidement été séduit par la solution de Mandriva dont nous ne connaissons pas d'équivalent à part Novell eDirectory et dans une autre mesure, Active Directory. Avec l'approche modulaire du programme, nous avons adapté le produit à notre architecture existante en n'activant que les fonctionnalités nécessaires. Nous avons choisi de ne pas installer les outils de messagerie, de quota et de gestion des mots de passe, ces aspects étant gérés en amont dans l'annuaire OpenLDAP central ou par des scripts. Nous avons également conservé nos procédures de création de comptes. Les entrées et les configurations de nos services DNS et DHCP ont été injectées dans le composant réseau. On peut ajouter que la tolérance aux pannes est réelle en activant les fonctions syncrepl d'OpenLDAP et la réplication de l'annuaire.

Déployé sur nos serveurs depuis la fin de l'année 2008, *Mandriva Directory Server* nous donne totale satisfaction. Le programme est fiable et consomme peu de ressources. Il répond parfaitement à nos attentes et permet aux différents administrateurs de gérer ensemble le service d'annuaire. Les modifications sont consignées automatiquement et sont visibles à travers le module d'audit. Les journaux systèmes sont également accessibles en ligne et la technologie Ajax offre une recherche rapide par mots clefs.

L'interface de navigation est aussi intuitive et bien documentée. La prise en main est rapide comme nous l'avons constaté lors de l'arrivée de nouveaux collègues dans l'équipe. Les risques d'erreurs de saisie sont grandement diminués grâce aux contrôles présents sur les champs des formulaires. De plus, la solution libre de Mandriva facilite l'accès aux ressources des serveurs et évite des connexions à distance sur différentes machines. Par ailleurs, nous pouvons positionner des droits de connexion sur le profil de chaque utilisateur et ainsi déléguer la gestion de certaines tâches. Ainsi, un personnel de l'administration pourra créer des comptes informatiques sans avoir accès au reste des fonctionnalités. L'interface de création de comptes est adaptée pour ces personnes et les différentes options de MDS peuvent être cachées ou activées en lecture seule. Ceci peut être utile pour créer des identifiants dans l'urgence quand les informaticiens sont indisponibles.

4 Conclusion

Mandriva Directory Server s'intègre particulièrement bien à un environnement de travail universitaire. Avec son approche modulaire peu consommatrice de ressources, elle s'adapte à l'existant sans remettre en cause les choix de départ. Elle offre de nombreuses fonctionnalités pour gérer le système d'information d'une entité et permet un véritable travail collaboratif entre les membres d'une équipe informatique. Facile d'accès, multilingue, elle fournit également une infrastructure robuste rendant possible une gestion des postes fixes dans des environnements hétérogènes. Open Source et gratuite, elle a tout pour plaire !

5 Bibliographie

[1] http://www.mandriva.com/fr/linux/server/directory/

[2] http://mds.mandriva.org/

[3] http://mds.mandriva.org/wiki/DownloadVmware240

[4] http://www.samba.org/samba/docs/man/Samba-HOWTO-Collection/passdb.html#id2587489

[5] http://www.solutionslinux.fr/