

Direction Informatique

édition du Direction informatique, Octobre 2004

Dossier

Intégrer les Mac pour mieux les gérer

01/10/2004 - En décidant d'intégrer ses 500 ordinateurs Macintosh dans Active Directory avec ses PC, l'Université de Montréal veut faciliter leur gestion et accroître la sécurité de son environnement.

Alain Beaulieu



Gérer les utilisateurs de Macintosh au même titre que les utilisateurs de PC en utilisant le service de répertoire Active Directory (AD) de Windows ne va pas de soi. En fait, AD ne peut, à la base, prendre en charge les utilisateurs de Mac et, par conséquent, être utilisé pour leur attribuer des droits et les modifier de la même façon qu'il permet de le faire avec les utilisateurs de PC, ce qui pose un problème majeur au niveau de la gestion et de l'authentification des utilisateurs de Mac dans des environnements mixtes.

AD est une banque de données centrales contenant les informations spécifiques des usagers (mots de passe, privilèges, attributs, etc.) et agit, à ce titre, en tant que

système d'authentification. Il sert, par conséquent, à gérer les politiques de sécurité corporatives.

Mac OS X, qui est fondé sur le système d'exploitation Unix, dispose d'un service similaire, appelé Open Directory (OD), mais celui-ci est incompatible avec AD qui est fondé sur le protocole LDAP (Lightweight Directory Access Protocol). Les deux services ne peuvent conséquemment s'échanger de l'information, ce qui constitue le coeur du problème. Il existe cependant un plugiciel (plug-in) offert par Apple pour faciliter les échanges, mais la communication demeure restreinte en utilisant ce plugiciel, qui permet l'authentification des utilisateurs de Mac au niveau de AD, mais ne permet pas de gérer leurs droits et leurs attributions. Apple promet de remédier au problème dans les versions subséquentes de Mac OS, en commençant par la prochaine, dont le nom de code est " Tiger ", mais ce problème est bien réel, dès à présent, pour nombre d'organisations.

" Mac OS X supporte certaines fonctions standard d'Active Directory, affirme Renaud Boisjoly, ingénieur de système pour le marché éducationnel chez Apple Canada. On parle surtout d'authentification. Il permet de déterminer quels utilisateurs ont droit d'accéder aux appareils, mais pour ce qui est de gérer les capacités des utilisateurs sur chacun des appareils, chaque plateforme a ses outils spécifiques. Nous avons, chez Apple, une série d'outils permettant de déterminer quel utilisateur ou groupe d'utilisateurs peut démarrer telle ou telle application, mais Active Directory ne peut pas le faire pour nous. Tiger va permettre de gérer les listes de contrôle des accès, donc de gérer de façon plus précise les droits et privilèges des utilisateurs en termes d'accès aux fichiers. Mais il ne va pas permettre de déterminer s'ils ont le droit ou non de démarrer tel ou tel logiciel. "

Pour contourner ce problème, plusieurs organisations disposant d'un parc informatique mixte ont appliqué jusqu'à date une stratégie d'isolement des Mac par rapport aux PC, en faisant des réseaux de Mac indépendants. Dans le cas où les Mac doivent accéder à des services partagés Mac-PC, l'organisation n'a alors aucun contrôle sur les Mac.

Repousser les limites

Étant donné la percée d'Apple dans le secteur de l'éducation, les institutions d'enseignement, tels les universités et les collèges, constituent des victimes toutes désignées de cette incompatibilité de répertoires. L'Université de Montréal, dont le parc informatique est mixte, figure parmi celles-ci. Mais cette dernière a décidé de recourir, cet été, aux services de la firme conseil montréalaise Mac911 qui a conçu pour elle un script repoussant les limites du plugiciel d'Apple et permettant conséquemment la récupération dans AD de l'information figurant dans OD.

Ayant initialement développé une expertise en dépannage et récupération de données dans l'environnement Macintosh, Mac911 a développé au fil des ans une expertise spécifique en intégration de Mac dans AD. Fondée en 1994, la firme emploie huit personnes et réalise un chiffre d'affaires de deux millions de dollars.

" Mac911 a développé une expertise peu commune sur AD, soutient Nathalie Lincourt, directrice pour le marché universitaire chez Apple Canada. Au niveau de ce qu'ils ont fait à l'Université de Montréal, personnellement je ne connais pas d'autres firmes ayant cette expertise. "

L'objectif de son intervention à l'UdeM était plus spécifiquement de permettre aux Mac de l'institution d'interagir avec l'information figurant dans AD sur ses serveurs Windows 2000, afin de permettre l'authentification des utilisateurs Mac et de contrôler leur accès physique au réseau de l'UdeM. Les Mac se trouvant principalement dans les laboratoires de micro-informatique de l'institution universitaire, ce sont près de 500 postes qui sont visés par l'intervention de Mac911, représentant au total quelque 4 000 groupes d'utilisateurs (étudiants, professeurs, infographistes...).

" Nous voulions que les ordinateurs Macintosh, autant que les ordinateurs Windows, et leurs utilisateurs, puissent être reconnus dans nos systèmes, qu'ils puissent s'y brancher et être contrôlés de la même façon que les ordinateurs sous Windows ", résume Pierre Bordeleau, vice-recteur adjoint aux TIC à l'UdeM.

" Le pont existait entre Active Directory et le serveur Macintosh, mais nous ne pouvions pas utiliser directement l'information obtenue par AD sans avoir à reconstruire de nouveaux groupes dans le Workgroup Manager d'Apple, précise Sébastien Dreyfus, analyste au soutien informatique à l'UdeM. Nous voyions l'information, mais nous ne pouvions pas prendre l'ensemble des usagers faisant partie du groupe et les mettre dans un autre groupe ; nous devons les prendre un à un.

Quand on a seulement une dizaine de groupes à gérer, ça peut toujours se faire, mais là nous en avons 4 000. "

Réutiliser l'information

Le script développé par Mac911 permet, plus spécifiquement, de vérifier l'appartenance de l'utilisateur à un groupe d'utilisateurs prédéfini et de lui accorder l'accès à l'ordinateur et au réseau en fonction des droits dont bénéficie le groupe en question. De cette façon, l'UdeM s'assure un meilleur contrôle sur les ressources auxquelles peuvent accéder les utilisateurs, en plus de lui permettre de réutiliser l'information qui existait déjà dans son infrastructure et ses bases de données, ce qui était le but de l'opération, puisque l'institution ne voulait pas avoir à saisir de nouveau cette information. Ce faisant, les spécialistes de Mac911 ont établi un pont entre AD et OD.

" Le script permet d'établir des groupes d'usagers selon divers critères, par exemple la première lettre de leur nom de famille, et d'accorder à l'usager l'accès aux ressources en fonction de son appartenance à ce groupe, explique M. Dreyfus. Le script vérifie donc l'appartenance de l'usager à un groupe avant de lui accorder l'utilisation de l'ordinateur attribué à ce groupe. Cela permet de limiter l'accès à l'ordinateur et par voie de conséquence au réseau. "

" Mac OS X étant fondé sur Darwin, le système Unix d'Apple, nous avons dû bâtir une interface permettant à Darwin de communiquer avec LDAP, de la même façon qu'Active Directory communique avec LDAP, de sorte à ce qu'Open Directory puisse communiquer avec Active Directory, ajoute Stéphane Pinheiro, président de Mac911. Nous avons bâti une sorte de filtre de traduction entre les deux services de répertoire, précisant les niveaux de langage, les paramètres à employer, etc. Bien qu'il permette aux deux services de répertoire d'échanger, le plugiciel fourni par Apple ne fournit aucune indication sur les informations à échanger, ni le format à employer. Nous avons réussi, et c'est là notre expertise, à élever la solution à un niveau où on parle le même langage et on offre les mêmes services qu'Active Directory. Nous y sommes parvenus en faisant de la configuration manuelle. "

Sécurité accrue

La solution mise en place par Mac911 permet, en outre, à l'UdeM d'accroître la sécurité de son environnement en n'ayant pas à créer des comptes locaux, ce qui faisait partie des principaux objectifs recherchés.

" La sécurité que nous avons préalablement était locale, reconnaît M. Dreyfus. On créait des utilisateurs locaux sur les postes individuellement, à la main, en fonction des besoins de chacun des postes. Donc, dans un laboratoire, on créait 72 fois le même compte et tout le monde rentrait avec ce compte-là et avait certains droits liés à ce compte local.

" C'était beaucoup moins sécuritaire. Rien n'empêchait un étudiant faisant partie d'un laboratoire, auquel on a donné un nom d'usager et un mot de passe local, de donner ce nom et ce mot de passe à quelqu'un d'autre et de lui indiquer le local où aller pour accéder au réseau. Alors qu'avec la solution que nous avons maintenant, l'usager va être plus réticent à transmettre cette information, car nous pouvons le retracer. "

La solution fournie par Mac911, dans sa forme actuelle, ne couvre pas l'ensemble des besoins de l'université, puisqu'elle nécessite encore un certain niveau d'intervention humaine jugé indésirable par l'institution.

" Une deuxième phase nous a été proposée, mais nous ne l'avons pas encore acceptée, affirme M. Dreyfus. Elle consisterait à développer un script qui prendrait automatiquement l'information dans la base de données d'Active Directory et la transférerait directement dans les groupes du Workgroup Manager de Mac, ce qui nous permettrait de gérer les utilisateurs de Mac exactement de la même manière que nous le faisons avec les postes Windows, c'est-à-dire de façon automatique et dynamique. Actuellement, cela peut être fait, mais manuellement, ce qui n'est pas quelque chose de viable dans notre organisation, car nous avons quand même 4 000 groupes à gérer. Donc, c'est très difficile pour nous de recréer 4 000 groupes sous Macintosh et de les gérer de façon dynamique. De la façon qu'Apple permet l'utilisation et la gestion des ordinateurs Macintosh, il faudrait recréer une structure d'Active Directory parallèle au niveau du Workgroup Manager d'Apple et d'y ajouter chacun des groupes manuellement, ce que nous ne pouvons pas nous permettre de faire. "

www.umontreal.ca
www.mac911.com

[Alain Beaulieu](#) est adjoint au rédacteur en chef de Direction informatique

[Fermez la fenêtre](#)