Avant-propos

L'économie en réseau, ou la netéconomie, est au cœur des débats et des stratégies de toutes les entreprises. Les organisations, qu'il s'agisse de société, d'administration publique ou de start-up, tentent tous les jours de créer de nouveaux modèles en tirant parti des liens électroniques qu'ils peuvent tisser avec leurs clients, leurs partenaires et leurs fournisseurs.

Les perspectives sont immenses : elles concernent aussi bien la réduction des coûts de fonctionnement, l'amélioration de l'efficacité des opérations, que la possibilité de générer de nouveaux revenus. Certaines entreprises ont réussi à réduire considérablement leurs coûts de fonctionnement à l'aide d'intranets et d'extranets, d'autres ont réussi à gagner de l'argent là où elles s'y attendaient le moins à l'aide d'Internet.

De nouveaux métiers offerts par de nouveaux acteurs ont aussi trouvé leur place dans cette économie en réseau. Les places de marché électroniques, les sites de ventes aux enchères, les sites communautaires, les portails ne sont que quelques exemples des opportunités qui se présentent. La créativité des hommes n'a pas de limites. Du BtoC *(Business to Consumer)* au BtoB *(Business to Business)*, en passant par le BtoBtoC *(Business to Business to Consumer)* ou le CtoC *(Consumer to Consumer)*, il y a des centaines de combinaisons et de modèles qui permettent d'apporter de la valeur aux citoyens, aux consommateurs et aux entreprises.

Cependant, le retour d'expérience de ces dernières années a mis en évidence d'autres enjeux, qui sont devenus majeurs pour l'entreprise :

- *la sécurité*, dont les menaces ont été favorisées par la prolifération des services en ligne et les réseaux de télécommunications mondiaux ;
- *l'efficacité des opérations,* dont la complexité augmente considérablement avec le nombre d'utilisateurs et de services ;
- et enfin *l'accessibilité à l'information*, gage d'adoption de la multitude de services offerts par l'entreprise, et ceci de façon ciblée par rapport aux attentes de chacun.

Nous détaillons chacun de ces points ci-dessous.

Les technologies de l'information et de communication ont apporté l'instantanéité de l'accès aux données de l'entreprise, à partir de n'importe quel endroit du monde et depuis tout type de terminal, comme un PC ou un téléphone mobile. Il est, par exemple, possible d'accéder à sa messagerie de n'importe où, à partir d'un ordinateur quelconque ou de son

téléphone portable, remplir sa déclaration d'impôts à partir d'un accès Internet à l'étranger, ou encore de consulter son compte bancaire de n'importe quel pays et vérifier instantanément les débits relatifs à tous les achats effectués.

Tout ceci rend les services en ligne et les informations échangées plus vulnérables, car accessibles à des personnes mal intentionnées, où qu'elles soient dans le monde. Par exemple, nous connaissons actuellement une augmentation croissante du nombre de « spam », ces courriers publicitaires envoyés à tous et qui polluent nos boîtes aux lettres. Ils constituent aujourd'hui plus de 70 % du trafic des messageries sur Internet ! Une des raisons de ce phénomène est que les adresses de messagerie saisies sur les sites visités sont utilisées à notre insu. Comment contrôler la diffusion de nos données personnelles, comme l'adresse de messagerie ou son numéro de carte de crédit ? Plus généralement, comment concilier deux tendances contradictoires : d'une part, la liberté d'agir de n'importe où et à tout moment rendue possible par les nouvelles technologies, et, d'autre part, la sécurité des données personnelles, des informations échangées et des transactions ?

Pour cela, il faut être en mesure d'isoler le système d'information de l'entreprise depuis l'extérieur, et de surveiller les flux qui transitent entre les deux. Il faut ensuite identifier, voire authentifier, les utilisateurs, et contrôler les services auxquels ils accèdent en fonction de leurs profils. Il faut protéger les informations personnelles fournies, comme l'adresse de messagerie personnelle, le mot de passe, le numéro de carte de crédit ou les données confidentielles et sensibles du dossier médical, et s'assurer que seuls les services et les personnes habilitées peuvent y accéder. Et enfin, il faut dans certains cas pouvoir chiffrer de bout en bout les informations échangées sur Internet ou sur d'autres réseaux publics, afin de s'assurer que seuls les destinataires peuvent les lire.

Par ailleurs, la multitude d'utilisateurs, de clients ou de citoyens, ainsi que la richesse des services en ligne offerts dans l'entreprise, sur Internet ou sur les réseaux de téléphonie mobile, rendent l'administration des comptes utilisateurs, dans les différentes applications, et des droits d'accès aux services fastidieuse et coûteuse. La gestion d'une abondance de mots de passe peut décourager les utilisateurs d'accéder aux services ou encore submerger un centre d'appel téléphonique de demandes de réinitialisation des mots de passes perdus. La création et la suppression des comptes utilisateurs dans les applications peuvent engendrer des coûts prohibitifs en fonction du nombre d'applications à administrer et du nombre de mouvements de personnes dans l'entreprise.

Pour rendre les opérations quotidiennes assurées par les entreprises plus efficaces, il est nécessaire de mettre en place des outils permettant, d'une part, de fédérer les informations d'identités concernant les utilisateurs, et, d'autre part, d'intégrer, de centraliser et d'automatiser autant que possible les différentes fonctions d'administration afin de réduire le nombre d'opérations effectuées par les administrateurs. Il faut aussi, dès que possible, déléguer les tâches d'administration à travers un extranet à des entités autonomes, par exemple, une filiale, des fournisseurs ou des entreprises « clientes ». Au-delà de la réduction des coûts, cela apportera plus de flexibilité et de réactivité aux entreprises face à de nouveaux besoins, comme un changement d'organisation ou de nouveaux utilisateurs.

Et enfin, la prolifération d'information, de contenu et d'applications dans l'entreprise, nécessite de mieux cibler les utilisateurs en fonction de leurs besoins. Par exemple, un responsable marketing sera intéressé en priorité par les descriptions des produits et leurs positionnements par rapport à la concurrence, alors qu'un responsable de l'ingénierie cherchera avant tout l'accès à la documentation produits, aux résultats de *benchmarking*, etc.

Pour cela, il faut non seulement fédérer les informations d'identité des utilisateurs, mais surtout définir les attributs qui vont permettre cette personnalisation, et partager une même sémantique au sein de l'entreprise, comme la fonction et le rôle d'un individu, afin de constituer une base de profils partagée par la société.

Pour tous ces aspects, il est apparu durant ces dernières années des technologies, des standards et des outils qui apportent des solutions à l'ensemble des questions posées. Ces outils, ainsi que les méthodes et pratiques associées, sont désignés par le vocable « gestion des identités » ou « Identity management » en anglais.

Les annuaires LDAP, objet de ce livre, constituent le principal composant de la gestion des identités.

Ils ont été conçus pour prendre en charge un grand nombre d'utilisateurs, et offrent généralement des performances en lecture supérieures à celle des bases de données relationnelles.

Ils contiennent en standard des mécanismes d'authentification ainsi que des informations normalisées sur les profils des personnes. Ils favorisent ainsi l'authentification unique et le partage de ces profils entre les différents services de l'entreprise.

À l'aide d'une organisation hiérarchique des données sur les personnes et les ressources, reflétant l'organisation des entreprises, ils favorisent la délégation de l'administration et la réduction des coûts associés.

Ils permettent aussi de décrire les ressources accessibles par les utilisateurs, comme les terminaux, les imprimantes et les serveurs de données, et même les applications informatiques et le contenu éditorial, favorisant ainsi l'adéquation d'un service offert par une ressource ainsi que sa personnalisation, en fonction des caractéristiques de la ressource et du profil de l'utilisateur.

Enfin, ils offrent des mécanismes intégrés de protection des données et de contrôle des habilitations, apportant ainsi une solution homogène et normalisée pour la gestion de la sécurité, qui ne dépend pas des applications.

Mais les annuaires LDAP ne sont plus le seul outil requis pour la gestion des identités : ils doivent être accompagnés d'outils de synchronisation des données, de gestion du contenu des annuaires, de gestion des mots de passe, de contrôle des droits d'accès aux applications, etc. Nous allons aussi décrire tous ces outils dans cet ouvrage, et donner des exemples concrets de mise en œuvre impliquant l'ensemble des composants d'une solution de gestion des identités d'entreprise.

Quel est l'objectif de cet ouvrage ?

L'objectif de cet ouvrage est de vous sensibiliser sur la notion d'annuaire et de gestion des identités, ainsi que sur leurs apports à travers des exemples et des études de cas.

Son but est aussi de décrire en détail et de façon pragmatique le standard LDAP et tous ceux qui lui sont associés, l'ensemble des outils requis pour créer un annuaire d'entreprise, ainsi que la démarche de mise en œuvre basée sur ces technologies.

Vous y trouverez également une description de tous les outils nécessaires pour intégrer un annuaire avec le système d'information de l'entreprise et son organisation, ainsi que des exemples de code pour interroger et mettre à jour un annuaire LDAP.

La structure de l'ouvrage

L'ouvrage est découpé en quatre parties.

La première partie est une introduction sur les annuaires et sur leurs applications. Elle est destinée à des néophytes, n'ayant pas de connaissance particulière sur les annuaires, et qui souhaitent comprendre les apports sans entrer dans les détails techniques :

- Le chapitre 1 vous fait découvrir la notion d'annuaire et les particularités de ceux-ci par rapport à des bases de données. Vous y trouverez ce que sont la gestion et la fédération des identités, ainsi que le rôle des annuaires dans ces contextes.
- Le chapitre 2 donne un aperçu de l'historique des annuaires et introduit la technologie LDAP.
- Le chapitre 3 donne des exemples d'applications de cette technologie afin de mettre en avant ses apports aussi bien dans le cadre d'applications Internet, de portails d'entreprise que d'extranets et d'intranets.

La deuxième partie présente de façon détaillée le standard LDAP :

- Le chapitre 4 décrit le standard de façon générale et détaille son modèle client-serveur.
- Le chapitre 5 décrit les quatre modèles du standard : le modèle de données, le modèle de désignation, le modèle de fonctions et le modèle de sécurité.
- Le chapitre 6 décrit les interfaces d'accès à un annuaire LDAP définies par les instances de normalisation, et donne un aperçu des travaux en cours pour étendre ce standard. On y présente aussi les autres standards comme DSML et SAML.

La troisième partie décrit la démarche préconisée pour concevoir et mettre en œuvre un annuaire LDAP. Elle contient aussi une description des outils nécessaires pour réaliser une application basée sur LDAP :

- Le chapitre 7 décrit la phase de conception fonctionnelle d'un annuaire LDAP. Il s'agit d'apprendre comment concevoir le modèle de données et le modèle de désignation, en tenant compte des besoins des utilisateurs et l'organisation de l'entreprise.

- Le chapitre 8 décrit la phase de conception technique d'un annuaire LDAP. Il décrit la gestion des habilitations, la topologie des serveurs, la réplication entre annuaires et la protection des serveurs LDAP par des firewalls.
- Le chapitre 9 contient des études de cas, mettant en application les démarches décrites dans les chapitres précédents, dont le cas la société Thomson.
- Le chapitre 10 décrit l'ensemble des outils requis pour mettre en œuvre un annuaire LDAP, ainsi que la gestion et la fédération des identités, les outils de SSO et ceux permettant de développer des applications basées sur ce standard.
- Le chapitre 11 décrit le cycle de vie d'un annuaire, comprenant l'organisation à mettre en place pour le faire évoluer ainsi que les outils adéquats. On y trouvera aussi une description du cadre légal associé à la protection des libertés individuelles, ainsi que les obligations des entreprises créant leur propre annuaire.

La quatrième partie comprend une description des principales interfaces de programmation LDAP :

- Le chapitre 12 décrit l'interface de programmation en C/C++ et donne des exemples de code.
- Le chapitre 13 décrit l'interface de programmation ADSI/.Net et donne des exemples de code.
- Le chapitre 14 décrit l'interface de programmation JNDI et donne des exemples de code.
- Le chapitre 15 décrit l'interface de programmation LDAP en PHP et donne des exemples de code.
- Le chapitre 16 décrit l'annuaire OpenLDAP, logiciel libre largement répandu dans le monde Linux.

À qui s'adresse cet ouvrage ?

Cet ouvrage s'adresse aussi bien aux responsables fonctionnels (maîtrises d'ouvrage) qu'aux décideurs de la stratégie technologique, aux chefs de projet, aux consultants et aux développeurs. Il est également destiné aux directions informatiques qui souhaitent comprendre la technologie LDAP et ses applications.

Les premiers chapitres permettront aux maîtrises d'ouvrage et aux directions informatiques de bien comprendre les apports de la technologie LDAP en regard de leurs métiers. Aucune compétence technologique particulière n'est requise pour les lire.

La deuxième et la troisième partie permettront aux décideurs de stratégie technologique, aux chefs de projets et aux consultants de bien comprendre ce qu'est LDAP et comment mettre en œuvre un annuaire reposant sur cette technologie.

La dernière partie est destinée aux développeurs qui souhaitent apprendre à réaliser des applications basées sur LDAP.

Nous vous recommandons bien sûr de lire la totalité de cet ouvrage. Néanmoins, si vous êtes pressé, vous trouverez dans le tableau suivant les chapitres à lire en fonction de votre profil et de vos préoccupations :

Votre profil	Vos préoccupations	Les chapitres à lire en priorité
Directeur ou responsable informatique	Comprendre les apports de LDAP et décider si cette technologie répond à vos besoins	Chapitres 1, 2, 3, 9 et 11
	Évaluer les ressources nécessaires pour mettre en œuvre un annuaire LDAP	Chapitres 7, 8 et 10
Responsable fonctionnel (maîtrise d'ouvrage)	Comprendre les apports de LDAP	Chapitres 1, 3, 9 et 11
Chef de projet	Comprendre la technologie LDAP	Chapitres 1, 2, 3, 4 et 5
	Encadrer une équipe de conception et de réalisation	Chapitres 7, 8 et 9
Consultant	Comprendre et concevoir un annuaire LDAP	Chapitres 1, 2, 3, 4, 5, 7, 8, 9 et 11
Développeur	Comprendre et mettre en œuvre un annuaire LDAP	Chapitres 5, 6, 8, 10, 12, 13, 14, 15 et 16

Questions et réponses

Qu'est que LDAP ?

LDAP signifie *Lightweight Directory Access Protocol*. C'est un standard destiné à normaliser l'interface d'accès aux annuaires. L'objectif de LDAP est de favoriser le partage et de simplifier la gestion des informations concernant des personnes et plus généralement de toutes les ressources de l'entreprise, ainsi que des droits d'accès de ces personnes sur ces ressources.

Qui est responsable du standard LDAP ?

Le standard LDAP, né des technologies Internet et X500, est normalisé par l'IETF *(Internet Engineering Task Force)*. De nombreux groupes de travail, constitués des principaux acteurs du marché, comme IBM, Sun, Novell, Oracle, Microsoft, Critical Path, font évoluer le standard au sein de l'IETF.

Que peut m'apporter LDAP ?

LDAP simplifie la gestion des profils de personnes et de ressources, favorise l'interopérabilité des systèmes d'information à travers le partage de ces profils, et améliore la sécurité d'accès aux applications.

De façon générale, un annuaire LDAP d'entreprise (groupware, intranets, à la sécurité du système d'information, etc.) permet de réduire les coûts d'administration et d'améliorer la sécurité. Un annuaire LDAP pour les applications de e-business (commerce électronique, extranets, etc.) permet de mieux gérer les profils des utilisateurs, de favoriser la

personnalisation des services et de déléguer l'administration à des utilisateurs externes à l'entreprise tout en contrôlant la sécurité.

Pourquoi LDAP est-il aussi important ?

La totalité des acteurs du marché ont intégré LDAP dans leurs outils. C'est le cas, aussi bien des systèmes d'exploitation comme Linux, Windows 2000/2003 et Sun Solaris, que des outils de travail de groupe comme IBM Lotus Domino, Novell Groupwise et Microsoft Exchange, et les progiciels de e-business comme ATG, Vignette ou Broadvision. C'est valable aussi pour les bases de données et des serveurs d'applications Java du marché, comme BEA WebLogic et IBM WebSphere. Enfin, c'est le standard retenu par la totalité des acteurs du marché pour la gestion de la sécurité, comme l'authentification forte à l'aide de certificats ou encore la gestion des autorisations d'accès à des applications Web.

Quelles différences y a-t-il entre LDAP et une base de données ?

LDAP contient des classes d'objets qui définissent des personnes, des applications et des groupes, qui sont toutes normalisés par l'IETF. On retrouve ces classes dans tous les outils conformes au standard LDAP.

L'organisation des données n'est pas relationnelle, mais hiérarchique, ce qui permet de la rendre plus proche de la hiérarchie en vigueur dans l'entreprise. Ceci facilite l'administration des données : par exemple, pour supprimer un groupe d'utilisateurs, il suffit de supprimer une branche de l'arborescence, et pour attribuer des droits à un groupe d'utilisateurs, il suffit de le faire sur une branche.

Le standard LDAP offre un service d'identification et d'authentification accessible à travers un réseau IP. Les mécanismes d'authentification sont normalisés et peuvent être étendus si nécessaire. Dans tous les cas, l'authentification est gérée par l'annuaire même et non par les programmes qui l'utilisent. Le niveau de sécurité est donc plus élevé et homogène entre les différentes applications.

Enfin, il est possible de gérer et contrôler les habilitations d'accès aux données dans l'annuaire même. Tout objet de l'annuaire peut être utilisé pour s'identifier à l'annuaire. Des ACL (*Access Control List*) permettent de décrire les droits (lecture, mise à jour, recherche) d'un objet, représentant généralement un utilisateur ou une application, sur les autres objets de l'annuaire.

Comment faire cohabiter un annuaire LDAP avec des applications existantes ?

Il y a différentes façons de faire cohabiter un annuaire LDAP avec des applications qui ne sont pas compatibles avec ce standard.

La méthode la plus simple consiste à mettre en place des outils de synchronisation des données à travers des échanges de fichiers.

Une autre méthode consiste à utiliser un méta-annuaire. Cette dernière est plus complexe à mettre en œuvre mais possède beaucoup d'avantages. Elle permet, à l'aide de connecteurs prêts à l'emploi, de synchroniser en permanence les données des différentes applications et de s'adapter facilement à tout changement concernant les sources de données ou l'annuaire lui-même. Il existe aussi des solutions, appelées « méta-annuaire virtuel », qui offrent, à l'instar d'un *proxy*, une vue LDAP sur des données qui se trouvent dans diverses applications et bases de données. Ce type de solution évite la copie et la synchronisation des informations dans un annuaire central.

Qu'est qu'un méta-annuaire ?

Un méta-annuaire est un outil qui se « greffe » au-dessus des applications et de leurs annuaires, pour offrir une vue unifiée ainsi qu'une administration centralisée de l'ensemble des données relatives aux personnes et aux ressources de l'entreprise. Le méta-annuaire devient le moyen d'accès privilégié à ces données pour toute fonction d'administration et toute nouvelle application. Il permet de conserver l'hétérogénéité des infrastructures tout en apportant une vue homogène sur ces informations. Il offre une interface basée sur un standard comme LDAP pour accéder aux données.

Qu'est-ce que la gestion des identités ?

On entend généralement par gestion des identités, l'ensemble des fonctionnalités et des services suivants :

- Un référentiel sécurisé, contenant l'ensemble des informations relatives à des personnes et à leurs identités, ainsi que des données sur les organisations auxquelles appartiennent ces personnes. Ceci nécessite généralement la collecte de ces informations dans les différentes applications et systèmes de l'entreprise de façon automatisée.
- La gestion du contenu de ce référentiel comprenant, notamment, des interfaces de mise à jour respectant les processus organisationnels de l'entreprise.
- L'allocation et la désallocation automatisée des ressources de l'entreprise : il s'agit notamment de mettre en place une administration centralisée des comptes utilisateurs dans les applications et systèmes de l'entreprise (messagerie, badge d'accès aux locaux, applications métiers, etc.). On désigne souvent cette fonctionnalité par *e-provisionning*.
- La gestion des mots de passe : il s'agit d'outils permettant de réduire, voire d'unifier, les nombreux identifiants et mots de passe des utilisateurs dans le système d'information de l'entreprise.
- La gestion des droits d'accès aux ressources de l'entreprise : il s'agit d'outils permettant de sécuriser l'accès aux applications et systèmes de l'entreprise, à l'aide de mécanismes d'authentification et d'une gestion des habilitations centralisée.

Quel lien y a-t-il entre la gestion des identités et un annuaire LDAP ?

La gestion des identités s'appuie généralement (mais pas nécessairement) sur un annuaire LDAP. Celui-ci constitue, dans ce cas, le référentiel sécurisé des données. De plus, il offre les interfaces d'accès normalisées pour l'identification et l'authentification des utilisateurs, ainsi que pour la lecture et la mise à jour des données dans le référentiel.

Qu'est-ce que la fédération des identités ?

La fédération des identités consiste à faire communiquer plusieurs systèmes de gestion des identités, tels que nous l'avons défini précédemment, afin d'éviter de constituer une solution centralisée, tout en assurant des services d'authentification unique, d'échanges d'attributs et de droits utilisateurs entre les différents sites auxquels ils ont accès.