

Le métaannuaire d'entre et organisationnel

► Si le concept d'annuaire unique d'entreprise relève de l'utopie, la gestion centralisée des identités des utilisateurs du système d'information peut tirer parti de solutions de type métaannuaire. À condition, toutefois, que l'on ait pris soin des phases en amont de ces projets d'infrastructure, sans négliger l'importance de leur composante organisationnelle.

Comment administrer de façon centrale les identités, profils et habilitations informatiques des collaborateurs de l'entreprise ? Comment sécuriser l'accès aux ressources, rationaliser les mécanismes d'authentification et automatiser les processus d'activation des applications ou les procédures d'accès à ces applications ? Ces questions sont apparues avec l'émergence de la gestion centralisée des identités des utilisateurs d'un système d'information. Reste que cette démarche, pour le moins ambitieuse, demande de s'appuyer sur une vue centralisée des informations d'identités relatives aux

collaborateurs, et parfois aux clients et partenaires. Or, l'entreprise possède non pas un, mais une multitude d'entrepôts de données d'identités. Ces informations sont stockées dans des applications aussi diverses

> FOURNIR UNE VISION COMMUNE DES IDENTITÉS EXPLOITABLE PAR D'AUTRES APPLICATIONS.

que des annuaires proprement dits (Open LDAP, eDirectory, Active Directory, etc.) ; des répertoires de serveurs de messageries (Notes et Exchange notamment) ; des bases de données liées aux ressources humaines ; ou des bases commerciales et des progiciels d'entreprise de type SAP ou Siebel. Ces référentiels gèrent des informations d'identités fragmentaires, pas toujours à jour, parfois incohérentes, et sous le contrôle de différentes directions fonctionnelles dans l'entreprise. C'est là que se profile l'idée du métaannuaire, dont la raison d'être est de fournir cette vision commune des identités que pourraient exploiter d'autres applications, de type « page blanche » ou authentifiant unique (SSO, *Single sign-on*) par exemple. Techniquement, le métaannuaire s'appuie sur un

moteur de jointure afin de synchroniser des sources de données, et s'interface avec lui via des connecteurs spécifiques et des mécanismes de publication-abonnement ; il est capable de consolider tout ou partie de ces sources de données, et de répercuter de façon synchrone ou asynchrone les modifications apportées aux informations que l'on aura jugé pertinent de partager. Ce concept de métaannuaire a suscité l'émergence d'une offre logicielle spécialisée qui, tel DirXML, de Novell, (rebaptisé depuis Identity Manager), a été proposée en complément des annuaires LDAP (eDirectory, en l'occurrence, chez Novell). Ces logiciels, encore imparfaits, commencent à gagner en maturité. Mais il est clair que le principal problème d'un projet métaannuaire est de définir une nouvelle architecture de services d'infrastructure, et non pas de sélectionner tel ou tel outil logiciel.

L'importance de la composante organisationnelle

La question des choix techniques, – spécifique ou progiciel – n'interviendra de toute façon qu'en phase de spécification détaillée, une fois bien définis le cahier des charges et l'analyse fonctionnelle. Chez les spécialistes de la gestion des identités, on souligne volontiers qu'un projet de métaannuaire a une grande composante organisationnelle, et que les phases de justification et d'analyse en amont ne doivent pas être négligées. Ce type de projet nécessite de mettre autour de la table des responsables fonc-

Si vous êtes pressé...

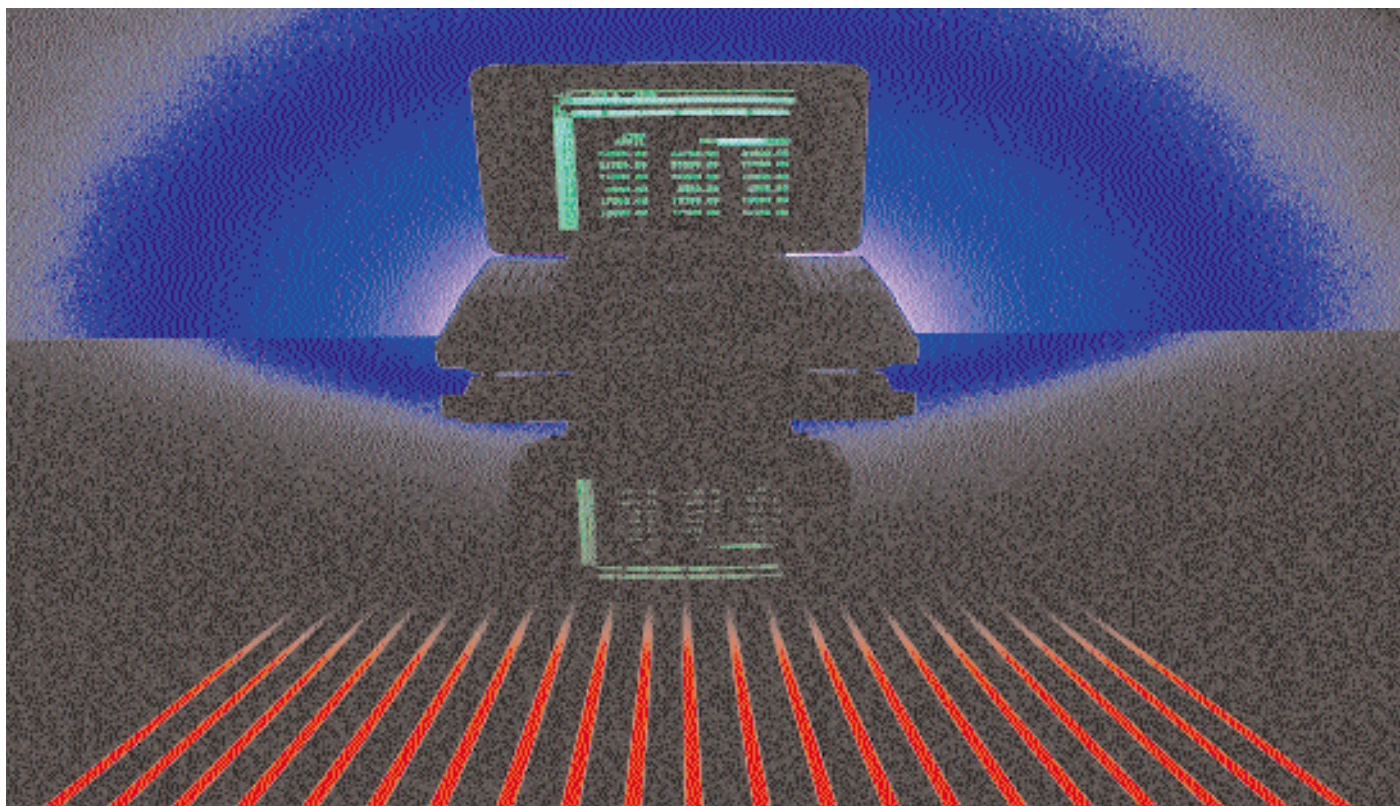
► **Identifier les sources de données fiables,** établir le modèle de données et le documenter, définir les modes de synchronisation ainsi que les mécanismes de *workflow*, telles sont quelques-unes des principales difficultés d'un projet de métaannuaire.

► **En fonction des contraintes du cahier des charges,** l'architecture technique du service de métaannuaire peut faire appel à des outils de métaannuaires

ou de *provisioning*, à du développement spécifique de connecteurs et/ou à de l'intégration façon EAI.

► **Le fait que l'on doive interconnecter des sources de données hétérogènes,** non nécessairement LDAP, et que les offres logicielles – immatures – montrent encore certaines faiblesses, peut compliquer la mise en service et l'optimisation du service de métaannuaire.

prise, entre technique



tionnels issus d'horizons variés (ressources humaines, informatique, sécurité, commercial, etc.). Parce qu'ils sont propriétaires de certaines des données concernées et/ou responsables de la définition des rôles et habilitations des personnels, ces managers seront d'emblée d'importants contributeurs du futur service. À condition qu'ils acceptent la relative perte de pouvoir sur leurs données qu'un tel projet pourrait occasionner, et que le « parrain » du projet réussisse à démontrer le bien-fondé du futur « pot commun » d'informations. La conception du modèle de données du métaannuaire demandera de se livrer au préalable à une cartographie des données d'identités de l'entreprise. L'identification des sources de données appropriées, la sélection, et la qualification des entités et attributs qu'il sera nécessaire de partager ne seront

pas les moindres des problèmes qui se poseront. Où trouver les données pertinentes ? Dans des applications qui font office de « sources » faisant autorité et dans des « référentiels maîtres », ainsi dénommés car indispensables au fonctionnement d'applications stratégiques. Ainsi ira-t-on chercher le nom de l'employé dans l'application Ressources humaines, l'e-mail dans le répertoire du serveur de messagerie et les numéros de téléphones sur le PABX de l'en-

treprise. Cette identification des données « maîtresses » et de leur propriétaire doit s'accompagner d'un travail de fiabilisation et de « nettoyage » des référentiels sources. Philippe Dajeau, responsable annuaire chez SoluCom, explique : « *Même des référentiels considérés comme maîtres ne sont pas toujours très fiables ; ils peuvent contenir des données qui auraient dû être supprimées, ou des informations de liens hiérarchiques non à jour.* » Ces phases d'analyse peuvent représenter ▶

SUN REVIENT SUR LE DEVANT DE LA SCÈNE GRÂCE À WAVESET

Courant 2003, un nouvel acteur visionnaire du marché des métaannuaires est apparu sur l'écran radar du GartnerGroup. Il s'agit de Waveset, petit concepteur de Lighthouse, un

métaannuaire de nouvelle génération qui, se basant sur une notion d'identité virtuelle, se veut très peu intrusif au niveau des serveurs de données. Une bonne aubaine pour Sun, qui n'a pas été très heureux avec son

ancienne offre Java System Meta Directory Server. En phase de réorganisation de son offre de gestion des identités, il en a profité pour acquérir Waveset en novembre 2003. Lighthouse se retrouve

aujourd'hui à la base de sa nouvelle solution de métaannuaire et d'e-provisioning Java System Access Manager. Reste à Sun à promouvoir une offre logicielle qui ne compte que peu de références en Europe.

Ils ont dit...

« On doit nécessairement s'orienter vers une logique de fédération des référentiels »

► **Philippe Dajean**, responsable annuaire chez SoluCom



Il y avait deux façons d'aborder le problème de l'annuaire d'entreprise : fédérer les référentiels existants ou mettre en œuvre un annuaire qui vient en lieu et place des référentiels d'entreprise. Cette deuxième approche n'ayant plus de sens, on doit nécessairement s'orienter vers une logique de fédération des référentiels et, donc, d'interconnexion via un métaannuaire. Toute la question est alors de savoir ce que l'on met derrière cette idée de métaannuaire, et comment réaliser ce type de solutions. On peut, en effet, se tourner vers des outils spécialisés de métaannuaire ou de *provisioning*, ou encore faire appel à du développement spécifique pour interconnecter les référentiels.

► une portion non négligeable du temps imparti : de l'ordre de trois à six mois pour un projet qui, toutes phases comprises (spécifications détaillées, réalisation, déploiement, interconnexion, etc.) s'étalerait sur un an. Dans un contexte de grande entreprise, il est recommandé de procéder par paliers d'un à deux ans, en veillant à circonscrire les périmètres utilisateurs et applicatifs, de façon à produire rapidement les premiers résultats concrets.

Explorer différentes pistes architecturales

Une fois spécifiés le service de métaannuaire, son modèle de données et ses processus de *workflow*, il sera alors temps de se pencher sur son architecture technique. Pour un projet de métaannuaire, comme pour tout autre projet d'intégration applicative, l'approche spécifique comporte un risque de dérive. Elle peut néanmoins, parfois, se justifier, notamment si le projet n'implique que quelques sources de données, ou si l'on n'envisage le recours au développement maison que de façon transitoire. Selon les exigences du cahier des charges, différentes pistes architecturales méritent en tout cas d'être explorées. S'il s'agit simplement d'harmoniser quelques sources de données, on peut

se contenter d'interfacier les annuaires par des liens point à point. La Sacem (Société des auteurs, compositeurs et éditeurs de musique), par exemple, a construit une solution SSO sur la base d'un annuaire LDAP Oracle interfacé avec son application Ressources humaines et avec ses annuaires bureautiques Active Directory.

On peut, dans des situations plus complexes, s'appuyer sur un annuaire fédérateur pour constituer le référentiel d'identités. C'est cette direction qu'avait choisie l'Adae, Agence pour le développement de l'administration électronique, pour son projet de métaannuaire interministériel Maia. Si le cahier des charges n'impose qu'une faible fréquence de mise à jour des données, journalière par exemple, la consolidation des informations peut très bien reposer sur un simple mécanisme d'extraction et de transfert de fichiers plats. Rien n'empêche aussi, sur le papier en tout cas, de tirer parti de l'infrastructure EAI de l'entreprise. Les progiciels EAI actuels disposant de connecteurs LDAP, il serait envisageable de les employer pour synchroniser des annuaires. Bien entendu, pour peu que l'on projette d'interfacier, non plus quelques-unes, mais des dizaines de sources de

données maîtres, que l'on veuille propager au fil de l'eau les événements de mise à jour, être en mesure de détecter les changements dans les bases sources – ce que ne peuvent faire les connecteurs EAI –, et/ou paramétrer des règles de jointure et des séquences de traitements complexes, une approche purement EAI des mécanismes de synchronisation serait inappropriée. On se tournera alors vers les progiciels de métaannuaire.

Les performances des métaannuaires en question

Par le passé, les performances de ces progiciels ont fait l'objet de critiques. Sur ce point, cependant, il est difficile de faire la part des choses. Les mises en cause portent, parfois sur l'incapacité des moteurs de jointure à traiter des flux importants d'événements, parfois sur l'inefficacité de certains connecteurs logiciels applicatifs. En fait, il ne fait aucun doute que les métaannuaires ont été pénalisés par leur architecture en « étoile », et qu'ils auraient tout avantage à s'inspirer des architectures en bus que l'on connaît bien dans le monde de l'EAI. C'est d'ailleurs ce qui explique, pour partie, l'acquisition par IBM du petit spécialiste métaannuaire qu'était Metamerger en 2002.

UNE OFFRE PROGICIELLE QUI N'EXCLUT PAS UNE RELATIVE DIVERSIFICATION FONCTIONNELLE

Éditeurs	Métaannuaires
Computer Associates	Fonction d'annuaires virtuels intégrée à l'annuaire eTrust Directory (fonction DXlink)
Critical Path	Meta Directory Server
IBM	Tivoli Directory Integrator
MaXware	MaXware Data Synchronisation Engine et MaXware Virtual Directory
Microsoft	MIIIS (Microsoft Identity Integration Server)
Novell	Nsure Identity Manager (anciennement DirXML)
OctetString	Virtual Directory Engine Suite
Radiant Logic	RadiantOne Virtual Directory Server
Siemens	DirXmetahub
Syntegra	Global Directory - Meta Edition
Sun	Java System Meta Directory Server (basé sur Lighthouse, d'origine Waveset)

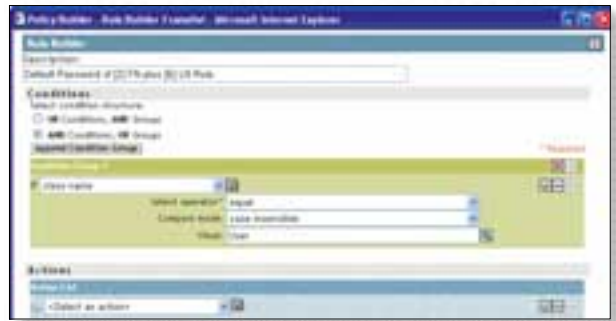
Certains éditeurs veulent résoudre la problématique globale de synchronisation à l'échelle d'une organisation. D'autres cherchent plus particulièrement à étendre les capacités d'interconnexion d'un annuaire (d'où la notion d'annuaires virtuels parfois mise en avant).

La synchronisation de sources de données multiples étant un problème complexe, il faudrait pour cela s'appuyer sur des technologies d'interconnexion irrécupérables. Sur ce plan, les outils métaannuaires souffrent encore de leur immaturité, au point que certains projets ont du mal à rendre les résultats attendus. Les connecteurs logiciels actuels sont quelque fois difficiles à mettre en place ou ne résistent pas aux fortes charges. Cette question reste un important point de différenciation des offres. Il ne faut pas perdre de vue « que les métaannuaires montrent de vraies différences fonctionnelles et financières », souligne Philippe Dajean. Selon les contextes, ils sont plus ou moins faciles à connecter, et peuvent marcher très bien chez l'un, et être plus durs à mettre en place chez l'autre ». L'idée de connecteurs « disponibles sur étagère » est donc quelque peu illusoire. Le fait qu'ils supportent XML contribue, bien sûr, à simplifier le travail d'intégration.

Interconnecter des données aux formats variés

Dès lors que l'on se propose de déclencher des actions et de coupler les événements de mises à jour d'information avec des processus de workflow (par exemple créations de comptes utilisateurs et ouverture de boîtes aux lettres), réclamant des actions de paramétrage avancées, on ne pourra faire l'impasse sur un examen détaillé des solutions commerciales. Si la mise en œuvre de connecteurs « de base », pour interfacier les serveurs de messagerie, intégrer des annuaires comme Active Directory, ou extraire des fichiers plats, ne pose pas de réel problème, il n'en est pas de même pour les connecteurs pour progiciels d'entreprise de type ERP PeopleSoft ou SAP, plus chers, plus sophistiqués mais inégaux d'un éditeur à un autre, et parfois générateurs de temps de latence importants. À la décharge des métaannuaires, il est vrai

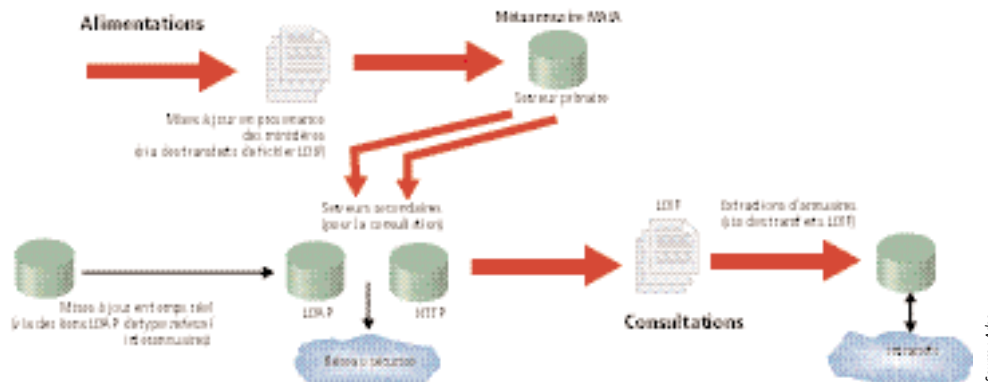
qu'on leur demande de synchroniser des données aux formats pour le moins hétérogènes. Comme le rappelle Jean-Cédric de Trémaudan, consultant chez Net2s, « il ne s'agit pas de synchroniser les seules sources LDAP ; toutes les entreprises ont des existants incluant des bases de messagerie, des SGBD relationnelles, des bases indexées, des fichiers plats, des fichiers propriétaires, des tableurs, et même, dans le cas des PME, des fichiers clients sous Access ». Parfois, les traitements à automatiser sont d'une grande complexité. Par exemple, on peut vouloir combiner des procédures de mise à jour asynchrones des données avec un mécanisme d'exception, nécessitant de rafraîchir de façon quasi synchrone certaines informations. Les exigences du cahier des charges, elles, sont susceptibles d'évoluer avec le temps ; ainsi peut-il être souhaitable de faire évoluer un service de métaannuaire asynchrone vers un mode de fonctionnement synchrone, afin de satisfaire aux contraintes de mise en place d'une solution de contrôle d'accès. Les métaannuaires doivent donc faire preuve de capacité d'évolution. D'un autre côté, c'est en principe aux annuaires LDAP – dans les infrastructures informatiques taillées pour cela – que revient la lourde charge de stocker les informations d'identités ; la plupart du temps, les métaan-



nuaires n'ont à répercuter que des modifications de données peu volumineuses. Même dans de grandes entreprises, il est peu probable que les opérations de suppression-création de comptes employés génèrent des flux d'événements importants. Par ailleurs, on n'a que peu souvent besoin de rafraîchir les données en temps réel. En conséquence, les outils sont loin d'être systématiquement utilisés au maximum de leurs possibilités. Certes, la mise en œuvre d'un métaannuaire n'a encore rien d'un long fleuve tranquille. Néanmoins, une fois déployé, le métaannuaire peut jouer un rôle structurant non négligeable. Ses promoteurs seraient, en effet, bien placés pour imposer leurs propres règles de qualité de service, et édicter les spécifications que les développeurs d'applications et d'annuaires auront à respecter pour interfacier leurs solutions au métaannuaire. ■

THIERRY JACQUOT

On demande aux métaannuaires de faire preuve d'intelligence en matière de filtrage, traitement et propagation des modifications d'information. C'est la raison d'être de modules de paramétrage avancé tels que Policy Builder, qui permet de définir les schémas de mapping, les règles de traitement conditionnelles et les ordres de séquençement des actions sous DirXML de Novell.



Le service de métaannuaire gouvernemental Maia. Dans sa première mise en œuvre, Maia (Métaannuaire de l'intranet interadministration) fédérait, par l'intermédiaire d'un annuaire X500 d'origine Critical Path exploité sur plates-formes Unix, un ensemble d'annuaires ministériels. Fin 2003, le service supportait trois millions d'interrogations LDAP par mois et cinq cent mille hits HTTP mensuels. Une deuxième itération de ce service, Maia 2, est en phase de réalisation.

Source : Adre