IT Business™

IT Business Brief

Enterprise Directories: The Key to Identity Management

by Michael Posever
PricewaterhouseCoopers

Our Mission

The mission of *IT Business* is to provide a platform for discussion and analysis of the successful use of IT to enhance business processes.

Ashton, Metzler & Associates
Leverage Technology & Talent for Success

Webtorials

Directory Services

March 3, 2004

A note from the founders

It was not that long ago that there was a lot of buzz surrounding the topic of enterprise directories. While that buzz has subsided somewhat, there has been a notable growth in interest in deploying identity management. In some cases this interest is driven by the general recognition that identity management makes good business sense. However, in industries such as healthcare and finance, the interest in identity management is also driven by regulatory requirements.

Since directory services are a key component of identity management, the growing interest in identity management necessitates our examining the state of the art in deploying enterprise directories. In order to do this, we turned to Mike Posever, an end user who has successfully deployed enterprise directories.

In this IT Business Brief, Mike Posever discusses how directories run the risk of being as fragmented as the user registries they were designed to replace. While avoiding the utopian promise of a single enterprise directory, Mike outlines a series of steps that IT professionals can take to minimize the number of directories that exist within an enterprise. As Mike points out, IT organizations that do a good job of managing directories will be positioned both to address and to capitalize on the challenges of the distributed applications era. In contrast, IT organizations that do a poor job of managing directories put the future viability of their companies at risk.

- *Jim Metzler, Ashton, Metzler & Associates*

Jim Metzler
jim@itbusinessmedia.com

Steven Taylor
steve@itbusinessmedia.com

IT Business Brief

Published by
IT Business Media.
www.ITBusinessMedia.Com

Cofounders
Jim Metzler
jim@itbusinessmedia.com

Steven Taylor
steve@itbusinessmedia.com

Design/Layout Artist
Debi Vozikis
dvozikis@rcn.com

Contact Jim Metzler
or Steven Taylor for
advertising information

Professional Opinions – All information presented and opinions expressed in IT Business Briefs represent the current opinions of the author(s) based on professional judgment and best available information at the time of presentation. Consequently, the information is subject to change, and no liability for advice presented is assumed. Ultimate responsibility for choice of appropriate solutions remains with the reader.

Enterprise Directories: The Key to Identity Management

Directories are intended to be repositories of information about the users of a system as well as the access rights of those users. The Lightweight Directory Access Protocol (LDAP) is a set of protocols for accessing directories. LDAP is based on X.500. However, as the name implies, LDAP is notably simpler than X.500.

During the dot-com bubble, directories were hot. The LDAP specification was updated 3 times in the 5 years spanning from 1993 to 1997, but it hasn't changed since. Are directories dead? The short answer is "No." To paraphrase Mark Twain, "reports of the death of directories are greatly exaggerated."

Gartner Research states[1] that Identity and Access Management technologies are "climbing the slope of enlightenment out of the trough of disillusionment". However, while that climb is occurring, the role that directories play in supporting applications is shifting. They are becoming components of a new cross-platform infrastructure – one of the shared services that underlie all applications on any platform.

Directories are still with us but they're no longer standalone products. They have been subsumed into many platforms – operating systems, e-Business suites, even databases. In short, they have been commoditized. This is both good and bad news. The good news is that directories are currently less expensive and more robust than ever. The bad news is that they are at risk of becoming information silos little different from the proprietary user registries they have replaced.

Creating a single directory to service the needs of all applications would be ideal. However, many application systems are not directory-enabled[2] ; i.e., they cannot operate without a specific directory product. Because of this, a single directory for most large enterprises is not possible. However, it is possible to minimize the number of directories in your organization.

There are three important reasons why the number of directory information silos should be minimized. The first reason is cost. Operating multiple directories is expensive.

The second reason is that in order to be truly useful, an enterprise directory must contain all of the users of all systems operated by or on behalf of the enterprise. This is important because an enterprise directory is not simply a repository for user information; it is also the repository for the access policies for those users. It is not enough to know simply who your users are; you must also be able to define what they can do. Keeping this information in different places is almost a guarantee that it will be inconsistent and therefore will compromise the integrity of enterprise data.

The third reason is because of Web Services or service oriented architectures (SOA) in general. Service oriented architectures require that users' identity and access privileges are maintained across each of the independent services that comprise an "application". Each person must be associated with a single identity context –

[1] Gartner Research. Strategic Analysis Report: "Hype Cycle for Information Security, 2003", 30 May 2003, R-19-9974.

[2] My definition of a directory enabled application is one that is directory product agnostic and can use any standards-compliant directory (via LDAP), not just the directory that is bundled with the application.

not just who they are, but also what they can do – for this to be both effective and efficient. How else can you know that "Bob" in repository "A" is the same person as "Robert" in repository "B"?

Consider, for example, how portals and application servers have been deployed in many enterprises as application integration tools. By using password vaults and other techniques "on-the-glass" integration has been achieved. But true integration means decomposing the underlying applications into services, which can then be reassembled, rapidly to create new highly customized applications. (This is akin to moving from a build-to-order to an assemble-to-order approach in a manufacturing context.) These services behave like highly specialized miniature applications. They are the sub-assemblies of the application "manufacturing" process and making them work together requires that a user's identity (and security context) be maintained in such a way that it can be passed between all of the services which will compose a "new" application. The alternative is to require a login each time. Even if simulated, the process is too slow and cumbersome to be workable.

Can this be accomplished? I believe that it can and to do so I would recommend that directory planners develop a strategy to:

- Minimize the number of directories within the enterprise by retiring existing application-level directories as soon as feasible.
- Provide for a standard means of synchronizing directory data. Multiple physical directories will continue to exist, but they must remain logically consistent.
- Develop and deploy a master directory to support the common user attribute, authentica-

tion and authorization needs of the enterprise encompassing both internal and external users of enterprise systems. This may be as simple as designating an existing system or directory as the system-of-record for user data.

- Delegate administration of directory data to the lowest-level possible within the enterprise in order to maximize data accuracy, minimize risk and ensure compliance with local policies, regulations and laws.

This is precisely the feature set that many Identity Management suites offer and is one of the main reasons that directories alone are not the center of attention they were in the recent past. These suites address data storage and synchronization and provide the ability to manage policies, subscriptions and to delegate administration of directory data throughout the enterprise. Most importantly they provide authentication and authorization functions as policy-based services. This abstracts a user's security context from a specific application – and from a specific service – and makes it re-usable.

This re-usability has numerous benefits and poses some new challenges. It reduces costs because individual applications and services do not have to include a redundant set of identity management services. This challenges IT organizations to manage their customers across a portfolio of applications rather than within a single application. It further reduces cost by creating a single authoritative source of identity data. This, in turn, creates challenges regarding the management of the personal and private information of employees and customers. It enables single sign-on and enforcement of consistent policies for access but challenges organizations to define those consistent policies and mitigate the risks posed by having one key that “unlocks” everything.

Whether your business challenge is supply-chain integration, value-chain optimization, developing a new sales channel, or deploying a corporate portal you must be able to identify your users and know what they are allowed to do – across application (and organizational) boundaries. This means being able to manage distributed applications, and is one of the real challenges – and opportunities – of e-Business.

As directories have matured, the challenges have shifted from a technology (LDAP) to a business solution (Identity Management). Though they are invisible, directories remain a central part of any e-Business strategy. The real payoff, however, is in managing them effectively. Do this well and your business will be not simply be positioned to address the challenges of the distributed applications era but to capitalize on them; do it poorly and the future viability of your business may be at stake.

Michael Posever *- is the Director of Architecture for the Global Information Technology group of PricewaterhouseCoopers (www.pwc.com) which provides industry-focused assurance, tax and advisory services for public and private clients. He can be reached at michael.posever@us.pwc.com*