



Directory assistance

Virtual directories offer a fast way to get directory-dependent applications online

News Story by Robert L. Mitchell

AUGUST 30, 2004 (COMPUTERWORLD) - The Boeing Co. has a diverse directory infrastructure that includes products like Sun ONE, Microsoft Active Directory and Oracle. Having a heterogeneous directory infrastructure in a company the size of Boeing is a practical necessity, but it also creates headaches for the aerospace company, which has 900 directory-enabled applications that serve some 150,000 employees.

The problem is that most identity management systems, Web portals and other directory-dependent applications are designed to access just one directory, but the data each requires may reside in many. Even when requested data is available in a single repository, it may not be structured in the way the application wants to see it. As a result, getting each application to work with the directory infrastructure can become a big project, says Marty Schleiff, a cyberidentity specialist at the Boeing Shared Services Group.

"Every requirement means changing an existing directory without breaking it for existing clients or setting up a new directory," Schleiff says. A third option, customizing the application, can be costly. Unlike with internal application development projects, the money spent customizing a commercial application can't be leveraged by other applications, and customization adds to the amount of code that must be maintained, he says.

To solve the problem, Schleiff is turning to virtual directory software, an emerging class of products that he says offers a more flexible approach to providing applications with access to user account data and other attributes.

Boeing has piloted and is ready to begin a phased rollout of Virtual Directory Engine from OctetString Inc. in Schaumburg, Ill. To the application, the virtual directory looks just like the target directory it expects to see. It takes requests for data from the application, retrieves it from the back-end directories, performs any transformations needed and presents it to the application in the format required. No modification to the application or target directories is needed.

"We're deploying it to support many client applications. We're trying to create a shared service," Schleiff says. Virtual directories are similar to another tool: metadirectories. Both can access user data from different repositories. Metadirectories, a core element of user provisioning tools, copy data into a new repository that must be created, maintained and synchronized. The need to keep data updated can be a headache when data in source directories changes frequently. Some business units may also object to the idea of creating a second repository for customer data that will be outside of their control, citing regulatory or strategic concerns.

In contrast, virtual directories access the attributes requested from each directory or database on the fly. The software uses a cache to speed performance but typically doesn't store data locally.

Virtual directory deployments can cost substantially less than alternative strategies. The software, licensed by the server, may cost \$10,000 to several hundred thousand dollars for a large project. But that's a small price to pay compared with the cost of rebuilding an enterprise directory or reworking each application, says Schleiff. "Anytime you're considering spending money to customize an application so that it can use your directory, you should look at virtual directory technology," he says.

The technology can even help applications that aren't sophisticated enough to deal with more complex directory mechanisms such as Lightweight Directory Access Protocol (LDAP) referrals. A virtual directory can follow the reference to locate the data and return it to the application.

But virtual directories also have a few drawbacks. Although they don't create an additional repository, they do create another layer of complexity because they require applications to access information indirectly through the virtual directory server rather than going to the directory that actually holds the data.

"There's a discomfort with adding another layer of infrastructure. If something happens to our Web single sign-on, our critical applications are down," says Schleiff. "Virtual directories ... both simplify and make the service offering more complex."

Another potential weakness: Virtual directories are only as good as the directories behind them. If a directory tends to go down frequently or offers poor response, a metadirectory that has its own data source may be a better choice. But users say virtual directories have advantages here, too. They have load-balancing and fail-over features that can be configured to redirect a request to an alternative data source. If the connection drops in the middle of a request, for example, the virtual directory retries another repository and returns the rest of the data. Starting Small Boeing is one of the first companies to make the virtual directory an integral part of its directory service, but programmers and directory specialists at many large companies have been quietly using the tools for several years for specific, one-off applications or departmental development projects.

The manager of directory services at a large family entertainment company, which he asked not be named, says a virtual directory made sense for his application for both political and technical reasons. The company uses a flat directory structure, but its identity management software expects user data to be organized hierarchically. Using a metadirectory to transform the data was out because management "really put the hammer down about replicating data to different business units," he says. Rebuilding the source directory would have required eight months, versus just one month to deploy a virtual directory. The technology provided a hierarchical view of the data "without provisioning our data all over again," he says. Choosing a virtual directory means looking at very small vendors, since the big directory players have yet to offer full-blown virtual directory products. The virtual directory vendors-about a half-dozen in all-are typically small, privately held firms with fewer than 30 employees and anywhere from five to 50 or more customers. Yet the vendors count many of the world's largest companies among their customers. "The larger and more complex the organization, the more need they have for this technology," says Gebel.

One way to mitigate the risk of going with small vendors is to leverage agreements they have with identity management software vendors and integrators. OctetString has for instance allied itself with Oblix Inc. Users can take other steps as well, says Gebel. "If you're implementing something that is higher risk, you need to take measures such as getting source code in escrow or going through a larger vendor," he says.

Another potential concern is scalability, says Gebel, although vendors disagree. While the products have been shipping for several years, they're evolving and have yet to prove themselves in many large-scale deployments, he says.

But those concerns don't bother Gebel. He says he plans to use the technology as part of a broader, single-sign-on project involving more than a half-dozen directories. "Because we aren't tied down to a true directory ... it's easier to add repositories as time moves on."

