FEATURE

Master Class

By: Michelle Kraus

Wanted: Cyber-glue for authentication Answer: LDAP

OpenLDAP is gaining importance day by day. From what I've seen, OpenSource LDAP v3 can help IT departments solve authentication issues. Case in point? Its use in an ISP setup, a challenging scenario on a number of fronts.

Information executives in any type of business sooner or later meet up with the major system-administration hurdles involved in updating all user profiles.

As you read this, it is some new employee's first day of work in some organization. Although HR has done all its paperwork, no network login has yet been created for the person, nor does the individual yet have an e-mail account. But these tasks are trivial. These needs will be resolved easily by the time the new employee returns from lunch. Other access items remain, however. In the afternoon, the employee will need to get into the corporate Intranet and CRM system, while tonight the same employee will need a Unix login and access to the dial-up server to access the corporate network from home.

Visit a week later, and we find that he can do his job as efficiently as any of his other colleagues. But there's one more glitch: Three months down the road, a colleague from another office will look for the newcomer's phone number. The number will not be found in the telephone list, a directory maintained by a secretary who was on a two-week vacation when the employee started work.

No single point of contact to make these changes all at once? No. For each of these applications, a different person had to take a different action. What's more, some of the user data is stored in a relational database, some of it in a flat file, and still more of it in a proprietary application. Yet another three months later, and this employee will decide to leave the

company. How much of his data will stay in the corporate records? How much should be removed?

And so it goes. **In any medium-sized enterprise, creating and removing users in different applications can be a full-time job for one or more people, as today's norm is one of networks running multiple operating systems and messaging platforms, each with its own directories of user and resource information.**

Authentication is a problem that every IT manager needs to address. Enter LDAP, the Lightweight Directory Access Protocol, which is used to access directory servers. The directory is a special kind of database that holds information in a tree structure. Proponents call it the premier method for standards-based network directory access. **LDAP v3.0 describes a directory-access system that behaves as the common meeting point that glues together users, services, and management.**

LDAP is used for portals, intranet, and extranet applications, using an LDAP-based directory in which to store user information. LDAP works because it is a flexible environment that can and should be adapted to a company's information structure. LDAP is more than just a database to which users can authenticate; it is a central repository where managers can store certificates and user information such as physical location and telephone numbers all in one place. As the way a user control is managed, **LDAP can be fashioned into a central repository for not only employees, but also the company's contractors, clients, and suppliers.**

But the use of LDAP, like any piece of the information-technology puzzle, takes careful business analysis as well as technology know-how. Setting up LDAP is only part of the challenge. Most important, security planners need to analyze their specific needs:

- Making a checklist-Where do you need authentication? Who is currently responsible for maintaining the different directories? Who should be responsible? Which users get which kinds of access to which applications?
- Designing the directory tree-Mapping a directory schema to your enterprise needs will be the most difficult phase of an LDAP integration. Be sure to build in enough time. At the same time, note that designing an LDAP schema isn't an exact science. There is no perfect mathematical solution.

Ample information about implementing LDAP is now available on the Internet, as our accompanying resource kit indicates. Most other programs, such as ERP packages, have some sort of LDAP integration. What's more, there are numerous Web browsers, e-mail packages, and other applications that have signed on to the LDAP standard. If your application hasn't, ask your vendor to implement it.

What about LDAP in an Open Source construct? OpenLDAP is gaining importance day by day. From what I have seen, OpenSource LDAP v3 can help IT departments centralize and solve authentication issues. Case in point: Consider its use in an ISP setup, a challenging scenario on a number of fronts. There are bound to be lots of users. Remember the 35K-user

entry limit? You can't store 300,000 users in an /etc/passwd. Users need a home page, dial-in access , pop3, Web mail and Web access through a proxy. Right there are at least five different places where they must be authenticated. In a perfect architecture, you will find an OpenLDAP server where all users are stored.

All

LDAP RESOURCE KIT (faq, how tos)

- www.umich.edu
- www.linuxdoc.org
- www.umldap.com
- www.openldap.org -OpenLDAP's project team manages the software development process, augmented from time to time with outstanding contributors. The goal is to develop a commercial-grade, fully featured and Open Source LDAP suite of applications and development tools.

OpenSource tools integrate with OpenLDAP. **Integrating OpenLDAP with familiar tools such as Apache, pam, squid, or Samba, for example, should not cause any problems.** For uploading and pop3 access, pam does well authenticating against the LDAP tree. Dial-in access can use radius mapped against an LDAP. Web mail can be accessed using the Apache Auth_ldap module. The proxy authentication process uses LDAP Authentication for Squid.

Once you solve the authentication problem you will have to start wondering what SSO means. And no, it is not Singapore Symphony Orchestra or Solar System Online. Stay tuned.

-Kris Buytaert is a Belgium-based consultant for IPNG (IP Net Generation), which is in the business of performing architecture design, Web development, and network security.

< | Last Rage >