

# Network Computing®

AUGUST 4, 2005 | WWW.NWC.COM *For IT By IT*

## Sneak PREVIEW

### Wow Factor Revealed

Red Hat's open-source LDAP for the masses

BY JOHN H. SAWYER

good

- Easy, centralized management with Red Hat Management Console
- Open source
- Compliant with LDAP 2 and 3
- Supports additional operating systems other than RHEL

bad

- Setup doesn't include RC start-up scripts
- Documentation is immense

**W**ho would pay millions to acquire proprietary software simply to release it as open source less than a year later? Red Hat, of course. In September 2004, the company entered into an agreement with America Online to buy various technology assets of AOL's former Network Security Solutions unit, including Netscape Directory Server. Red Hat is now commercially releasing that server, replete with a fresh management console and modifications under the hood, as an open-source product under the name Red Hat Directory Server.

Compatible with LDAP 2 and 3, the Red Hat offering creates a centralized network repository of application settings, user profiles, group data, policies and access control information. It supports 32-bit Red

#### Network Computing Exclusive

Hat Enterprise Linux (RHEL) 3 and 4, 32- and 64-bit Sun Solaris 9, and 64-bit HP-UX 11i.

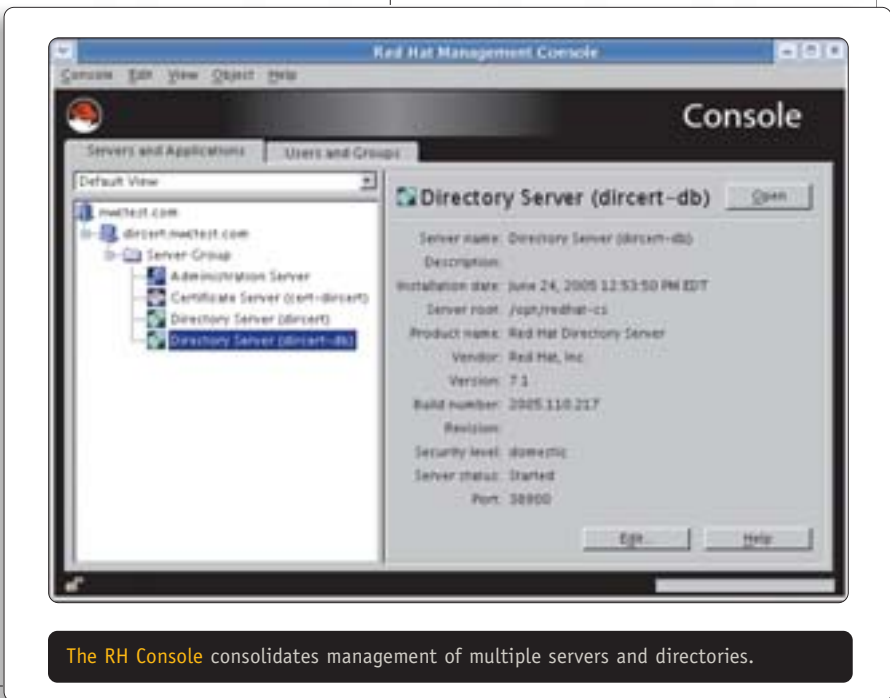
I tested a version 7.1 beta of Red Hat Directory Server at the NETWORK COMPUTING Real-World Labs® at the University of Florida. Setup was easy, and after installation of the RPM, the "setup" executable was run from the /opt/redhat-ds/setup/ directory.

#### See the Manager

The Management Console is a

GUI that connects to the Red Hat Administration Server, a Web server providing a common management framework between Red Hat products like Directory Server, the soon-to-be-released Certificate System and the Administration Server. From the GUI, you can configure the Administration Server, Directory Server or individual directories. It also lets you create or clone directories, as well as manage user and group functions.

I created three new directories that could all be managed through the same instance of the Console. Clicking on a directory provided a status window showing server name, description, installation date, server root, build number, running status



The RH Console consolidates management of multiple servers and directories.

# Sneak PREVIEWS

and network port. The “open” button brought me to detailed management tabs for simple tasks, such as stopping and starting the directory, and for more advanced functions like replication configuration, logging, plug-ins and encryption.

Surprisingly, there was no way to start the server automatically during boot-up. Considering that Directory Server is a Red Hat product, I expected it to include an *rc* script allowing for this, in addition to easy start, stop, restart and status functions.

## Replication Station

I created three clones of my original RHEL 4 virtual machine and set up Directory Server on each to test the multimaster replication scenario detailed in the Administration Guide provided. Each server acted as a “consumer” and a “supplier” of data to the others in the replication process, meaning directory information modified on one server was quickly replicated to the others. When the same information is modified on multiple servers, Directory Server resolves the conflict by treating the most recent change as the valid one.

To add users and groups, I tested both the Console and *ldapmodify*, a command-line tool that is part of the OpenLDAP tools package I installed. It was easy to modify directory content in the Console GUI, which meant I didn't have to become overly familiar with *ldapmodify*.

Large-scale directory population is best accomplished by importing data in LDIF (LDAP Interchange Format). If there's a problem, as I experienced, the process provides and saves excellent feedback about any data that can't be imported in a separate file for troubleshooting. I checked out the feedback, and after a quick reconfiguration of my directory, 650 pieces of information instantly imported

into my empty directory.

Directory Server's ACIs (access-control instructions) let you configure security as granularly as you'll ever need. From the point-and-click interface, I designed ACIs with user access limits, including types of access, access targets, hosts from which access is gained and a schedule of when access is allowed.

Directory Server's manual recommends adding ACIs en masse through an LDIF import, but the syntax can cause confusion if you're not familiar with LDAP. Thankfully, Red Hat provides extensive documentation on the LDIF ACI syntax.

I configured the RHEL 4 client to retrieve user authentication information from Directory Server. On modern Linux distributions, this type of setup is simple and requires only two checkboxes, though older RHEL distributions or similar may require more advanced configuration to make this work. On the server side, I used the Console to modify the account profile to include the proper UID, GID and home directory in the Posix User tab obtained from the local RHEL 4 client. Then I logged out of my current user and logged in with the “John Doe” user credentials previously set up. As my user, I set up the Evolution e-mail client to use the Directory Server as an LDAP-based address book. When I created a message, the option to search the LDAP directory was enabled, and typing in “Doe” led me to John Doe's e-mail address in the directory.

## Windows Integration

To check out Windows integration, I tested PGina 1.8.1—a replacement for the regular Microsoft Gina that uses plug-ins to provide additional authentication methods—with the LDAPAuth 1.5 plug-in for LDAP authentication. I easily logged on to my Windows XP with the John Doe credentials. Next, I configured Soft-

ra's freeware LDAP Browser 2.6 to view the directory remotely and had no problem digging through the LDAP structure. With the administrative version of Softerra's product, I'm sure that adding, deleting and modifying data would be just as easy.

Directory Server boasts advanced functionality for synchronization with either Windows Active Directory or the Windows NT 4 SAM. However, I couldn't get the two services to synchronize, even after following every step in the Administration Guide. The product's beta status may have been the reason, though another possibility is that Directory Server was incompatible with the Fedora sync-enabling tool I had downloaded.

Documentation was comprehensive, but a little too much to take in when you're trying to set up the product quickly. I'd like to see Red Hat put together a special “Quick Install Guide” for those who just want to drop in a disk and go.

Overall, Red Hat Directory Server is a solid entry into the enterprise directory market and will only get better as it matures through the Fedora open-source development project. And because it is LDAP-compliant, it's easy to drop into an environment using LDAP, or it can be easily set up where LDAP is being introduced. If it's missing a feature you're looking for, its open-source status means it can be modified to do exactly what you want. With the upcoming Red Hat Certificate System, Red Hat is working to gain a larger foothold in your organization.

■ **RED HAT DIRECTORY SERVER 7.1**, \$15,000. Red Hat, (866) 273-3428, (919) 754-4366. [www.redhat.com](http://www.redhat.com)  
*John H. Sawyer is the systems security engineer for the Institute for Food and Agricultural Science statewide network at the University of Florida. Write to him at [jsawyer@ifas.ufl.edu](mailto:jsawyer@ifas.ufl.edu).*