Samba Does Windows-to-Linux Dance

Alexander Wolfe, Science Writer

With heterogeneous networked environments becoming the rule rather than the exception, there's more need than ever for Windows and Linux to work and play well together. Enter Samba, the print- and file-sharing tool that enables files residing on Linux hosts to interact with Windows-based desktops.

Samba, an open source effort that's freely available under the GPL (GNU General Public License), first hit the streets in a 1994 release written to support Unix. Its march toward common usage began in the form of deployments on servers running popular open source implementations such as HP-UX, IBM's AIX, and Sun's Solaris.

In recent years, the rampant rise in usage of Linux in the server world has catapulted Samba into almost ubiquitous deployment. (In typical setups, Samba serves as the missing link, allowing client desktops running Windows to access files stored on such Linux servers.)

Indeed, the fact that Samba ships as a standard part of nearly every Linux distribution has given the software a stealthy penetration that's surprisingly large. There may be as many as 14 million to 16 million Samba servers in use in various forms. To break the numbers down more meaningfully, however, not all of those setups are "high-stress" environments. Estimates peg the number of large Unix and Linux installations (defined as hundreds or even thousands of users per server) running Samba at somewhere between 2.5 and 3 million.

According to its FAQ, Samba "is a suite of programs which work together to allow clients to access a server's filesystem and printers via the SMB and CIFS protocols" (see figure 1). The SMB (Server Message Block) protocol was invented by IBM in the 1980s and extended by Microsoft. Microsoft renamed SMB to CIFS (Common Internet File System) during the 'Net frenzy of the 1990s.

In terms of its functionality, Samba consists of two key components: `smbd` (server message block daemon), and `nmdb` (name resolution and browsing daemon). Both implement CIFS file-and-print services.

So just why should Samba, which seems to have a fairly narrowly defined mandate, be of interest to the developers? Because it offers a window into the intricacies of networking and can provide developers with a virtual

Mounting remote

LINUX DRIVES UNDER

WINDOWS IS EASIER

THAN YOU THINK.

front-row seat for the handling of intercommunications among heterogeneous interconnected systems.

SAMBA 3

That's evident in Samba 3, the latest revision of the tool, released in September 2003. Samba 3 adds full-fledged domain control support (minus Microsoft's security account manager database replication) for the still widely used Windows NT 4 operating system. Domain support means Samba essentially mirrors the architecture by which NT stores user account credentials. Thus, Samba has a means for deciding whether to grant accredited users access to server-based files, enabling the Linux-to-NT interoperability.

If that description seems arcane, consider that, according to Josh Malone, a NetBSD and Windows system administrator, "Samba seems to just be one of those packages that you just need to see in action to understand."

Malone made his comment in a Slashdot.org review of a new book, *Samba-3 by Example* (Prentice Hall, 2004), written by Samba team member John Terpstra. Terpstra suggests that an understanding of Windows networking functions can shed light on the precise mechanisms by which Samba allows a host Linux or Unix server computer to interact rather transparently with a Windows client.

Terpstra recommends that nuts-and-bolts professionals obtain a copy of the free Ethereal network protocol analyzer tool and use it as a sniffer to capture and review the packets traveling across a network to get a peek under the covers. As Samba runs, it makes use of information buried in thousands of those packets about the identity of the Windows clients on the network.

SECURITY

For the Samba user, this knowledge may whet the appetite for a broader understanding of the intricacies of Windows networking. This in turn may raise the red flag of security—an issue of burning concern, especially in the area of interoperable networks. There's an ongoing debate about the relative security advantages of Windows and

Linux, with open source advocates blasting Windows as being inherently weak because it's a closed system that's not subject to scrutiny by the software developer community. (Microsoft makes the counter argument that protected source code is more resistant to exploits because hackers don't know what's in it—precisely the reason that the public posting of open source code raised alarms in Redmond.)

I queried Samba team member Terpstra about how system administrators of heterogeneous environments grappled with perceived security differences between Samba/Linux and Windows. "Interesting question, because you'll find that views on that are poles apart," says Terpstra. "Windows-style networking is inherently insecure. The reason is, the ability to browse, or to go into your 'network neighborhood' and see all of your machines, is based on a broadcast technology."

You might argue that each Windows machine assumes a trusting environment, and so doesn't mind announcing itself to all the world. The obvious problem is the all-too-familiar *untrusting* environment. To be fair, this is a mistake that plenty of groups other than Microsoft have had come back to bother them. Witness the e-mail spam epidemic, a problem that arguably stems from an early premise that e-mail would be sent between trusting parties (who could ever want to send you e-mail that you

didn't want and spoof the return address?).

Via such broadcasts, machines send packets across the network identifying themselves and their IP addresses. As a result, anyone with a sniffer capable of capturing traffic, even if they don't have administrative privileges, may be able to hack into the network.

"To the Unix security buff, that is a no-no," Terpstra says. "The server is advertising itself to the world."

Fortunately, Samba implements features to shield the operating system from the user as much as possible. Additionally, because Samba is resident on non-Windows server platforms and doesn't implement all the features of Windows, it's able to cut out a lot of potential exploits for Windows, according to Terpstra.

Though Microsoft has no specific involvement with Samba, it too is concerned with security. Seeking to minimize the ability of hackers to exploit Windows, Microsoft is working hard to design improved security into its next-generation Longhorn operating system, due in 2006.

"With Longhorn, there's a good possibility that Microsoft will introduce entirely new technology," Terpstra says. "I believe that is entirely appropriate, because the current Windows networking technology is fundamentally insecure. It's grown topsy-turvy over many years. It's probably more cost effective to start with a clean slate than to try to fix the ills of the current technology."

Microsoft is expected to buttress security in Longhorn by overhauling the basic Windows file system with a new model dubbed WinFS. Because Microsoft's file systems are proprietary, and because it isn't likely to open up the new file system, the Samba team will have to work hard to enable the software to maintain interoperability between Unix/Linux and Longhorn.

Terpstra says the Samba team doesn't yet know fully what the consequences of WinFS will be. But it is prepared to introduce support for any WinFS or Longhorn protocol extensions into Samba.

SAMBA 4

Indeed, Samba is already being upgraded to make it more adaptable to emerging technologies. The next version of the package, Samba 4, has been in development for about a year and is scheduled for release within 12 to 18 months. "It constitutes a very significant reengineering of the Samba technologies," Terpstra says. "It introduces the capability to support newer technologies that will be very valuable going forward, [including] support for the full semantics for any file-system type you might need to handle."

According to a recent presentation by Andrew Tredgill, a founding author of Samba, another major design goal of Samba 4 is to make it much easier to install and configure. For clear evidence that that will be welcomed, you need only turn to the linux.samba newsgroup, which is filled daily with nitty-gritty configuration questions posted by sys admins. Tredgill's other design goals for Samba 4 include the move to flexible process models and a flexible database architecture, and the streamlining of the package's suite of test support code.

INTEROPERABILITY WITH MICROSOFT

As Samba looks ahead to Longhorn, another issue is whether the software will remain free, or whether the changing intellectual-property landscape could throw up roadblocks to interoperability with Microsoft-based clients. Historically, Microsoft has not opened up its networking specs; however, neither has the software giant imposed any restrictions on Samba. It's widely accepted that everyone's interests are best served if Unix, Linux, and Windows machines can talk to each other.

This brings up an obvious question: If Microsoft hasn't opened up its specs, how has Samba been able to build in the ability to interoperate with Windows? The answer is, the same way x86 clones have been able to mimic Intel's hardware architecture, which isn't completely documented for public consumption either: via a combination of working off of those portions of Microsoft's networking specs that have been documented in bits and pieces and written up in disparate documents, by drawing on the empirical knowledge and experience of networking experts on the Samba team, and through heuristics and real-world testing.

Though it will remain in Microsoft's interest to enable Longhorn interoperability, a new issue may be arising on the intellectual-property landscape. In a March 2004 antitrust decision by the European Union, Microsoft was fined for monopolistic behavior. The EU also said, however, that Microsoft may be allowed to pursue future

RESOURCES

Main Samba Host Site

This page points to the organization's Web mirror sites and download servers
<http://www.samba.org/>

Samba FAQ

<http://us1.samba.org/samba/ftp/docs/faq/Samba-meta-FAQ.html#introduction>

Samba 4

Presentation by Andrew Tredgill
http://us1.samba.org/samba/ftp/slides/sambaxp04/tridge_samba4_sambaxp04.pdf

Ethereal

Free network protocol analyzer tool
<http://www.ethereal.com>

licensing revenue from APIs (application programming interfaces) it publishes. This decision could potentially impact Samba, since it interoperates with Microsoft APIs.

Practically speaking, Terpstra doesn't see Microsoft extracting royalties from Samba. "The Samba team is not a financially driven business, nor does it have a structure by which it may participate in the payment of fees for licenses and/or royalties," he says. "In my opinion, the European Union ruling will drive Samba development away from Europe and further toward those nations and states that are not so willing to offer restrictive and protective monopolies."

Whether uptake of Samba overseas becomes driven by politics such as the EU ruling remains to be seen. Nevertheless, over the next few years Samba may well see its biggest deployments in areas where the adoption of Linux is growing by leaps and bounds. These include Japan, China, India, and the former Soviet-bloc countries. Q

LOVE IT, HATE IT? LET US KNOW

feedback@acmqueue.com or www.acmqueue.com/forums

ALEXANDER WOLFE received his electrical engineering degree from Cooper Union in New York City. A science writer based in Forest Hills, New York, he has contributed to *IEEE Spectrum*, *EE Times*, *Embedded Systems Programming*, and *Byte.com*.

© 2004 ACM 1542-7730/04/0700 \$5.00