Remote possibilities

Thanks to remote network administration, your Web master need not fly to the US every time he wants to configure your Web site

Imagine a company with offices spread over various buildings in your neighbourhood and only one system administrator to look after those 200-odd computers. Physically visiting the site for maintenance of each machine can be very taxing on the administrator. He can, however, work around this problem by remotely configuring the machine. While anything that involves physical handling will obviously not be possible, remote administration via the network can save a lot of energy and time.

Things to do

Primarily, three categories of functions can be carried out remotely:

Service management: Allows an administrator to control the services a server offers to a client.

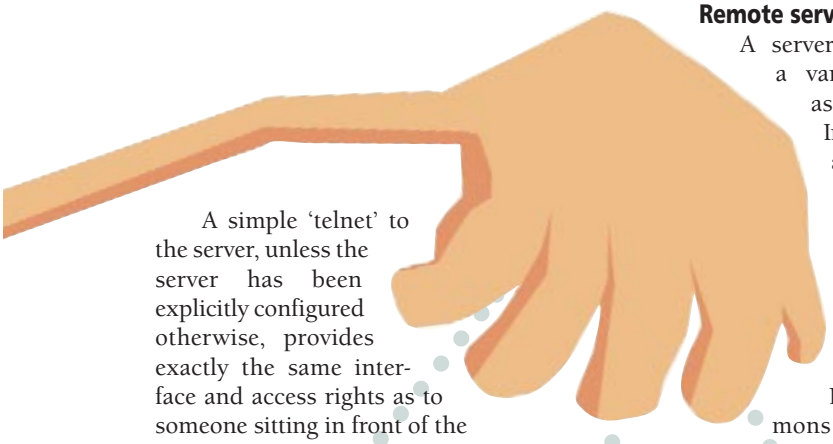
Network management: Configuration of a server or client's (user's) network.

Hardware management: The ability to control hardware through software, such as rebooting a machine or conducting hardware diagnostics.

What you need

The first requirement is a link between the machine to be administered remotely and the administrator. This link may be a Local Area Network, a dedicated modem and dial-up line, or the Internet. For security reasons, the type of access rights available may vary with the type of connection used to access the server.

Next, the machine being administered needs to support remote administration. With Linux (and other Unix derivatives) this is not an issue since the system inherently supports it.



A simple 'telnet' to the server, unless the server has been explicitly configured otherwise, provides exactly the same interface and access rights as to someone sitting in front of the machine. Owing to the design of the X-windowing system (*See box 'Formula X'*), a graphical user interface can also be used remotely without any significant differences. Windows NT inherently supports remote access too, but is relatively limited.

Some machines can report any hardware failure to the operating system (these machines traditionally ship with Windows NT, but other options are available now).

Logging such information can help an administrator work remotely on hardware problems, without having to spend time diagnosing the problem first.

Remote service management

A server may be used for a variety of purposes—as the company Intranet Web server or a background back-up server—and using remote service management, the administrator can decide what services to offer its clients. Services under Linux are called daemons (Greek for messenger between the Gods and the people), while Windows NT unimaginatively sticks to the name 'service'. Both operating systems allow services to be remotely configured, started and stopped.

Managing network configuration

Managing network configuration comprises two parts: controlling what the client uses for its configuration and managing the network servers—which make the configuration information available to client PCs.

The popular NetWare IPX/SPX protocol, now obsolete, automatically handled client configuration, as did NetBEUI, Microsoft's popular but poorly designed and now abandoned network protocol. The present standard, TCP/IP, requires manual configuration at the client-end. On Linux, this is done using the console. On NT, the `Network Properties` item from the `Control Panel` is used locally, and the `Registry Editor` remotely.

Configuring TCP/IP involves assigning a unique IP address to every machine. This is no issue when dealing with five to ten computers, but increase the number to 200 and it starts to get problematic. Now every time a machine is configured and assigned an IP address, the administrator will have to check that the particular address is not already in use.

Doing an immediate check on the network for another machine with that address will not work all the time because that particular machine may have been turned off at that time.

Fortunately DHCP or the Dynamic Host Configuration Protocol, the same protocol that your ISP uses to assign you an IP address when you go online, makes client configuration mostly automatic. DHCP allows client computers to request all the information they want via port 547 of the User Datagram Protocol (UDP), the counterpart to the Transfer Control Protocol (TCP, of TCP/IP fame).

However, regardless of how it is configured, TCP/IP depends upon name resolution to convert between domain names and IP addresses. It does so by using the Internet-standard Domain Name Service (DNS) or the Windows Internet Name Service (WINS). Windows NT server comes bundled with support

LIKE A HOLE IN THE HEAD

Back Orifice (the name is a pun on Microsoft s Back Office), is well known as a trojan for taking control of remote W indows machines on the Internet. Creators Cult of the Dead Cow (www.cult-deadcow.com) however, officially describe Back Orifice as a remote administration tool. Back Orifice consists of a server for use on user machines and a client for use by the administrator. The client portion has both Windows and Unix (and Linux) flavours and connects to the server using a pre-determined network port (the default is 31337). The server part needs to be configured by the administrator and manually installed on the user s machine. The administrator can optionally make it invisible to the user. Once the client and server portions make contact, the client has near-total control over the user s computer. Using the client, an administrator can navigate the file system, control file sharing, edit the registry, control running processes (applications), capture screen display, reboot the system if necessary, and even display a notice to the user. Back Orifice is a particularly useful tool because it

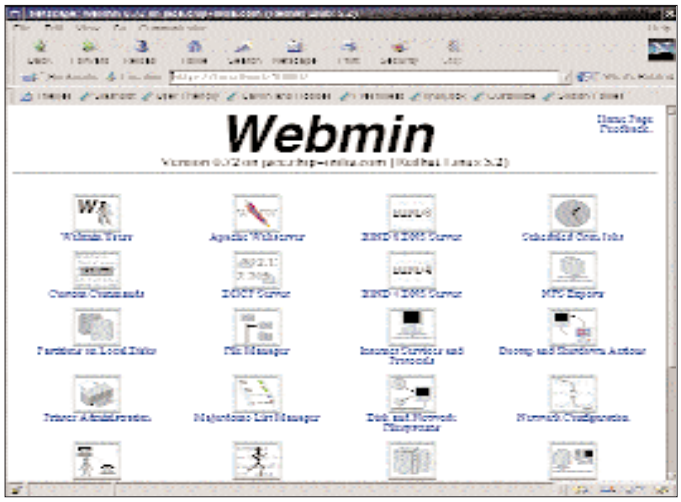
for these two protocols, as services. Linux supports DNS and WINS using BIND (Berkeley Internet Name Daemon) and Samba (a pun on the Windows SMB protocol), respectively. BIND and Samba come as part of all major Linux distributions. Windows NT requires separate management applications namely DNS Manager and WINS Manager to remotely control the DNS and WINS services. With Linux, configuration is again controlled from the console.

Web-based configuration

Back in the dark ages of computing, command line interfaces were the only way to get things done. Then graphical computing burst upon us and everyone started to point and click, but system administrators of the Unix school still stick to the command line, insisting that no graphical tool can beat the speed, flexibility and remote usability offered by the command line. Several attempts have been made to change this scenario and the most advanced so far is WebMin, an HTML-based system configuration tool that works with a wide array of Unix-like operating systems. It is up-to-date (works with even Red Hat 6.0 which is barely two months old), and can configure just about anything.

Linux programs use individual, inconsistently formatted configuration files. These files are kept separated from each other (unlike the registry in Windows) to help reduce the chances of accidental loss. The inconsistency is necessary to take full advantage of the program's abilities. This however is disturbing for the inexperienced administrator who has to spend many frustrating hours finding configuration files and then learning to modify them. WebMin smoothens this problem by providing a list of all available modules right at the start, and then using individual modules for individual configuration files, and designed to make possible everything that the configuration file allows, graphically.

Among the various configuration modules included are for the Apache Web server, the BIND DNS server, the Cron scheduler, the DHCP server, the hard disk partition table (that's right, WebMin allows remote disk partitioning!), printer configuration, the Majordomo mailing list manager, general network configuration, disk quotas (like the 500 KB that VSNL imposes on shell account users), the Samba Windows Network Neighbourhood file sharing server, the Sendmail Internet Mail Transport Agent (MTA), the Squid proxy server, general software installed on system, and user accounts and passwords. WebMin also includes a Java-based file manager, thereby making it possible for an administrator to remotely navigate the file system using a Windows Explorer-like interface.



The main screen of WebMin, as seen in Netscape on Linux

Network monitoring

Like network configuration, network monitoring involves two parts: the device being monitored, and the device doing the monitoring. The device under scrutiny usually makes information available to the supervising device through the Simple Network Management Protocol (SNMP) or at times, through a variety of vendor-specific proprietary protocols. The information available through SNMP depends upon the specific components that are using it.

Under Linux, the '/proc' section of the file system contains detailed information about running processes, the CPU and the file system. This information can be reported using SNMP and can be used to evaluate the performance of a system. Windows NT provides the same via a tool called Performance Monitor, which is capable of simultaneously monitoring and archiving data from both local and remote machines at a time.

KIRAN JONNALAGADDA

FORMULA X

The X windowing system, the standard graphical user interface system for Unix-like operating systems, can be a real boon to the remote system administrator. Designed at MIT s Project Athena to provide a standard windowing system based on open standards, X makes graphical interfaces possible when communicating with remote servers.

X s design uses an inverted client-server model an X server running on the user s machine displays graphical output from the client application running on the remote machine. This allows a system administrator to run a graphical configuration utility on a remote server on the other side of the world and see the display on the local machine with no apparent difference except for the latency due to bandwidth limitations. Implementations of the X server are available on almost all Unix-like OS distributions (including Linux), Windows and MacOS. There is now even a Java version that can run in your Web browser.

However, in spite of sounding like a dream come true, X is not. Apart from being very bandwidth intensive, X is low on security levels. X allows applications to grab screen displays or capture keystrokes, which means that a rogue application can also connect to your X server and monitor all your activities. Further, the transmission channel between server and client is unencrypted, allowing anyone with a packet sniffer to capture the data stream and scan