

Open Source in the Enterprise

When is deploying Linux the better option in a corporate network? In this article, I will look at how Linux can be the option of choice, even in an otherwise proprietary environment. Specifically, I will highlight the different advantages of deploying the Linux server platform in IT environments characteristically rich in Microsoft Windows.

Organizational Needs

We rely on corporate computing systems to provide:

- communications, typically via email and website,
- data storage, documents and databases, and
- application access, many of which have become based on HTTP/HTTPS or web technologies.

We rely on computing systems for background or hidden services. These are the services which support the visible services end users expect. These can include backups, email filtering, user access control more commonly called directory services, and domain name services (DNS). More sophisticated organizations may also have services specific to network devices, such as log management and configuration back-up.

A Little about Linux

The differences between the Linux operating system and Windows or other proprietary systems give each a strategic advantage, and understanding these can help you to choose the right solution. Think of it as knowing when to use a screwdriver instead of a chisel.

Linux differs from Windows in two major ways. It doesn't have a registry; everything is stored as a file. And, Linux, based on UNIX, has been around for years, and is known for its stability. A third overly discussed difference, that Linux is available for free, is not the focus of this article.

Where Windows Works

Microsoft Windows is the popular choice in operating systems, especially in corporate environments—there is no arguing against that. And, there are advantages to deploying it. With this popularity comes a high availability of IT professionals who can support the Windows environment. Microsoft has also put together a very effective directory service called Active Directory.

Linux Advantages

Linux outshines Windows in the manipulation of flat text files. The Linux command line allows for a succession of commands to be executed as one command. These commands typically operate as a Boolean 'and' via the pipe command, represented by the "|", a symbol normally found above the Enter key. I use pipe to separate text filters by linking the grep command s to comb through logs files looking for an incident. See our knowledge base article for details. [Linux Files - Parsing #1](#)

Linux comes with a graphical user interface or GUI but it is not required. Turning it off leaves the hardware free to efficiently perform your tasks, without being swamped by continuously redrawing the graphic display.

Linux can perform tasks on less hardware than Windows, so the initial hardware outlay is lower. This can allow you to recommission older hardware.

Places for Linux

Linux is more ubiquitous than you might think. You may already have instances running within your corporate environment. I'll run through a few instances you may recognize.

Email Filtering

If you have a commercial email filter, such as Barracuda, you already have a Linux box in your environment. Or you can build your own email filter system. The basic tools available in the open source arena are; GreyList-milter, SpamAssassin and ClamAV.

- Grey Listing: Your grey list will tell the computer sending in emails to try again in a specified number of minutes. This works as a filter because the typical SPAN-BOT PC can't accept such a request: it doesn't have a mail queue and so that mail is never returned. Only servers with a proper mail queue will retry allowing legitimate email to come in.
- SpamAssassin: This tool ranks email based on header and body content. Each element adds to a cumulative score. If the final score reaches a specified threshold, the email is flagged as spam.
- ClamAV: ClamAV is an antivirus scanner which will stop email from reaching the intended recipient if a virus is detected.

Web Server

Since the mid-1990s, Apache has been the dominant and unchallenged web server on the public Internet. Once you tie in a database and CMS, which are available license-free, you can have a Linux-based web development platform for only the cost of the hardware and the talent. Due to the no cost, open license nature of Apache many network appliances and hardware management systems use Apache for browser based management.

Domain Name Services (DNS)

BIND (Berkeley Internet Name Domain software) is the DNS server distributed with every Linux distribution. BIND was created in the early 1980s. It is one of the most popular DNS server packages out there. Ten of the 13 Internet Root servers run BIND. While you may not be running an Internet Root server in your environment, anyone inside the organization using the Internet is relying on them.

More Places for Linux

Now I'll introduce you to some areas in your organization where Linux is the platform of choice.

Log Server

As I hinted at earlier, storing log files from network devices is a perfect task for a Linux server. Log files are the security camera of the network. Log files tell you what happened in the past and allow you to piece together with more clarity if and how an incident took place. It is important to note that nearly all network devices lose their logged data when they are rebooted, making a separate log file server a valuable asset.

Bandwidth Recorder

Enterprise network switches, routers and firewalls maintain a number of different counters for each physical and logical interface. The counter types include; packets in/out, bits in/out, octets in/out and errors. Each of these counters can be queried and recorded. An application called 'The Multi Router Traffic Grapher', or 'MRTG', is perfect for recording these counters and providing pretty pictures of the resulting values. Again, storing these data logs on a Linux server can assist when the primary assets are power cycled.

Configuration Repository

Enterprise network switches, routers and firewalls typically have text-based configurations. Manually maintaining these configurations off-box is difficult and arduous. The application 'Really Awesome New Cisco confIg Differ' or RANCID automates this process. RANCID does more than just collect configuration files from Cisco. RANCID also works with Alteon, Bay Networks (Nortel), Extreme, Force10, Foundry, HP Procurve switches, Juniper Routers and edge (ERX) routers, Redback, MRTd daemon, Lucent TNT, Citrix NetScaler load balancers, Netscreen firewalls, Zebra routing software, and the ADC-Kentrox EZ-T3 mux. RANCID mimics an administrator login to issue commands and provides the returned output back to the system. RANCID only runs on Linux or UNIX and like the other tools mentioned it is free.

By combining the previous three applications, SYSLOG + RANCID + MRTG, we can build a Network State Server (NSS). For more information on the eSubnet NSS refer to [Application Services](#).

Maintaining logs files on a platform different from your principle file storage operating system helps guard against corruption in the event of a virus or worm outbreak. Viruses and worms are typically targeted at a single OS or application.

Conclusion

For IT environments rich in Microsoft, a Linux-based application server is best positioned as a 'set it and forget it', customizable appliance. Commercial network application appliances are often expensive, overly complicated and have more features than are required. Linux-based solutions can be used in the enterprise as simple network monitoring appliances. They can also be deployed as proof of concept for larger endeavors as Linux allows for a lower initial capital expenditure due recycled hardware and zero licensing fees. So the next time you are looking to gain a little insight into your network or if you are looking to provide a proof of concept, consider Linux. It can save you money.

Originally published May, 2010

About the Author

Richard Danielli is the founder and President of eSubnet Enterprises. He has broad expertise in the fields of networking and data security. Based in Toronto, eSubnet provides superior customized solutions for networking and data security. Additional articles are available at <http://www.esubnet.com/fragment.html>.

Reprints

1. Commercial use: Commercial newspapers, magazines and websites that wish to reprint an article should contact eSubnet for permission.
2. Non-Commercial use: Any reproduction of content (excerpt or full text) by nonprofit organizations or companies wishing to share information with their members or clients requires that you notify us, whether for print or online usage.

Regarding reprints, contact Mr. Danielli at [rdanielli\(at\)esubnet.com](mailto:rdanielli@esubnet.com) or at (416) 203-1223.