IBM®

L08

Replacing Windows Servers With Linux

Mark Post

zSeries Expo	Nov. 1 - 5, 2004

Miami, FL

Agenda

- Reasons to move away from Microsoft Windows
- What Windows functions can be replaced?
- What can replace those functions?
- What training will be needed?
- Migration considerations
- The downside to migrating

Reasons to move away from Microsoft Windows

- Windows NT 4.0 is at End Of Life
- Increased hardware costs
- Increased software costs
- Microsoft Licensing 6.0
- Continuing security problems

What Windows functions must be replaced?

- Active Directory
- Domain Controller
- DNS
- DHCP
- Windows Internet Name Server (WINS)
- File and print server
- FTP server

- HTTP (web) server
- Web Application Server
- Remote Access Server (RAS)
- Email server
- Groupware (calendars, etc.)
- Database server
- Proxy server/firewall

What can replace those functions?

Active Directory	Kerberos, OpenLDAP
Domain Controller	Samba
DNS	BIND
DHCP	ISC DHCP
WINS	Samba
File and Print Server	Samba

What can replace those functions (2)?

FTP Server	ProFTPD, vsftpd
HTTP Server	Apache, thttp
Web Application Server	Jboss (EJB), Tomcat/Catalina (servlets, JSP), WebSphere, Weblogic, iPlanet
Remote Access Server	pppd, Radius

What can replace those functions (3)?

Email Server	Exim, Postfix, Sendmail, Insight, IMP
Groupware	Insight Server
Database Server	MySQL, PostgreSQL, Informix, DB2, Oracle, SAPDB
Proxy	Squid
Firewall	Iptables, Dante, Guarddog, FireWall-1

What training will be needed?

- Do you currently have UNIX skills in-house?

  – UNIX skills are largely directly transferable

- System Administration

  – No Registry, fewer/different GUI configuration tools - Major shift in mindset

- Certification

  – LPI, RHCT/RHCE, SUSE (based on LPI), GNU/SAIR

- Application Development
- Reference Library - O'Reilly books

Migration considerations

- ## Develop a standard system profile
  - Decide what software packages you want to have on *all* your Linux systems.
  - What additional packages will be needed for each type of server.
- ## Get your security and network teams involved early
- ## Figure out what level of support you need, and get it
- ## Figure out what system management tools you need
- ## Start small to build familiarity and confidence
  - Infrastructure type server such as DNS or DHCP
  - Departmental web server or file server

Active Directory

- Active Directory is essentially LDAP and Kerberos tied together (although slightly modified)
- OpenLDAP is the usual LDAP implementation
- Kerberos is usually Heimdal, but can be GNU Shishi
- If you decide to keep Active Directory, Samba version 3.0 or higher is needed to integrate well with it

Domain Controller

- Samba can act as a Primary Domain Controller for a Windows NT domain

- Samba 2.x does not support

  - Domain Trusts
  - SAM replication with Windows NT Domain Controllers
  - Adding users via the User Manager for Domains
  - Acting as a Windows 2000 (AD) Domain Controller

- Much of that has changed with Samba 3.x

Domain Name System (DNS) server

- Berkeley Internet Name Domain (BIND) is one of the many industry standard Open Source packages that make up much of the Internet infrastructure.

- Domain name serving is one of the easiest (and most transparent to the end user) conversions you'll face.

- BIND works from plain text configuration files, not a GUI.

- Start with a secondary, then move to the primary.

- O'Reilly and Associates publishes what is considered the definitive reference on BIND, "DNS and BIND, 4th Edition."

Dynamic Host Configuration Protocol (DHCP) server

- ISC's DHCP is another industry standard Open Source package
- I've seen a number of cases where it works better with Windows clients than a Windows DHCP server
  - Plus, it's "smarter" in some ways
- DHCP server keeps its configuration data in a .mdb file
  - Makes migrating the data difficult, but not impossible
- Clients can be migrated in a piecemeal fashion, or in a few large moves

Windows Internet Name Server (WINS)

- Samba can act as a WINS server, when needed
  - Takes one parameter in the smb.conf file
- Unless you keep the same IP address, requires a change on the user's desktop
- Samba does *not* provide for WINS replication
  - Don't mix Windows and Samba WINS servers on the same network
- Active Directory is eliminating the need for WINS

File and Print Server

- Basic file and print serving is also a fairly transparent conversion for the end user

  - Samba was originally designed with the intent of looking as much like a Microsoft-based file and print server as possible

- Automatic printer driver downloading for Windows NT/2K clients can be a problem to get working right

- Watch out for so-called "Win-printers"

- Samba performs better on the same hardware

- Samba can act as a BDC with a Windows PDC

File and Print Server (2)

- Advanced permissions will require ACL support in Linux

- Setting up all your printers will be a manual effort

- SWAT (Samba Web Administration Tool)

- Strongly recommend using CUPS (Common UNIX Printing System) for print/printer management

FTP Server

- Large number of FTP servers for Linux

    - Some distributions ship two or more

- wu-FTPd was very common, but very insecure

- ProFTPD, and vsftpd are now preferred by most distributions

- Anonymous-only servers don't require user accounts for everyone. **Remember that with FTP, all traffic is clear text**

- There are secure clients, but typically no one uses them

- Consider using scp in place of non-anonymous FTP

HTTP Server

- Apache is the most popular web server in the world

  – 60%+ of the servers in the world run it

- It even runs on Windows systems

- Much, much, more secure than IIS

- Active Server Pages (ASP) will be a problem to migrate

- Application developers will need to switch to

  – CGIs (Perl, etc.)

  – PHP (has had its share of security issues)

  – Java Server Pages (JSP)

  – Apache mod_asp module

Web Application Server (Java)

- Lots of products in this area. Probably the same ones that you run on Windows are available for Linux
    - WebSphere
    - BEA WebLogic
    - iPlanet
    - JBoss

- Installation, configuration and management should be the same or very similar across platforms

Remote Access Server

- Use the pppd package that comes with your distribution
- pppd supports a variety of authentication protocols, such as PAP, CHAP, and RADIUS

  - Of course MS had to have their own MS-CHAP

- Microsoft RAS authenticates dialup users in the same way it validates local logins

  - No way to extract the userid/password pairs for migration to the Linux RAS system.

- IP forwarding must be turned on in the Linux kernel

Email Server

- Again, lots of choices on Linux

  - Sendmail, exim, postfix, etc.

- A lot depends on what version of MS email server you're at

  - MS Mail

  - MS Exchange

  - MS Exchange 200x

- The email delivery piece is the easy part (see next slide)

- Most Linux distributions only package one

  - IMAP, POP3, and web mail packages are also available.

Groupware Server

- One of the big things that keeps companies tied to MS Exchange is shared calendars, etc.

- There are few alternatives to the Exchange/Outlook combination.

- Bynari's Insight server is one, but only scales up to about 50,000 email boxes.

- Ximian Insight Connector (now owned by Novell) is another

- This is probably the most sensitive migration to be made

Database Server

- About the only database not available for Linux is the one Microsoft sells.

- The two most popular Open Source ones are MySQL and PostgreSQL

- DB2/UDB, Oracle, Informix, etc.

- Migration effort will depend largely on how many MS-SQL-specific features your developers use

Proxy Server

- Linux comes with a native transparent proxy/gateway capability
- Socks proxy software is available, such as Dante
- Squid is probably the best, and best-known, Open Source proxy server
  - In addition to being an HTTP, FTP, SSL proxy server, it will also perform caching of "Internet objects," reducing access time as well as bandwidth requirements.
  - Can be run in transparent mode, or require userids and passwords

Firewall

- Linux comes with a native firewall capability
- Linux also has native support for Network Address Translation (NAT), also known as IP masquerading
- The iptables command is what is used to create firewall and NAT rules. There are GUI front-ends available to make that easier.
- Commercial firewalls are also available for Linux, such as Check Point's Firewall-1, Phoenix, StoneGate, etc.

The downside to migrating

- Initially increased training costs
- Initially lower productivity from your support staff
- Possibly finding new support provider(s)
- Having to learn new ways of getting software and support
- Some hardware suppliers don't provide Linux device drivers
- Open Source software is subject to Sturgeon's Law
  - But then, so is proprietary software.

Questions?