How to Fit Linux into your Enterprise

John H Terpstra, CEO, PrimaStasys Inc

jht@PrimaStasys.com
Today We Will Cover

- The Structure of a Linux Platform
  - Component Capabilities
  - Key Services and Interoperability
- The Business Decision Framework
  - Implementation and Integration Strategies
  - Measuring Costs and Exposure
  - Planning the IT Roadmap
- Conclusions
What is this about?

- This is NOT a Linux 101 course
- IT Executives want to know:
  - HOW WILL LINUX AFFECT MY BUSINESS?
Linux Platform Structure

• Compare with MS Windows 200x Solutions
  – That is THE Enterprise benchmark

• Need to identify key structural components
  – Be Familiar with:
    • What are they?
    • What is the utility of each?
      – How does it affect my enterprise?
    • What are the benefits and the risks?
Σ: Structural Overview

• Core Issues Affecting Enterprise Integration
  - Authentication Subsystems
    • PAM (Pluggable Authentication Modules)
    • NSSwitch (Name Service Switch)
  - Control of System Services
    • Inetd/Xinetd (Network Super Daemon)
    • System V Initialization Scripts
  - Printing Infrastructure
  - Firewall and VPN (Virtual Private Networking)
  - Software Update Maintenance
The Linux Standards Base

- Linux Standards Base defines the platform
  - Refer: http://www.linuxbase.org
  - Is a working unit of The Free Standards Group
    - Refer: http://www.freestandards.org
- First LSB Specification was released: June 2001
  - All major Linux distributions are LSB compliant
Authentication Subsystems

- PAM (Pluggable Authentication Modules)
  - Linux, like Unix has:
    - /etc/passwd database, /etc/shadow file, /etc/group file
  - NIS (Network Information Service)
  - LDAP (Light Weight Directory Service)
  - Kerberos (MIT or Heimdal)
    - Ticket based authentication service
MS Windows Interoperability

- Opportunity for Integration of Microsoft Windows into Unix environments
  - LDAP and Kerberos with proprietary extensions
    - Require custom software / client drivers
    - Active Directory is a super-set of LDAP and Kerberos
    - Can act as an LDAP / Kerberos Server
  - NIS support for Windows NT/200x
    - Requires client software drivers (GINA)
  - eDirectory (Novell product)
    - Requires client software drivers
PAM and Microsoft Integration

- Samba Winbind Integrates Microsoft Network Authentication into Linux/Unix environment
  - Other Samba server authentication server
  - NT4 Domain Controller as authentication server
  - Active Directory Authentication Server
- Caldera/SCO VAS
  - Uses Unix extensions to Active Directory
    - Integrates Linux into Active Directory Environment
    - See http://www.sco.com/products/authentication
Other PAM or External Options

● Novell e-Directory
  - On NetWare or on Linux
    • See http://www.novell.com/products/edirectory

● Sun One (iPlanet) Directory Server
  - LDAP Based Server
    • See http://www.sun.com/software/products/directory_srvr/home_directory.html

● IBM Authentication Server
  - LDAP Based Server
Linux User Accounts

• Contains very basic Information
  – User names limited to 32 characters
    • No upper case, no spaces
  – Group names limited to 16 characters
    • No upper case, no spaces

• Groups can NOT be nested
  – Has scalability and management implications

• Has account expiry capability
Example Linux Account Entries

/etc/passwd:
  jht:x:500:100:John H Terpstra:/home/jht:/bin/bash
  ajt:x:501:100:Amos Terpstra:/home/ajt:/bin/bash
  met:x:502:100:Melissa Terpstra:/home/met:/bin/bash
  lct:x:503:100:Lyndell C Terpstra:/home/lct:/bin/bash

/etc/shadow:
  jht:$1$pziz8yzz$6RXcJ/kO/gatqx7Xs4BiV.:12172:0:99999:7:::
  ajt:$1$6zezJyzQ$JVIp.4WF2SeH9zU.46Ij/0:12172:0:99999:7:::
  met:$1$CgWs5xyz$klM.j82dKbKgqw/ma1mMv.:12172:0:99999:7:::
  lct:$1$//wztlsz$e.jx4ftSTW.U04mKKOsWG1:12172:0:99999:7:::

/etc/group
  ntadmin:x:71:jht
  ntpowerusr:x:73:jht
MS Windows NT/200x Accounts

- Contains comprehensive data
  - User names can be up to 254 characters
    - CAN have mixed case
    - Spaces are allowed
  - Group names can be up to 254 characters
    - Local Groups
    - Global Groups
    - Universal Groups
- Groups CAN be nested
Microsoft Windows Accounts

• Features NOT in Linux OS Accounts
  - Password uniqueness controls
  - Workstations from which Access is Permitted
  - Can set future dated account activation
  - Desktop profile controls
  - Per user and/or per workstation access policies
  - Logon script control
  - Other subtle features
Key Basic Services

- Basic Services
  - DNS (Domain Name Service)
    - Internet Software Consortium
    - Bind 9 has support for Dynamic DNS
  - DHCP (Dynamic Host Configuration Service)
    - Internet Software Consortium
    - DHCP version 3

- Both are RFC (standards) compliant
Printing Infrastructure

• Original Choice
  – AT&T System V Spooler or Berkeley LPR/LPD

• Then came LPRng (LPR Next Generation)
  – Still in popular use. Default on some Linux platforms

• CUPS – Common Unix Print System
  – Comprehensive print filtering and rendering system based on IPP (Internet Print Protocols)
Security Services

• Firewall
  - Kernel based IPTables
  - Several configuration and management tools

• Virtual Private Networks (VPN)
  - Open Source package is a Linux Kernel add-on called FreeS/WAN
    • Current stable version 2.00 (released April 28, 2003)
  - Does IPsec
Linux Software Updates

• Automatic Update services available for
  - Red Hat Linux
  - UnitedLinux (SuSE, SCO, Conectiva, TurboLinux)

• Many network administrators prefer manual update
  - Safety concerns
  - Control issues
    • Dislike of feature creep
    • Principle of less surprises
Commercial Security Tools

• Main players include
  - CheckPoint: Firewall-1 and VPN-1
  - FWBuilder: http://fwbuilder.sourceforge.net
  - Phoenix Progressive Systems: Adaptive Firewall
    • Inside Sun's Cobalt Microcube solutions

• Commercial Support is offered by many organizations
Σ: Key Layered Services

- Layered Services
  - File and Print
  - Electronic Mail and Messaging
  - Web Proxy Services
  - SQL Server
  - Web Serving
  - Directory Services
File And Print

- MS Windows support provided by Samba
  - Current stable version 2.2.8a
    - NT4 style Domain Control support
    - No Internal Unicode support
    - Can not natively join an Active Directory Domain

- Apple MacIntosh support by NetAtalk
  - Current stable version 1.6.2

- NetWare support by MARS_NWE package
  - Current stable version 0.99pl20
File and Print: Samba-3 Futures

- Can natively join MS Active Directory
- Internal Unicode support
- Extended LDAP support
- New Security Account Manager database
  - Similar database as MS Windows NT4/ADS
- New Documentation for easier deployment
- Many new NT4+ Win2K+ features
- New tools to allow full control of MS Windows networking from Unix/Linux environment
- Better integration with NT4/Win200x admin tools
Electronic Mail & Messaging

• Every Linux system has a mail server

• Component lexicon
  - Message Transport Agent (MTA)
    • Does the sending and receiving
  - Message Delivery Agent (MDA)
    • Affects local delivery
  - Mail User Agent (MUA)
    • Used by the user to send/receive/manage mail
  - Message Retrieval Agent (MRA)
    • Can be used to access mailbox (mail store)
Popular Applications

• Application Types
  - MTA: Postfix, sendmail
  - MDA: Deliver, local
  - MUA: Most popular is MS Outlook Express
  - MRA: Pop2/3, IMAP

• Mail Boxes can be:
  - System mail box, or a file in the user's home directory, or a file system database
  - An SQL back-end
Microsoft Exchange Server

• Exchange components include:
  - MTA, MDA, MRA
  - MS Outlook Exchange Client

• A Directory
  - NT4 Domain or Active Directory database

• Data Store
  - File based with Backup/Restore facilities

• Interfaces
  - Virus Scanning, SPAM control, etc.
Linux Exchange Alternatives

• Roll your own from components
  - Postfix, imap, pop, cyrus extensions, etc.

• Commercially Supported Solutions
  - SuSE OpenExchange Server
  - SCO Office Server
  - XchangeNetwork
    • http://xcserver2.xcnetwork.com/index.jsp
  - Included in commercial solutions
    • Virus Scanning (several 3rd party)
    • SPAM Control
Web Proxy Services

- Main package is called SQUID
  - Installed based estimated at 1.5M systems
  - Has access control facilities
    - Time of day
    - Per User / Group
    - Can use NT4/ADS authentication backend
    - Can do content and URL filtering
  - High performance
SQL Server Options

• Major Open Source Projects: (Have ODBC drivers for Windows clients)
  – Postgresql: http://www.postgresql.org
  – MySQL: http://www.mysql.com

• Major Commercial
  – Oracle SQL
  – IBM DB2

• There are many commercial SQL server products
Web Servers

• The dominant web server today is Apache
  - Installed base is approx. 24M servers (62% of market)
    • See http://www.netcraft.com/
    • Approximately 50% of web servers run on Linux

• Apache modules are VERY important
  - SSL, PHP, Perl, Jakarta Tomcat + many more

• Apache and Modules can be run on many platforms including MS Windows
Directory Services

- OpenLDAP is the main open source package
  - Current stable version 2.1.17
- What is OpenLDAP?
  - Open source implementation of LDAP version 3
    - Light Weight Directory Access Protocol
- What is LDAP?
  - A lightweight protocol for accessing directory services, specifically X.500-based directory services
  - Details of LDAP are defined in RFC2251, and more
OpenLDAP: Data Organization

The Organization

Organizational Unit

Person

uid=babs

ou=People

ou=Servers

dc=example

dc=com

dc=DE

dc=net
LDAP Schema Files

• The following schema files ship with OpenLDAP
  - Core (needed by OpenLDAP)
  - Cosine (Internet X.500)
  - Interorgperson (POSIX User Account Info)
  - Others (misc, NIS, OpenLDAP Experimental)

• Are other schema files required?
  - Yes!
    • Samba schema
      - MS Windows user / machine account information
LDAP Features

- Integrity and Confidentiality Protection via TLS (SSL)
- Internationalization (Unicode)
- Referrals and Continuations, Schema Discovery, Extensibility
- Delegation and Replication
- Strong Authentication (SASL/GSSAPI)
  - Simple Application and Security Layer Services
  - Generic Security Services Application Programming Interface
    - A generic API for doing client-server authentication
∑: Linux Platform Summary

• Has many of the features / services of MS Windows NT4 / 200x environments

• Services are similar
  – NOT the same
  – Some have deficiencies
  – Some have greater functionality / utility
  – You have a CHOICE

• Linux and MS Windows can transparently share a common Network environment
Σ: Business Decision Framework

• Implementation and Integration Strategies
  – In-House orientation versus Out-Sourcing
  – Maintenance of Integrity
  – Managing Potential Exposure
  – Disruptiveness and Change Control
Σ: Decision Framework - I

- Measuring Cost of Ownership
  - Comparison of Linux and MS Windows Solutions
  - Hardware requirements and life-cycle
  - Staff Overheads
  - Software Upgrade and Maintenance costs
- Risks
  - Technology / software suppliers going out of business
  - Support Availability
  - Bugs and Defects
Σ: Decision Framework - II

- Application Concerns
  - Availability of the Right Package
  - Application and Data Interoperability
- Intellectual Property
  - What is the debate really about?
  - Schizophrenia and Reality
Σ: Decision Framework – III

- Planning the IT Roadmap
  - Preparing for Futures
  - Avoidance of Isolation
- Common Objections and Answers
  - From the User's perspective
  - The Administrator's Dilemma
Σ: Summary

- Linux is a rapidly maturing platform
  - Many features are ready for enterprise adoption / deployment
  - Some questions still not answered
- Microsoft Windows is here to stay
  - Interoperability is paramount factor in Linux deployment
- Alternatives can be financially attractive
DEMO:

A brief look at some key interoperability capabilities