Integrating UNIX and Linux with Active Directory

John H Terpstra

CTO, PrimaStasys Inc.

jht@primastasys.com

Agenda

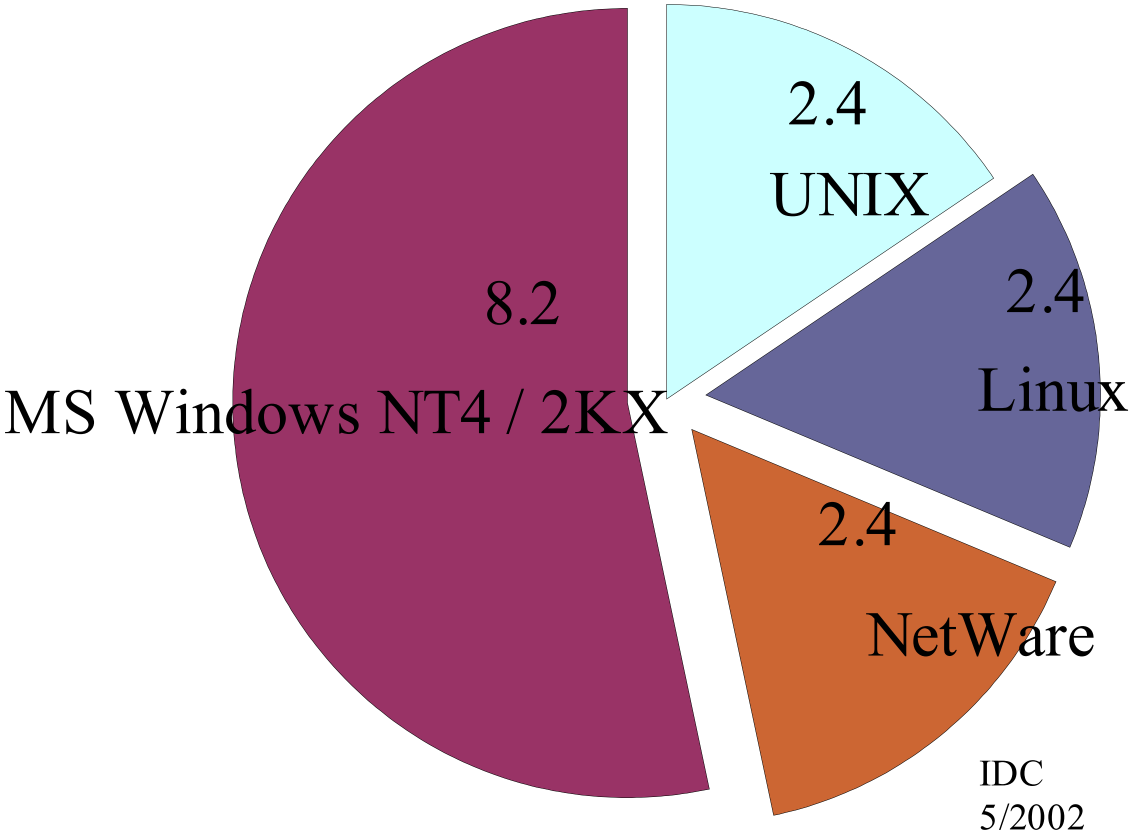
- Definition of the Integration Problem
- Technical Background
- Review of Solution Choices
  - Kerberos
  - LDAP
  - Samba Winbind
  - Vintela Authentication Services
- Making the choice for CIFS ID Management
- Demonstration

Market Information

- MS Windows NT4 Migrating to MS Windows Server 200x
  - With Active Directory
  - NAS / UNIX / Linux CIFS usage is growing
- Therefore:
  - Integration need growing

Server Market Share - 2001

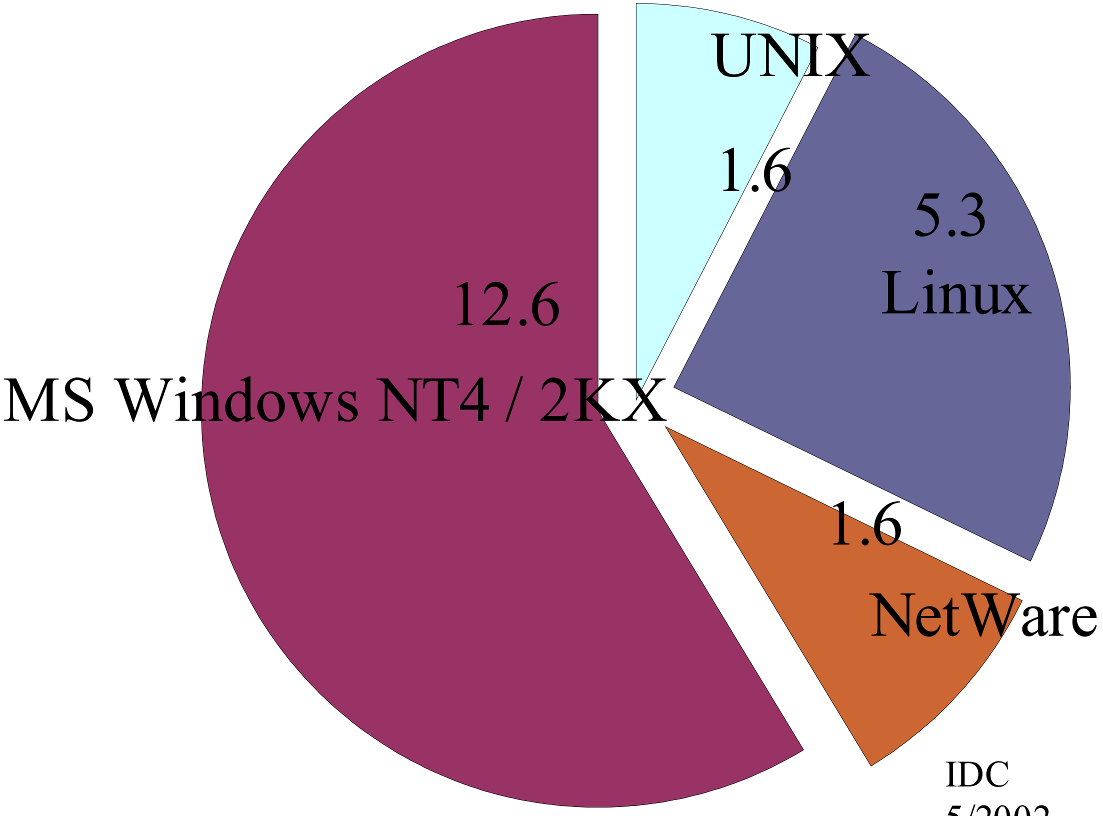
15.4 Million of Servers



IDC
5/2002

Market Share – Forecast 2005

21.1 Millions of Servers



IDC
5/2002

Problem Definition

- CIFS File System operations require
  - Authentication
    - Front-end to access controls
    - Datastore location is a network design decision
      - Can be local to each device or centralized
    - Must know limitation of protocols and methods
  - Identity Resolution
    - Needed to provide unique attributes per user
    - Used to control access to CIFS resources
    - Needs to bridge disparate identity attributes

User Identity Differences

- UNIX / Linux User Identifiers
  - Older – 32 bit Unsigned Int
  - Newer – 64 bit Unsigned Int
    - uid=543(jht) gid=876(users) groups=876(users),71(ntadmin),238(engrs)
- MS Windows has complex security identifiers
  - Incompatible with UNIX / Linux eg:
    - S-1-5-21-1593769616-160655940-3590153233-2013

Bridging the ID Gap

- MS Windows Security Identifiers
  - Design Issues
    - Map to UNIX compatible UID/GID
      - On central store
      - On client / domain member server
    - Store extended information in AD Schema

Cross Machine Integrity

- How to ensure integrity:
  - Provide Consistent UID/GID for all users
  - Essential for cross protocol file sharing
    - CIFS / NFS
- Centralization v's Synchronization
  - Sync solution requires more supervision
  - How secure is sync method?

Technical Background

- Microsoft Active Directory
  - Kerberos / LDAP support
  - In Windows only environment also uses proprietary protocols
- AD is the Authentication and Identity management backend of choice
  - Provides centralized network user identity administration
  - Integrates with external directories through tools like MIIS (was MMS – Microsoft Metadirectory Service)

What works with AD?

- Interoperability Choices
  - Kerberos – complex to install, addresses Athentication
  - LDAP – Identity Management, does not address Authentication
  - Samba Windbind
    - Authentication and Identity Management
    - Has own ID Map solution
  - Vintela Authentication Services
    - Authentication and Identity Management
    - RFC2307 schema extension for UID/GIDs

Pure MIT / Heimdal Kerberos

- Key Limitations
  - Must generate a per client keytab file
    - Need to migrate keytab to each client
  - Time must be kept in sync between AD servers and all Kerberos clients
    - Uses extra external process (NTP)
  - Inconvenient Authentication Only solution
    - Requires client machine pseudo-user account in AD
    - Must sync /etc/passwd with AD User Accounts to provide UID/GIDs etc.
    - No disconnected mode operation

PADL LDAP Tools

- Available from PADL Software
  - Two modules:
    - pam_ldap, nss_ldap
  - Benefits:
    - Runs on most UNIX platforms today, Free
    - Supports RFC2307 + MS Service for Unix
- Disadvantages
  - Poor Scalability
  - Lacks secure authentication to AD
  - No disconnected mode operation

Samba Winbind

- Has three parts:
  - PAM: pam_winbind.so, handles authentication
  - NSS: libnss_winbind.so, handles identity management
  - Daemon: winbindd, handles communication with remote NT4 DC's and with Active Directory DCs
  - Caches user ID info in winbindd_cache.tdb
- New to Samba-3.0.0 winbind also does all Samba ID Map handling
  - Stores mapping info in winbindd_idmap.tdb
  - Maps Windows SIDs to Unix UIDs/GIDs

Samba Winbind

- Pros:
  - NO disconnected mode operation
  - Authentication and Identity Management
    - UNIX Accounts AND for Samba
  - Scalable through caching of data
- Cons:
  - Same UID/GID across all Samba servers ONLY with LDAP Account backend
    - Complex configuration
  - Exposes ALL backend accounts
    - NT4 Domain / Active Directory Domain

Vintela Authentication Services

- Commercial Solution
  - AD RFC2307 AD Schema Extension
  - Microsoft Management Console Snap-In
    - UNIX Account enablement / disablement
    - Stores UID/GIDs and other UNIX account attributes
  - Uses secure Kerberos authentication
    - LDAP over Kerberos
  - AD member client cache
    - Stores only UNIX enabled account info
    - Does periodic intelligent sync to keep current

Vintela Evaluation

- Pros:
  - Has disconnected mode operation
  - Easy configuration
  - Consistent UID/GIDs
  - No local accounts needed
  - Scalable
  - UNIX / Linux machines get AD Machine Account
- Cons:
  - Commercial (Payware)

Making the Choice for CIFS

Viable choices are:

Method	Authentication	ID Management
Samba Winbind	OK	OK
Vintela Authentication Services	OK	OK
Both	OK	OK

Demonstration & Questions