Windows 2000 Planning

at the University of Michigan

by

MaryBeth Stuenkel
Dave Detlefs
Andrew Wilson

(U-M Information Technology Division)

5/16/2000

Presented at the May 2000 Common Solutions Group meeting

http://www.stonesoup.org/Meetings/0005/mtg.pres/detlefs.htm
W2k Goals

• Leverage Windows 2000 technology for benefit of students, faculty and staff

• Integrate Windows 2000 with existing computing infrastructure (UMCE)
  • DNS, Kerberos, Directory Services, Account Administration, etc.

• Enable campus-wide sharing of W2k-based resources and services
Existing Infrastructure

• MIT Kerberos
  • K5, K4 and AFS support (umich.edu realm)
  • Three other realms, presently K4 prod and/or K5 test
  • Clients: MIT K4K5, Kerb95 (K4)

• Primary Directories
  • OpenLDAP 1.2.10 (LDAP V2, 100k users, mail groups)
  • Netware 4.11/5.0, NDS 6/7
    • 100k objects, 40k users, 350 servers

• DNS
  • Mostly Bind 8.2+, some delegated Name Servers
  • U-M Standards and Practices Guide on DNS names
Existing Infrastructure
(continued)

• Data Sources
  • M-Pathways Project (Peoplesoft)
  • Accounts Office
  • Human Resources
• U-M Uniqname
  • Each U-M person assigned (8 char max) uniqname id
  • Process coordination with U-M Accounts Office, U-M Directory, Kerberos KDC, M-Pathways, etc.
• Windows (NT 4, Win95/98)
  • Numerous, independent NT 4 domains
  • No centrally managed NT 4 infrastructure
  • U-M Computing Sites...highly customized NT 4 workstations
Potential W2k Benefits

• Integration
  • Common identification, via U-M uniqname and Active Directory
  • Common authentication, via Kerberos and PKI

• Resource Sharing
  • W2k applications, files, web services
  • Across U-M campus, facilitated by Active Directory
  • Off campus, facilitated by PKI and AD identity mapping
  • Terminal Server-based applications

• Administration
  • Forest-wide administration and policy via Active Directory
  • Delegation of authority as needed
  • Terminal Server-based administration built in
Potential W2k Benefits
(continued)

- **Security**
  - MS Kerberos primary security protocol
  - Delegation of authority via impersonation
  - Uniform policy enforcement across Site, Domain, OU
  - PKI integrated with operating system
  - Smart card, Encrypting File System support
  - Delegation of authority via impersonation
  - 128-bit security mode
  - Terminal Server over-the-wire encryption

- **Networking**
  - IPv6 support
  - Virtual Private Network support
  - Terminal Server works over dial-up
Potential W2k Benefits

(continued)

- Scalability
- QOS (Quality of Service)
- Load Balancing
- Clustering
W2k Forest Design

- **W2k Forest**
  - Common AD schema
  - Trust relationships between domains
  - Easy resource sharing, manageable infrastructure

- **W2k Tree**
  - Contiguously named domains (bar.org, foo.bar.org)
  - Boundary for W2k LDAP query referrals

- **W2k Domain**
  - Security, identity, administrative boundary
  - Separate Kerberos realm

- **W2k Site**
  - Collection of subnets, used for AD replication, W2k Administration

8
W2k Forest Design
(continued)

- **Forest Models**
  - Single Domain
  - Single Tree of Domains
  - Multiple Trees
  - Multiple Forests
  - National Parks

- **Single Domain**
  - Single, unique set of user identities guaranteed
  - Delegation of administration via Active Directory OUs
  - Requires buy-in from entire campus
W2k Forest Design (continued)

- **Single Tree of Domains**
  - Eases DNS integration problems, compared to multiple trees
  - Tree is boundary of W2k LDAP query referral
  - Multiple security, identity, administrative spaces
  - Requires acceptable root domain name
  - More autonomy for individual domains
  - Enterprise tasks correspondingly more difficult
W2k Forest Design

(continued)

• Multiple Trees
  • Existing DNS roots preserved (foo.org, bar.org)
  • Most trees will contain only one domain
  • Danger of domain proliferation (like NT4)
  • W2k LDAP query referrals don't cross trees
  • Potential to increase size of AD Global Catalog
  • Multiple security, identity, administrative spaces
  • More autonomy for individual domains
  • Enterprise tasks correspondingly more difficult
• Multiple Forests
  • Common schema not guaranteed
  • Explicit trusts relationships required between forests
  • Complete autonomy possible
  • Resource sharing more difficult
  • Most difficult to administer as enterprise
  • Not an option that we are considering
  • Single forest is our minimum goal
U-M Forest Design

- Domain Structure (tentative)
  - Multiple Tree variation
  - Forest Root domain a placeholder, for security, stability
  - Joinable Root domain (tree) advocated for campus units wishing to create separate domains
  - Joinable Root domain to also host users and OUs for campus units that don't want to run own domain
  - Separate trees for campus units wishing to preserve DNS name
  - Design influenced by advocacy of large campus units
  - Hope is that smaller campus units will not create own domains
  - Potential proliferation of domains
U-M Forest Design
(continued)

- Active Directory Structure (tentative)
  - Flat user namespace with schema extensions (ou=)
  - Namespace mapped from U-M Directory
  - Attributes more flexible than assignment to OU
  - All users in single OU, part of "joinable root" domain
  - All other domains are, ideally, resource domains
  - Users in other domains not centrally administered
  - Increased reliance on W2k Security Groups for administration
  - Group Policy based upon inclusion of groups within OUs
U-M W2k Security

- **Basic Goals**
  - Single signon for W2k clients (K4, K5, NetWare, AFS, etc.)
  - High level of security
  - Integration with existing infrastructure
  - Support both existing and new applications

- **Strategy**
  - Authenticate to UMICH.EDU (MIT) realm
  - W2k tickets via 1-way Kerberos trust to MIT realm
  - 1-1 mapping of U-M uniqnames to W2k
  - Enforce high security with W2k Group Policy
  - W2k Domain Controllers run in high-security native mode
  - Forest Root domain is placeholder, for stability, security
U-M W2k Security
(continued)

• Under Consideration
  • Support for down-level Windows clients (probably not)
    • Affects security, Kerberos interoperability
  • Synchronization of MIT/W2k passwords (probably not)
    • Needed for down-level clients
U-M W2k Status

• Testing, Phase 1
  • 9/99-4/00
  • ITD and large campus units
  • Get our feet wet
  • Begin interoperability projects
  • Use experience to plan for phase 2

• Testing, Phase 2
  • 4/00-6/00
  • Rebuild forest
  • Test forest model resembling production, Phase 1
• **Production, Phase 1**
  - 7/00
  - Forest root support for LSA, Engin domains
  - Kerberos interoperability support may not be ready
    - MIT Kerberos update required
    - Won't work with down-level Windows clients
  - Joinable Root may not be populated with users
    - OpenLDAP software to populate AD
  - Planned transition to production, Phase 2
    - NT 4 domains migrate workstations to W2k
    - Need all W2k for Kerberos interoperability, security
U-M W2k Status (cont.)

- Production, Phase 2
  - 7/01 or earlier
  - Kerberos interoperability support
  - Joinable Root populated with users from U-M Directory
  - Available to all of U-M campus
Concluding Remarks

- U-M hopes to collaborate with CSG institutions on common Windows 2000 issues.
  - W2k strategies, experience
  - Single signon (network providers, GINA?)
  - W2k clients/services
  - Certificate/PKI issues
  - Interoperability issues
  - Anything else?
- http://www.umich.edu/~lannos/win2000/