AIS/W2K Pilot Project

Presentation by
Marc DeBonis
Doug Edmonds
Michael Johnson
Overview

- Motivation
- Active Directory
- Security
- Anytime Anywhere Data
- Remote Management
- Project-wide lessons learned
- Where we’re going
- Futures
- References
Motivation

- To leverage the features and functionality of Windows 2000 as an enterprise computing environment.
- Offer the University community the option of managed
  - Security
  - Anytime Anywhere Data
  - Desktop Management
Motivation

- Microsoft Windows 2000 AD shift for MS
- Reduce total cost of ownership (TCO)
- Anticipate seat management requirements
- Enable proactive rather than retroactive support
- Build a data storage mechanism that is available regardless of location
- Build a mechanism to distribute driver and system updates with minimal human interaction
User accounts reside in root, resources in children
Active Directory

VT.EDU

HOKIES

W2K

Child domain

CC

juser

W2K AD namespace

 NOTVT

V T

CC

Domain admins
Computers
Users
juser

W2K AD OU structure
Active Directory

Benefits of Active Directory in a Windows 2000 Environment
- Delegation of Administration
- Active Directory Sites
- Kerberos Authentication
- Group Policy
- Advanced management toolset (MMC)
- Quality of Service (QoS)
- Enhanced Telephony API (TAPI)
- Enhanced IP security (IPsec)
- Enhanced File and Print services
Base components

- **Security**
  - Serious need for basic security at the desktop.

- **Anytime Anywhere Data**
  - Decouple user data from system and application data.

- **Remote management**
  - Large TCO for current desktop implementations; difficult to distribute patches, upgrades, and track hw/sw inventory.
Security

- Managed workstation firewall
  - BlackIce agent from NetworkIce
  - Uses IceCap console with SQL database
- Managed security policy
  - Based on AD membership
  - Can be selectively assigned based on OUs
- Managed automated OS hotfixes
  - In-house developed application “Daisy”
  - User has control when it runs and what it does
Security

- Managed anti-virus scanning
  - Norton Antivirus 7.5 Corporate Edition
  - Uses Norton SCC management suite
  - Can push antivirus updates on scheduled or realtime cycle
- Managed event logging
  - In-house developed application “Event mirror”
- User rights for daily activity, “runas” for administration
Security (lessons learned)

- Users want varying levels of control over security settings
- Some applications require very high security rights to install and function
- Workstation firewall susceptible to slow scans, user error and application error
- Default user rights limit functionality as compared to typically running as administrator
Anytime Anywhere Data

Roaming Profiles
- User’s desktop environment follows them around the network

Folder Redirection/Offline Stores
- Data availability on or off network

Centralized storage
- User data located on network attached storage (NAS)
- User data secured via NTFS permission
- NAS backed up via Tivoli backup (TSM)
- NAS is in a physically secure location
Anytime Anywhere Data

**Disaster recovery**
- **Lazarus**
  - In-house developed application
  - Universal Disk Image (UDI)
  - Restores computer to generic install
- **Snapshot**
  - In-house developed application
  - Pre-emptive disaster recovery
  - Use to capture an image of a computer prior to a configuration change (i.e. software or driver install)
Anytime Anywhere
Data(lessons learned)

- New paradigm of backup strategy
  - Implementing lazarus and folder redirection, coupled with user education, client backups are unnecessary
- UDI still not really “universal”
- Group policies can be used to implement domain-wide configuration changes instead of making changes manually on each computer
- Use of roaming profiles and folder redirection increases network load, slower access
Remote management

**Core features of SMS**
- **HW and SW inventory**
  - >600 hw Properties defined, can define prop. for new hw
  - Audit client machines for file types
  - Occurs at admin-defined intervals
- **Software distribution**
  - Single files, entire applications, or instructions
  - Clients made aware of packages via advertisements
  - Optional and mandatory advertisements
Remote management

Remote desktop control

- Radmin by Famatech
  - Integrated with NT security
  - User has control over service
  - Company license purchased by VA Tech

SMS

- Possible to create console for helpdesk view of user’s hw/sw Inventory information
- Can use this inventory to help in disaster recovery
- Inclusion in SMS is optional, user initiated
Remote management (lessons learned)

- SMS not appropriate as disaster recovery mechanism
  - SMS is schedule driven not event driven
- Radmin and runas
- SMS site defined by IP subnet
- Most apps must be re-packaged for sw distribution
- SMS server roles can be distributed across multiple servers
Project-wide lessons learned

Always a balancing act between security and usability

Anytime Anywhere Data requires a shift in thinking about data (user, application and system)

Remote management requires considerable planning and resources but very valuable

Thorough testing requires a feedback cycle with continuous communication

Microsoft Consulting Service critique of the VT AD implementation provided valuable feedback, changes to architecture pending
Where we’re going

Central Services

- Designed for departments without the knowledge, time or money to bring up their own W2K child domain
- Generic child domain for member workstations or servers to join
- Will give members benefits of participation in AD
Where we’re going

- AIS domain migrating to W2K
  - Week of Thanksgiving
- Signoff on base components
- Pilot participants get new desktops
Futures

- Next steps in the lab
  - Telephony, QoS
  - Thin-client computing
  - Virtual private networking (VPN), wireless
  - Public key infrastructure (PKI), biometrics
References

- **Windows 2000 Vision Statement**
  - [http://www.w2k.vt.edu/vision.txt](http://www.w2k.vt.edu/vision.txt)

- **Windows 2000 at VT**
  - [http://www.w2k.vt.edu](http://www.w2k.vt.edu)

- **Microsoft Windows 2000**

- **Microsoft SMS**
  - [http://www.microsoft.com/SMS](http://www.microsoft.com/SMS)

- **Radmin**
  - [http://www.radmin.com](http://www.radmin.com)
AIS/W2K Project

Presentation by
Marc DeBonis
Michael Johnson
Doug Edmonds
Pop quiz!

What is one of the managed components?
(a) Hardware distribution
(b) Remote Management
(c) Software Management System
(d) All of the above
(e) None of the above
(f) a, b, and e