MIG

- **Microsoft Implementation Group**
  - Primary responsibilities include
    - Maintaining the VT Active Directory (Hokies)
    - Developing AD-enabled and AD-enhanced apps
  - Our focus
    - Provide a stable, scalable, and secure Microsoft-based computing environment
  - We work to accomplish this by following three functions: **adopt, adapt, and improve**
MIG - Adopt

- New MS applications, systems, and services in a controlled and timely manner
- Future MS technologies to showcase and highlight benefits, pros, and cons
- Testing and feedback methodologies for existing MS products
MIG - Adapt

- Existing MS technology, customize for a university setting
- Computing infrastructure based on MS technology, provide to university customers
- MS and open source technology for best-of-breed results
MIG - Improve

- Existing and "last-mile" service and support to avoid "dropped" issues
- In-house hardware and software to gain greatest benefit from MS relations
- Between VT and MS marketing, support and developers
Other Avenues of Support

- VT Windows User’s Group meeting
  - First Thursday of every month
  - 20-30 departmental admins attend
  - [http://vtwug.w2k.vt.edu](http://vtwug.w2k.vt.edu)

- MIG has a yearly contract with a MS TAM (Technical Account Manager) through Microsoft Services

- Periodic ThinkTank and OU admin meetings
MIG - Staff

- Marc DeBonis
  - Lead System Administrator
  - MIG Manager
- Zeb Bowden
  - Secondary Systems Administrator
  - Lead programmer
- Steve Warrick
  - Data Curator
  - Secondary programmer

http://vtmig.w2k.vt.edu
AD History

- Migrated from an NT 4.0 “Master accounts domain” to Windows 2000 on July 10, 2000
- Required to provide seamless migration, required populated root, cracking passwords, etc.
- Tested ADMT - found it inadequate
- Very little MS documentation at the time
- Did presentation at SANS Monterey, 2000 entitled “Migrating from NT 4.0 to Windows 2000 in the real world: The good, the bad, and the dirty little secrets”
- http://www.w2k.vt.edu
AD present

- Populated root called w2k.vt.edu (Hokies)
- Two top level OUs; VT and NOTVT
  - Most objects placed under VT in a defined OU or in the ‘notou’ OU
  - OUs in the NOTVT branch are for hosted third party facilities management customers
- OUs are defined by a strict 1:1 ratio with the DNS zone list maintained by CNS (Communications Network Services)
  - cs.vt.edu = computer science = CS OU in the VT branch
OU Structure

- Predefined groups are created within OUs if there is local admin
  - “X admins”, where X is the OU name
    - CS admins
  - Group is populated with local administrator’s account (also resides in OU)
  - Permissions are then delegated to OU admins
    - Full control groups, reset password, read all properties, manage profiles, manage workstations, create GPO link
Current AD Object Stats

- 164 OUs
  - Compare to 248 subdomains in CNS’s DNS
- 46 OUs have OU admins
- 4722 full users
- 7306 contacts
- 7376 objects in notou (768 users, 6608 contacts)
- 778 resource/ sponsored accounts
Object Creation

- Changes to the Enterprise Administrative System (SCT Banner) triggers DB record replication to the Enterprise Directory registry (OpenLDAP system).
- ED-registry builds a filtered LDIF extract of specific demographic info for all VT-STAFF/VT-FACULTY.
- An AD process polls LDIF record every 15 minutes:
  - Updates any existing record
  - Creates new records as contact objects in NOTOU.
- All faculty and staff have at least a contact in the AD.
Full user accounts have a description \#user\#uid
- uid is a unique, never reused number synched with ED system
- AD name = ED pid
  - in ED user is juser, which is also the samAccountname of the account in AD

Contact objects have same uid so we can detect ED account renaming

Resource accounts do not have uids
- Don’t have a 1:1 ratio to a account in ED
- uid for the resource is the responsible person’s uid
- Description is \#resc\#uid
- Examples: projectors, boardrooms, items that require scheduling via Exchange
DNS Division

- Virginia Tech’s DNS zone is vt.edu
  - Tried Bind 8 and CNS’s DNS during testing of W2K
  - Problems encountered:
    - No dynamic or secure updates (the way MS does it)
    - Underscores in names unacceptable
    - 8 was in beta
  - CNS seceded us the namespace w2k.vt.edu
    - All AD-related systems now have dual citizenship
      - Machine.dept_zone.vt.edu and machine.dept_zone.w2k.vt.edu
      - Requests for *.w2k.vt.edu are forwarded to our DNS servers
      - Lookups outside of *.w2k.vt.edu for AD clients are forwarded to CNS’s DNS servers
  - We do strict RFC, AD integrated, secure DNS without reverse lookups
Child Domains

- Currently have 16 child domains
  - Previously had up to 20 one-way NT 4 trusts
- Child domain names must match their department’s DNS sub zone according to CNS
  - Allows pairing of the CD and corresponding OU in the root
- Child domains must adhere to the ROE: Rules of Engagement
Child domain (CD) must have at least two full-time/online peer (backup) domain controllers (DCs).

DCs must meet Microsoft's minimum computer hardware requirements.

No third party or MS add-on software allowed on DCs.

DCs must be in a backup program and have full recoverability tested.

DCs must allow and not attempt to block GPOs replicated from the root AD.

All W2k systems within the child domain must follow the proscribed DNS naming scheme.

- Machine name matches CNS DNS hostname
- Domain name matches CNS DNS zone name
- Example: a system currently registered as foo.bar.vt.edu
  - Machine name: "foo" in a W2K child domain called "bar"
  - Full DNS entry: foo.bar.w2k.vt.edu
All W2k systems within the CD use root AD DDNS server settings
- CD controllers will use static IP entries
- No DHCP servers
- Delegation of CD DNS zones may be allowed on a case by case basis.
- CD will not attempt to create further child domains "below" theirs
  - Use organizational units instead
  - Exception for valid CNS DNS domain underneath the current W2K CD
- No non-administrative local logins allowed to the CD controllers
- CD controllers housed in a secure area with controlled access
- Keep two week backups of event/audit logs
  - Access to backups given to the AD enterprise administrators for security/debugging purposes
  - All service packs installed in a timely manner, coordinated with root AD controller upgrades.
- Failure to comply results in a remediation/re-evaluation period followed by CD disconnection if compliance problems are not resolved in a timely manner.
Special Child Domains

- **Central Services domain**
  - Built for domain consolidation
  - Allows delegation to departmental admins at OU level
  - Admins can add users and workstations, manage GPOs

- **University Services domain**
  - Built for facilities management
  - Allows us to push GPOs, do security scans, and other services based on location of the workstation’s computer object
DC Distribution

- Two DCs in one IP subnet
  - Both are GCs
  - One holds all the FSMOs except infrastructure master
  - Both also act as DNS servers
- One DC in a different subnet (physically located in the same room)
- Working on bringing up a geographically removed DC
  - Due to past incidents
  - Thought about putting it in a separate site to control replication, but found it unnecessary
  - Will make it a GC and a tertiary DNS server
Pilot Systems

- Three Dell 2650s running w2k-pilot.vt.edu
  - Allows testing of E2K 3, Unix/ Samba systems, Mac OS X system integration, etc.
- Three Dell 2650s running behind a VPN in a non-routable IP subnet
  - Used to test schema updates and other non-recoverable testing
Challenges, Part 1

- Users do not:
  - Understand the differences between a standalone workstation and one that is a member of a domain
  - Understand the benefits of directory services
  - Use W2K/XP built-in tools to manage group, account, and workstation membership

- Fairly high TCO for end users
  - User -> call center -> help desk -> IRM (information resource management) -> MIG group
Challenges, Part 2

- Designed a project to rapidly prototype and develop a series of web-based applications to abstract Active Directory and the services it provides.

- Hokies Self-Service
  - My Information
  - My Security
  - My Services
  - My Exchange
  - My Storage
HSS Demo

- Demo Hokies Self-Service
  - [http://selfservice.w2k.vt.edu](http://selfservice.w2k.vt.edu)
  - Using PHP, CDO, and Winbatch
  - Web server is Xitami from Imatix
Problems along the way

- Reverse engineering how the Exchange Admin tool processes a user into a mailbox enabled user was difficult.
  - PSS said it wasn’t supported
  - Had to install E2K add-on on web server
  - Easy to crash the RUS
- PSS said it wasn’t supported
- Had to install E2K add-on on web server
- Easy to crash the RUS
- Lack of documentation on:
  - Mapping LDIF attributes to AD attribute names
  - How (if) they are exposed through standard interfaces
- Created a “fervor” when we required new versions of IE/Netscape for website
- Temporarily messed up attachment for E2K users without InternetEncoding attribute set
- Difficulty working with partial SMB implementation of NetApp NAS when pre-creating share space. Issue with security when profile is created.
- Complicated process to add/remove a workstation from a domain (for users at least)
HSS Timeframe

- Started 9/2/02
  - My Information Released - 10/17/02
  - My Security Released - 11/1/02
  - My Services Released - 12/11/02
  - My Exchange Released - 2/11/03
  - My Storage Released - 3/12/03
- Finished 3/12/03
- ~6 months with two developers
- [http://opensource.w2k.vt.edu](http://opensource.w2k.vt.edu)
HSS Statistics

- 3,087 of workstations in AD
- 12,000+ logins to HSS
- 932 users have used HSS to convert into a full user
- 283 people used HSS to create NAS space
- 879 users have used HSS to get an Exchange mailbox (either full or calendar only)
- 48 workstations in NFM
- 20 workstations in SFM
OU Admin

- Created so that OU admins could move people into/out of the ‘notou’ OU.
  - There is no simple way to delegate the ability to move a user
  - If a user is in an OU without an OU admin group, they can move themselves
  - If ou does have an ou admin, it becomes restricted and user cannot move themselves out of it
  - OU admins arrange movement of user account when user changes office

- Previously managed DNS cnames for child domains
  - Since we don’t allow child domains to run DDNS
  - Avoided awkwardness of trying to delgate DNS permissions
OU Admin Demo

- Demo OU admin
  - [http://ouadmin.w2k.vt.edu](http://ouadmin.w2k.vt.edu)
  - Using PHP, dnsadmin RSK tool, and Winbatch
  - Web server is Xitami from Imatix
OU Admin Stats

- Started 3/17/03
- Finished 4/28/03
- ~2 months with one developer
- 500+ logins to OUadmin
On the Horizon

- Web-based application for administration by IRM staff
  - Remove delegated rights through MMC
  - Build custom pages to avoid data entry or mis-linked uid/ resources
- Improvements/additions to “My” functions groups within HSS
- Add features to OU admin to allow finer control over password management of users in sub-administrated OUs
Active Directory at Virginia Tech

Best Practices - Self-Service

Marc DeBonis
Senior Systems Architect
MIG - Virginia Tech
Nov 12th, 2003