W2K migration and consolidation - issues and answers

Marc DeBonis
Virginia Tech – IS&C
Marc.DeBonis@vt.edu
Domain structure – NT 4.0

NT system types

- **Standalone (workstation or server, all 9x)**
  - Do not participate in a domain
  - Local users and groups only (NT only)
- **Member (workstation or server)**
  - Participate in a domain
  - Local and domain users and groups
- **Domain Controller (server only)**
  - Run domain, maintain domain user accounts, trust relationships
  - Domain users and groups only
**NT 4.0**

- Standalone
- **Srv**
- Domain A
  - Wrk
- **Srv**
- Domain B
  - Wrk

- **Netbios** or **DNS**
- **WINS needed**
- **All trusts one way**
- **No trust transitive**
Domain structure – W2K

W2K system types

- **Standalone (workstation or server)**
  - Do not participate in Active Directory (AD)
  - Local users and groups only

- **Member (workstation or server)**
  - Participate in AD
  - Local and domain users and groups

- **Domain Controller (server only)**
  - Runs domain, maintains domain user accounts, maintains trust relationships, root or child of AD
  - Domain users and groups, universal groups
  - Organizational Units (OUs) help organize

© 2001 Marc DeBonis, v1.0
W2K

- Netbios = dns
- DDNS needed
- All trusts two way
- All trusts transitive
AD overview

Active Directory

- Combines the NT domain model into a hierarchical forest, based on an LDAP (X500) directory using domain name service (DNS) as a service location and naming mechanism
- Provides organizational units (OUs) to manage users, groups, computers, shared folders, etc.
- Provides local, global and universal groups for security and distribution control
- New security model allows fine-grain control of security attributes and role delegation
W2K pros

- Provides a wide range of new benefits, features and functionality
  - Value – Lower TCO
  - Reliability – uptime (17% > NT 4, 50% > 9x)
  - Mobility – Laptop support, hibernation, APM
  - Manageability – Group policies, MMC, delegation
  - Performance – speed (27% > 9x)
  - Security – VPN, IPsec, LT2P, biometrics
  - Internet – IE 5, WebDav, Active Desktop
  - Data Access – Intellimirror, DFS, offline store
  - Hardware – PnP, USB, Firewire

© 2001 Marc DeBonis, v1.0
W2K cons

- Requires significant time, money, and personal investment
  - Training issues for admins and end users
  - Operating system, client access license, and add on services costs
  - Significant change in code base, many new features, greater chance of errors
  - Slow adoption, smaller knowledge base
  - Requires infrastructure changes, DNS
HOKIES/VT AD root

User accounts reside in root, resources in children
HOKIES/VT AD root
Domain migration

When NT domain = DNS zone

- Read the rules of engagement (ROE)
- Move domain user accounts to Hokies
- Define member servers and workstations to follow the DNS naming convention
  - netbios name = DNS hostname
  - domain name = DNS zone
- Secure resources based on Hokies accounts
- Upgrade current domain controllers to w2k
- Bring domain in as a child domain of the VT AD root (Hokies)

© 2001 Marc DeBonis, v1.0
Migration example

Hokies (w2k.vt.edu)

AIS (ais.vt.edu)

Users & Resources

Hokies (w2k.vt.edu)

Users in AIS OU

AIS (ais.vt.edu)

Resources

&

AIS (ais.w2k.vt.edu)

© 2001 Marc DeBonis, v1.0
Domain consolidation

When NT domain ? DNS zone (or multiple NT domains exist in same DNS zone)

* Bring domain administrators into new w2k child domain called DNS zone (political)
* Define member servers and workstations to follow the DNS naming convention
  * netbios name = DNS hostname
  * domain name = DNS zone
* Create OUs in new W2K child domain, each OU contains groups, computers, shares, printers, etc. corresponding to old NT domains
* NT domain administrators given admin control over corresponding OU (role delegation)
Consolidation example

Users and resources exist in each NT domain here

VTUSD, 4HELP, CC-OP

Users in CC OU

Hokies (w2k.vt.edu)

CC

(w2k.vt.edu)

CC-OP

3 OUs exist here
VTUSD, 4HELP & CC-OP

© 2001 Marc DeBonis, v1.0
Migration vs. Consolidation

When to do which?

- Migrate when a NT domain already matches 1:1 for a DNS zone
- Consolidate when there is a many:1 ratio for NT domains to DNS zones

Administration issues

- A ladder of trust is required for consolidation
  - Root level = Enterprise Administrators
  - Domain level = Domain Administrator(s)
  - OU level = Delegated rights to user or group account(s)
- This is a political issue rather than technical
NT/9x AD extension client

Gives you
- Site awareness (closest DC is used)
- Active Directory Service Interfaces (ADSI)
- DFS fault tolerance client
- Active Directory Windows Address Book
- NTLM version 2 authentication

Does not give you
- Kerberos support
- Group Policy nor IntelliMirror support
- IPsec nor L2TP support
- SPN nor mutual authentication
Standalone or Member?

- Only member workstations and servers have computer accounts in a child domain.
  - With a computer account an authenticated user can:
    - Browse the AD non-anonymously (shares, printers, etc.)
    - Kerberos and IPsec security
    - Secure local resources via non local accounts and groups
    - Group policies
    - Intellimirror, DFS, offline store
    - Use cached credentials for login
    - Dynamically registered IP/DNS via DHCP
    - Access resources in other domain secured by Hokies ID

© 2001 Marc DeBonis, v1.0
In conclusion

- W2K significantly enhances the Windows OS family
- These enhancements necessitate centralized system and service management for the W2K infrastructure
- Migration and consolidation allow the NT domain administrator to move into W2K AD while delegating roles and reducing domain redundancy
- Available AD client extensions provide some backwards compatibility for those systems unable or unwilling to migrate to the W2K AD
- Users must login to a W2K child domain to gain all the features and functionality of W2K and AD

© 2001 Marc DeBonis, v1.0
W2K migration and consolidation – issues and answers

Marc DeBonis
Virginia Tech – IS&C
Marc.DeBonis@vt.edu