Upgrading To Windows Server 2003 Active Directory From Windows NT 4.0 And Windows 2000

David Alberto

Senior Consultant

Microsoft Consulting Services

Agenda

- Understanding Functional Levels
- Windows NT 4.0 to Windows 2003 Server upgrade
- Windows 2000 to Windows 2003 Server upgrade
- Domain restructuring with ADMT V-2

Understanding Functional Levels

- Review mixed mode – native mode
- Functional Levels as Active Directory versioning scheme
- Overview of domain functional levels
- Overview of forest functional levels

Mixed Mode And Native Mode Domains

- Mixed Mode domains
  - Allow Windows NT 4.0 domain controllers
  - Restrict user and group management to what Windows NT4.0 DCs understand
    - No Universal Groups
    - No nested groups
    - No SID History
  - You can have mixed mode domains with 2003 Server domain controllers
    - Windows 2003 Server PDC will replicate to NT4.0 BDCs
    - Even without any Windows 2000 DCs
- Native Mode domains
  - A.k.a., “No more Windows NT 4.0 domain controllers, please” mode
  - Enable all features for group/user management
  - Can have Windows 2000 and 2003 Server DCs

Functional Levels

- Required in order to introduce non-backward-compatible features
  - Admin manually advances functional level when all DCs in forest/domain are upgraded
  - Level only increases – no going back
  - Legacy DCs blocked from joining/starting
  - Think Windows 2000 Native Mode++
- Available functional levels
  - Windows 2003 Server forest functionality
  - Windows 2003 Server interim forest functionality
    - Allows mixed-mode domains (Windows NT 4.0 BDCs), but no Windows 2000 DCs
  - Windows 2003 Server domain functionality

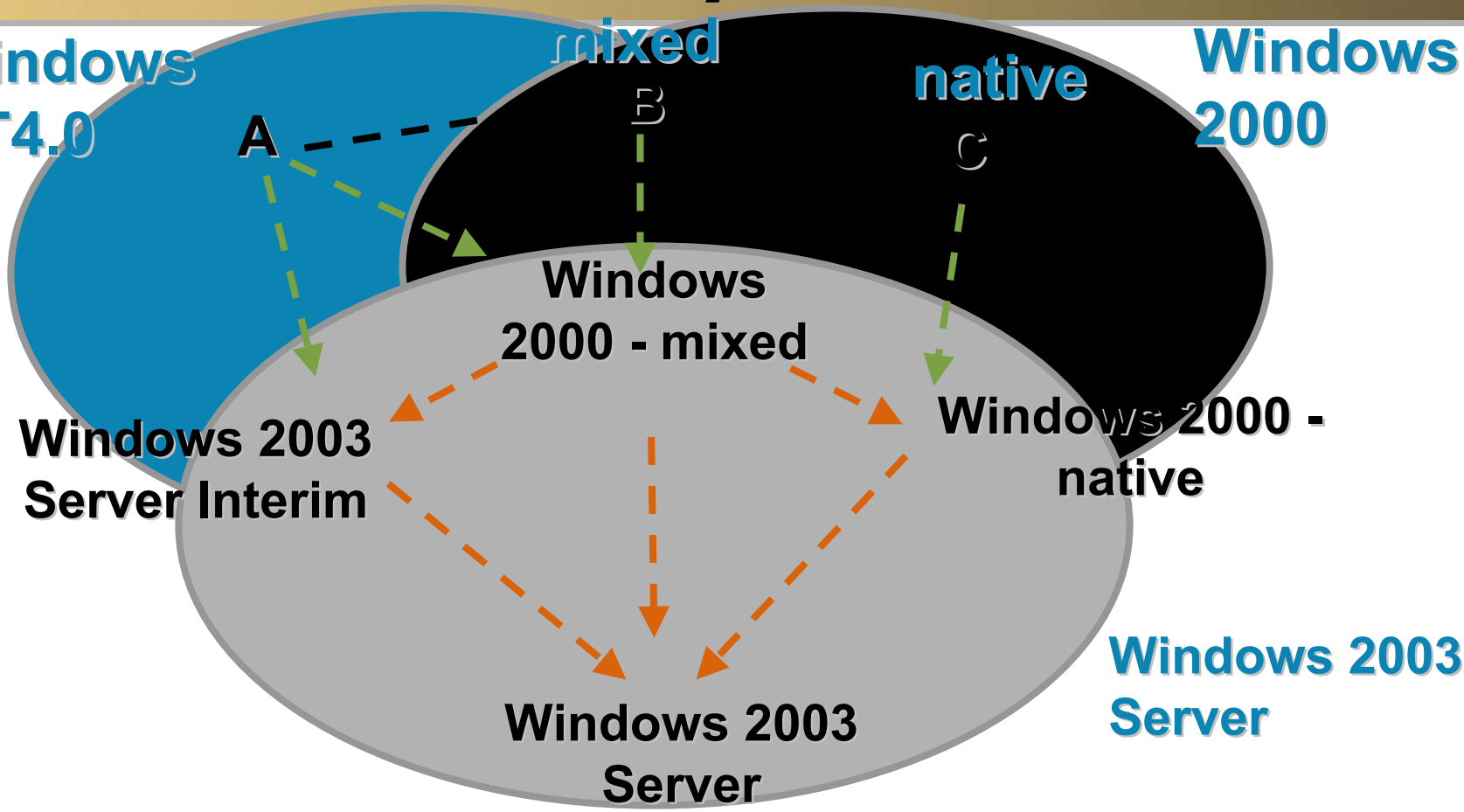
Domain Functional Levels

Domain Functionality	Enabled Features	Supported DCs in domain
Windows 2000 mixed	▪ Install from media ▪ Universal Group caching	Windows NT4.0 Windows 2000 Windows2003
Windows 2000 native	All mixed mode, plus ▪ group nesting ▪ Universal groups ▪ SIDHistory	Windows 2000 Windows 2003
Windows 2003 Server Interim mixed / native	Same as Windows 2000 mixed / native mode, depends on whether domain is mixed or native mode	Windows NT4.0 Windows 2003
Windows 2003 Server	All Windows 2000 native, plus ▪ Update logon timestamp attribute ▪ Kerberos KDC version ▪ User password on INetOrgPerson	Windows 2003

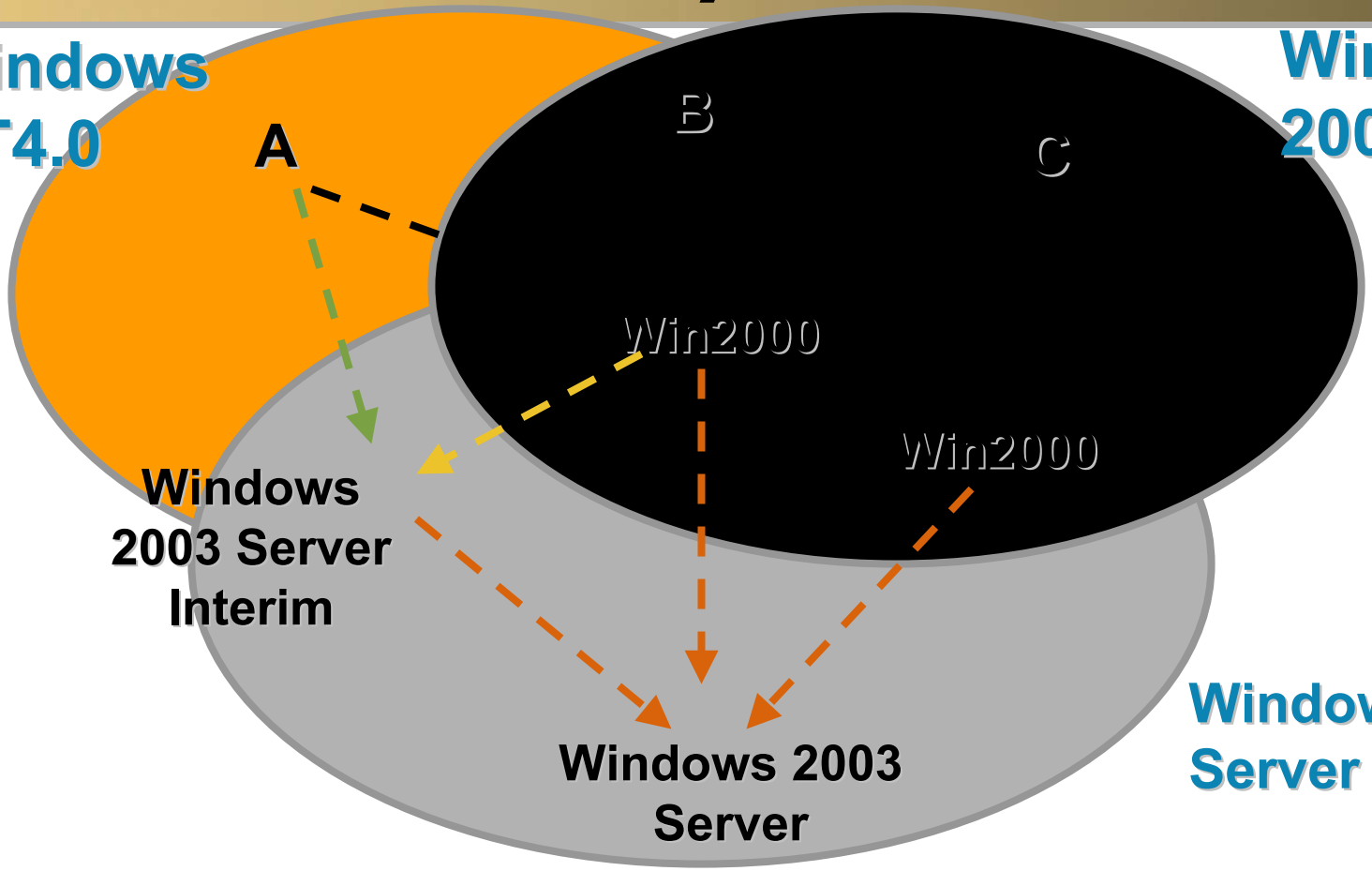
Forest Functional Levels

Forest Functionality	Enabled Features	Supported DCs in forest
Windows 2000	▪ Install from media ▪ Universal Group caching	Windows NT4.0 Windows 2000 Windows 2003
Windows 2003 Server Interim	All Windows 2000, plus ▪ LVR replication ▪ Improved ISTG	Windows NT4.0 Windows 2003
Windows 2003 Server	All Windows 2003 Server Interim, plus ▪ Dynamic aux classes ▪ User to INetOrgPerson change ▪ Schema de-/reactivation ▪ Domain rename ▪ Cross-forest trust	Windows 2003

Domain Functionality



Forest Functionality



How To Verify Domain/ Forest Functional Levels

- Easiest way: Domains and trusts snap-in
- Attributes in the directory
  - Domain Level
    - Mixed/native mode

      nTMixedDomain attribute on domain

      No value OR "1": mixed mode domain

      "0": native mode domain
    - Domain functional level

      msDS-Behavior-Version attribute on domain

      No value OR "0": Windows 2000

      "1": Windows 2003 Server interim functional level

      "2": Windows 2003 Server functional level
  - Forest Level

    msDS-Behavior-Version attribute on partitions container

    No value OR "0": Windows 2000

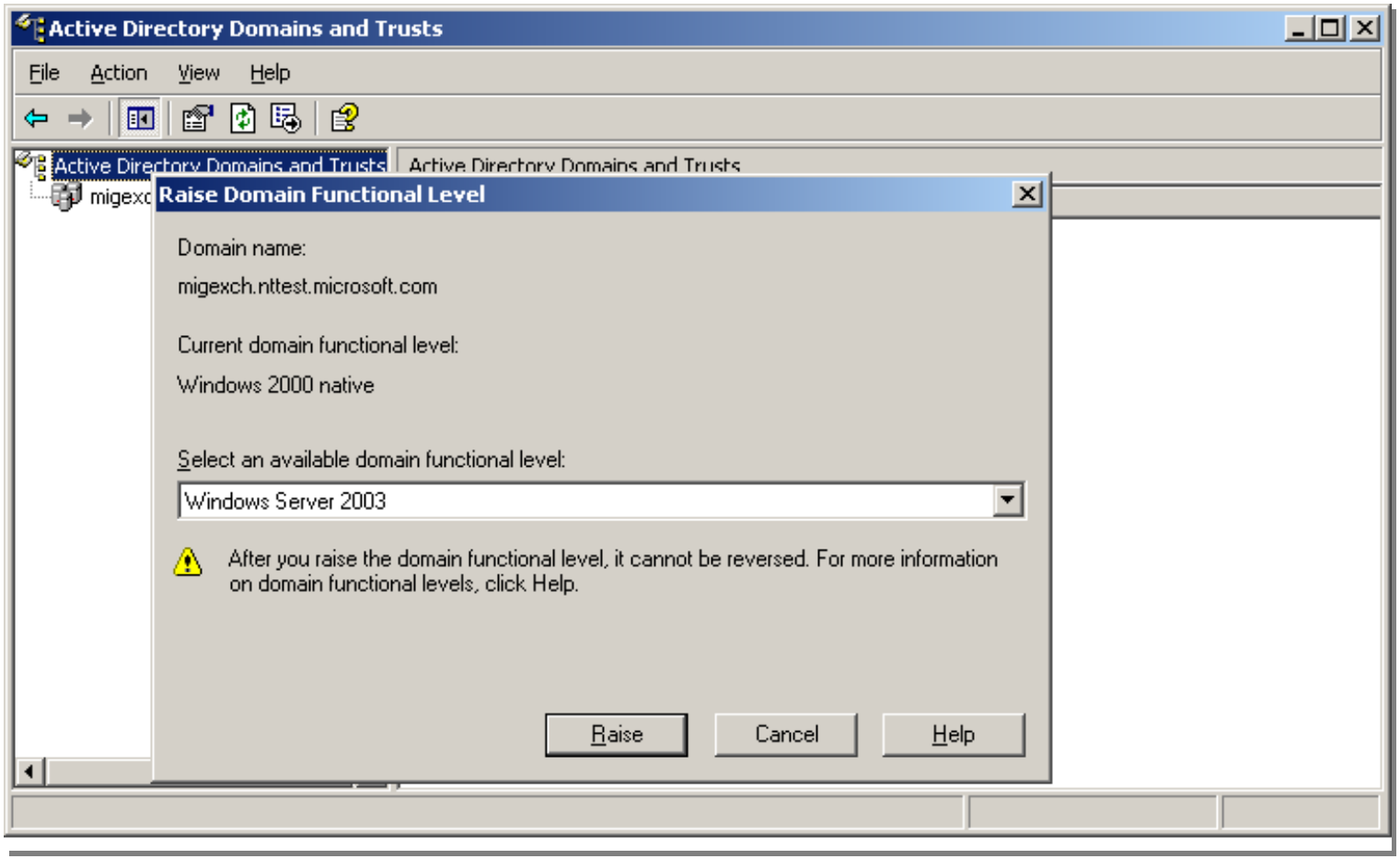
    "1": Windows 2003 Server interim functional level

    "2": Windows 2003 Server functional level

Best Practices For Functional Levels

- Windows NT 4.0 Upgrade
  - Motivation to move to Windows 2003 Server interim level
    - Linked-value-replication (large group support)
    - Improved KCC/ISTG
  - Set Windows 2003 Server interim forest level
  - Once all Windows NT 4.0 BDCs are upgraded, advance forest to Windows 2003 Server functional level
    - This automatically advances all domains to Windows 2003 Server functional level
- Windows 2000 Upgrade
  - Do nothing until all DCs are running Windows 2003 Server
  - Make sure that no mixed mode domain is left in the forest
  - Advance forest level to Windows 2003 Server functional level
    - This automatically advances all domains to Windows 2003 Server functional level

Raising Domain Functional Level



What Else Happens When I Upgrade…

- Domain Level
  - Special operations on PDC upgrade or role transfer to PDC operations master
- Forest Level
  - Special operations when forest is switched to Windows 2003 functional level
- Domain and Forest Level switches
  - Attributes that define functional levels are initialized

Upgrading PDC

- New well-known and built-in groups are created
  - Builtin\Remote Desktop Users (not on XP)
  - Builtin\Network Configuration Operators (not on XP)
  - Performance Monitor Users
  - Performance Log Users
  - Builtin\Incoming Forest Trust Builders (DC only)
  - Builtin\Performance Monitoring Users (not on XP)
  - Builtin\Performing Logging Users (not on XP)
  - Builtin\Windows Authorization Access Group (DC only)
  - Builtin\Terminal Service License Server (DC only)

Upgrading PDC

- Some new group memberships are established
  - If **Everyone** is in the **Pre-Windows 2000 Compatible Access** group, **Anonymous Logon** and **Authenticated Users** is added
  - **Network Servers** is added to **Performance Monitoring** alias
  - **Enterprise Domain Controllers** is added to **Windows Authorization Access** group
- Well-known security principals added to configuration container
  - Makes security principals rename safe
  - 8 new security principals
  - Example: WinThisOrganizationSID: “This Organization”
- Containers for Quotas are created
- Has low network / performance impact

Forest Switch To Windows 2003 Functional Level

- Domain controllers switch to new replication pause values
  - Windows 2000: registry values
    - 5 minutes / 30 seconds
  - Windows 2003: new default values if registry keys are not set
    - 15 seconds / 3 seconds
  - At forest functional switch
    - DCs delete registry values if values are Windows 2000 defaults
    - Automatically switch to 15 seconds / 3 seconds

Forest Switch To Windows 2003 Functional Level

- Attributes added to the GC
  - ms-DS-Trust-Forest-Trust-Info
  - Trust-Direction
  - Trust-Attributes
  - Trust-Type
  - Trust-Partner
  - Security-Identifier
  - ms-DS-Entry-Time-To-Die
  - MSMQ-Secured-Source
  - MSMQ-Multicast-Address
  - Print-Memory
  - Print-Rate
  - Print-Rate-Unit
  - MS-DRM-Identity-Certificate
- No GC – Full Sync – low replication impact!

Agenda

- Understanding Functional Levels
- Windows NT 4.0 to Windows 2003 Server upgrade
- Windows 2000 to Windows 2003 Server upgrade
- Domain restructuring with ADMT V-2

Before You Begin 1/2

- Review Active Directory logical and physical structure
- Create inventory of servers and workstations
  - Hardware, network cards, operating system, server role
  - Special emphasis on Windows 95 and Windows NT 4.0 workstations with SP2 or lower

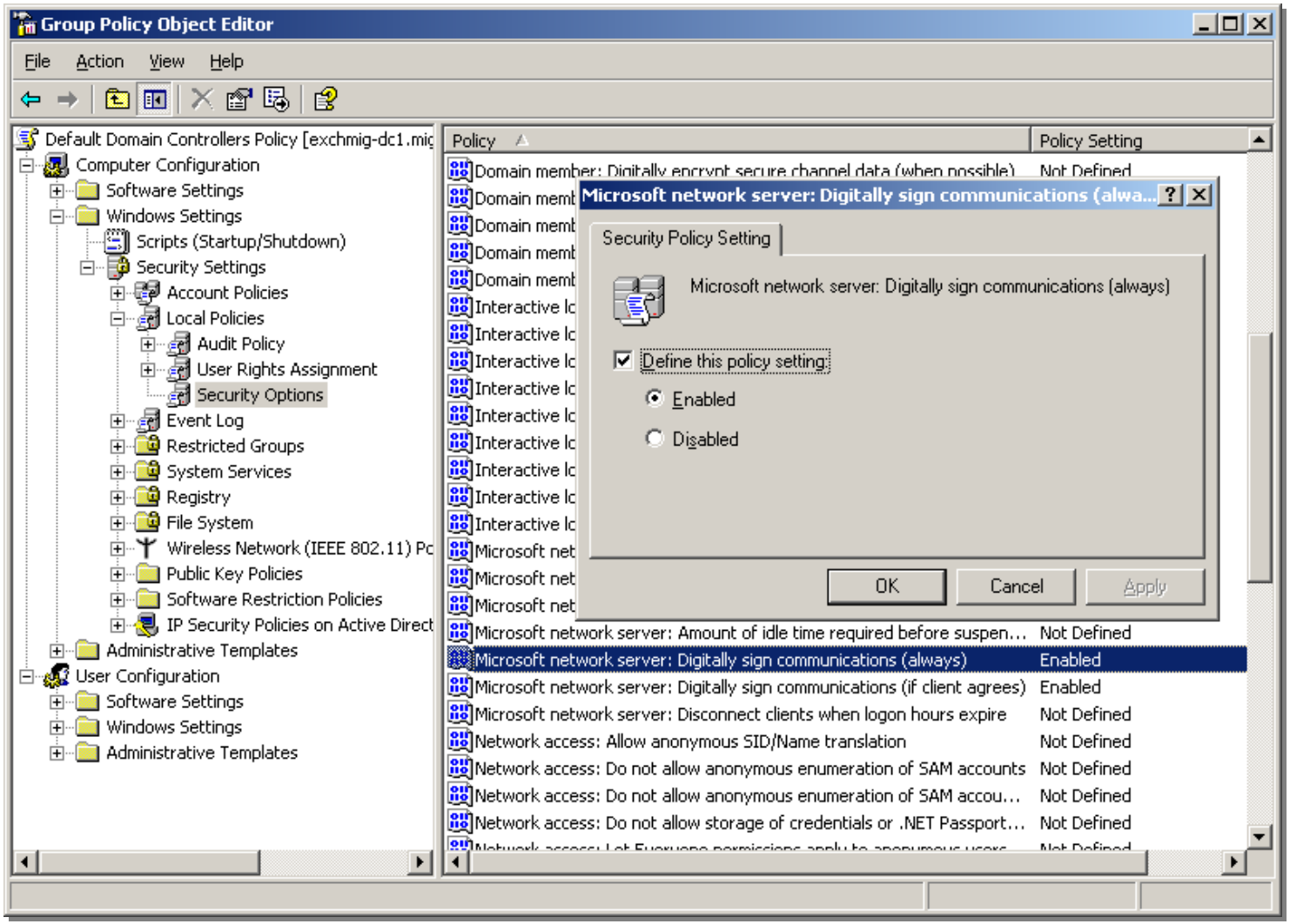
Before You Begin 2/2

- Document services and service accounts
  - Special emphasis on services that run under local system
- Develop a test plan
- Develop a recovery plan
  - Backup tapes of Window NT 4.0 DCs
  - Keep one BDC off-line in storage

Clients And Windows 2003 Servers

- Security improvements change behavior of Windows 2003 Server Domain Controllers
  - SMB signing enforced
  - Domain Controller access policies
- Adjustments needed for older clients
  - Windows NT 4.0 SP3 and higher, Windows 2000, Windows XP clients work without adjustments
  - Windows 9x and Windows NT 4.0 pre-SP3 require to make changes to the default policies
    - Disable enforcement of SMB signing
    - Network access, allow anonymous SID look-up
- Fully documented in the Windows 2003 Server Deployment Kit and KB article

SMB Signing Policy



Services Running As Local System

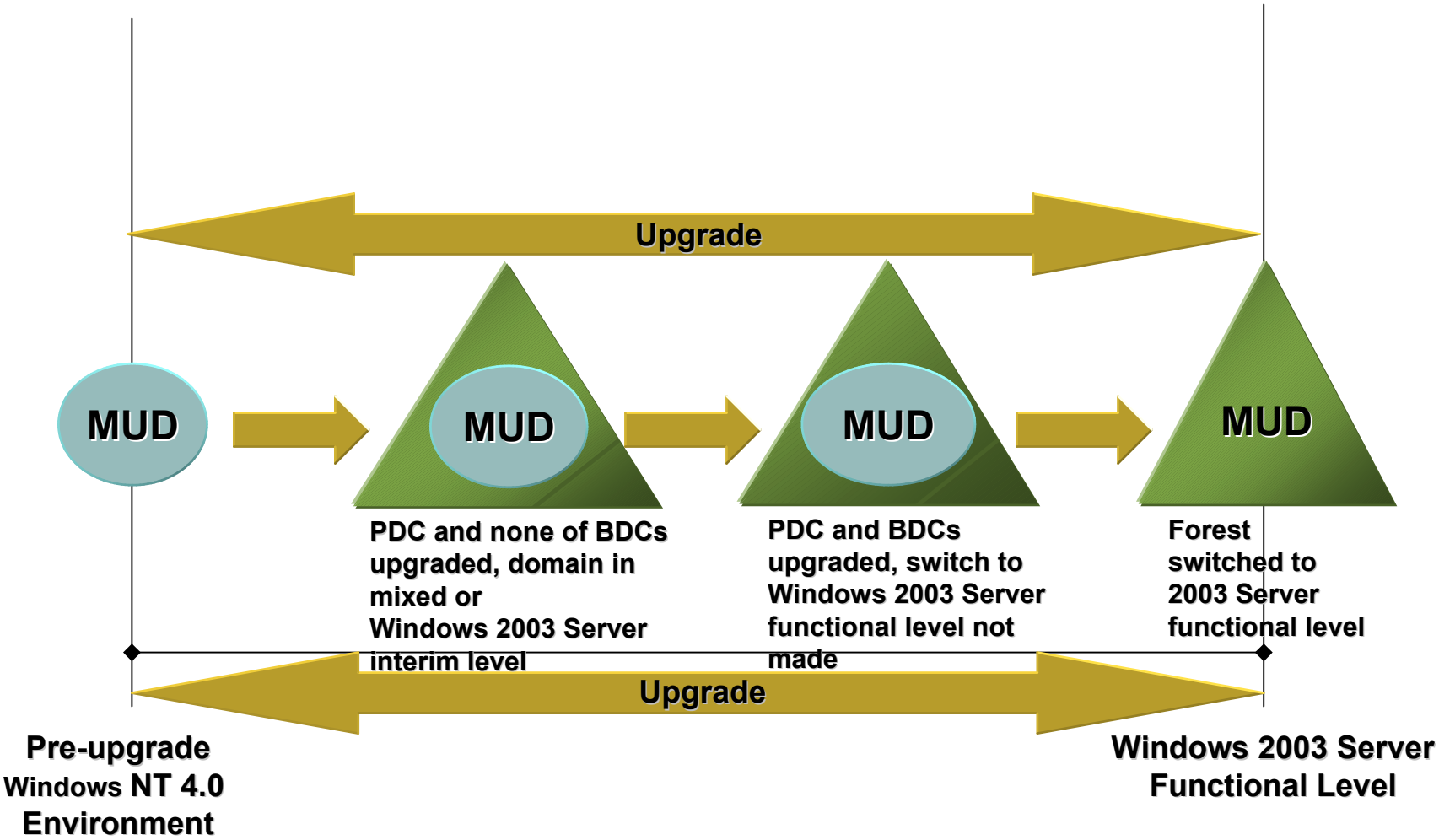
- Services using Local System sometimes need to access resources over the network
  - Windows NT4.0: Use NULL session (unauthenticated)
  - Windows 2000 and higher: Use local computer account
- Example: RAS services running on a member server verifies RAS access for user
  - Needs to contact domain controller over the network
- Solution
  - Upgrade servers to Windows 2000 or higher, or
  - Configure domain to allow anonymous access
    - In dcpromo
    - Adds Everyone group and Anonymous Access group to Pre-Windows 2000 compatible access group
    - Anonymous access should be removed once all servers are upgraded by removing these groups from everyone

Preparing The Upgrade

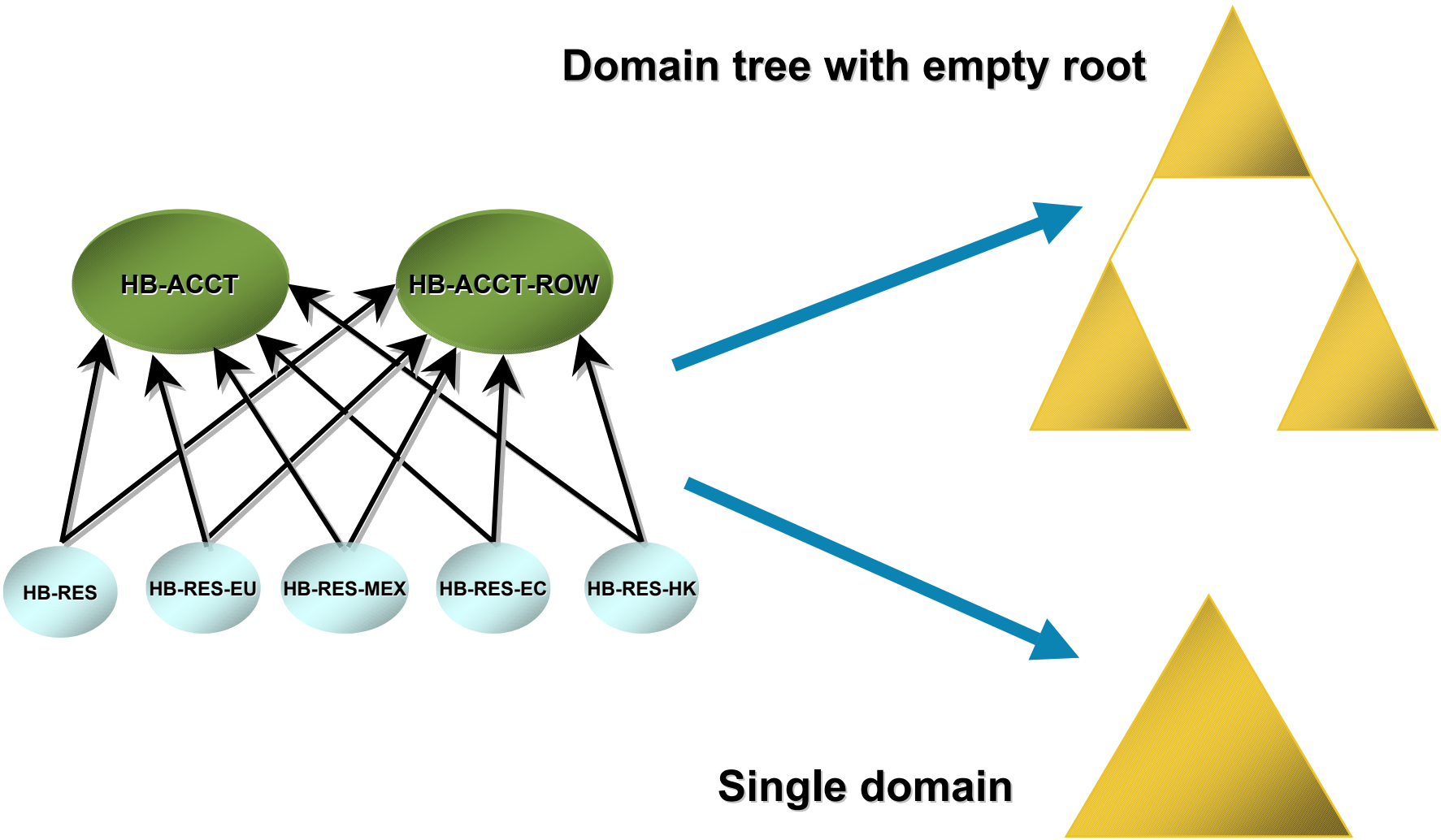
- If you already have DNS
  - Create delegation entry in parent DNS domain for the first domain controller
- Configure lmrepl service
  - LanManager File replication service, used in Windows NT 4.0 to replicate logon scripts
  - Export server is typically the PDC
  - Lmrepl export service should be last domain controller to be upgraded
    - Configure BDC to be lmrepl export server, or
    - Transfer PDC role

Upgrade Considerations

Stages of upgrade



Upgrading From Windows NT 4.0



Upgrading Into Single Domain Forest 1/2

- Upgrade OS on PDC
- Start dcpromo
- Dcpromo will read delegation entry for PDC and prompt to install DNS Server
  - Install DNS Server
  - DNS zones for forest wide DNS entries and domain wide DNS entries will be created automatically
  - DNS client will automatically point to local DNS Server as preferred DNS Server
- Set Windows 2003 Server interims forest functional level when dcpromo runs on PDC

Upgrading Into Single Domain Forest 2/2

- Continue upgrading BDCs
  - Run OS upgrade and dcpromo
  - Install DNS Server
  - Create delegation entries
- Once all DCs are upgraded
  - Advance forest to Windows 2003 Server functional level
- Begin restructuring of remaining account/ resource domains
  - SID history requires native mode/ Windows 2003 Server target domain

Upgrading Into Multi-Domain Forest

- Install empty forest root domain first
  - Use AD integrated DNS
  - Advance domain to Windows 2003 Server domain functional level
- Set Windows 2003 Server forest interim functional level
  - No UI, use ldp or adsiedit
- Create delegation entries for PDC
- Upgrade PDC and create child domain of empty root domain
  - DNS Server will create application partition for DNS data
    - Must be logged on as Enterprise admin
  - Domain will be automatically set to 2003 Server interim functional level
- Create delegation entries for BDCs and upgrade BDCs
- Once all DCs in forest are upgraded, advance forest functional level to Windows 2003 Server

Agenda

- Understanding Functional Levels
- Windows NT 4.0 to Windows 2003 Server upgrade
- Windows 2000 to Windows 2003 Server upgrade
- Domain restructuring with ADMT V-2

Upgrade From Windows 2000

- Easy and seamless upgrade process
  - No restructuring necessary
  - No forest, domain, OU or replication planning necessary
  - No user/workstation/profile migration
- Windows 2003 Server DCs fully compatible with Windows 2000 DCs
  - Windows 2003 Server DCs can play in Windows 2000 forest/ domain in any role
    - New DC (dcpromo)
    - Upgrade of existing DC
- Preparing forest and domains are separate step from introducing the first 2003 Server DC

Active Directory Upgrade Management

- New features or fixes in Active Directory require changes
  - New objects must be created
  - ACLs need to be adjusted
  - Schema extensions
- Multiple sources might need changes
  - SP update, QFE, new OS major release
  - These can be the same changes
- Upgrade management is idempotent
  - Upgrade application can run many times, change will be applied only once
- Entries in the directory express that change has been applied successfully
  - GUID based entries
  - Forest wide changes in cn=Operations,cn=ForestUpdates,cn=configuration,dc=<fores_root_domain>
  - Domain wide changes in cn=Operations,cn=DomainUpdates,cn=system,DC=<domain>

Windows 2000 Forest / Domain Upgrade

- New Windows 2003 Server features require upgrade operations
  - Anonymous != Everyone
  - Security fixes (changes in default security settings)
  - Display specifier updates
  - Schema extension
- Single tool (adprep) to accomplish all tasks
  - Run once per forest (adprep /forestprep)
  - Run once per domain (adprep /domainprep)
- Adprep /forestprep replaces schupgr

ADPREP /FORESTPREP

- Schema upgrade
  - Calls schupgr
  - Needs to run on schema master
  - Does not cause a GC full-sync
    - Partial Attribute Set extended when forest is advanced to 2003 Server forest mode
  - Small number of new indexed attributes
    - Indices need to be built on local DC when schema change replicates in
    - Pre-SP3 DCs: Performance impact while indexing runs
    - SP3 DCs: No performance impact
  - Schema extension creates little replication traffic only
- Display specifiers
  - Enables new features in UI
  - Creates around 100KB replication traffic

ADPREP /FORESTPREP

- Adjusts ACLs to enable new features
  - RSOP, Everyone != Anonymous logon, PKI
  - Little replication traffic only
- Adprep /forestprep has only small impact
  - Replication
  - Domain controller performance
    - No impact on Windows 2000 SP3 DCs
    - Small impact on pre-Windows 2000 SP3 DCx
  - AD database size
- Creates special container when finished successfully
  - CN=Windows2003Update,CN=ForestUpdates,CN=Configuration,DC=<forest_root_domain>

ADPREP /DOMAINPREP

- Needs to run on Infrastructure Master in each domain
- Creates three new objects in the domain
  - One for WMI, two for COM
- Extends small number of ACLs to make new features work
  - RSOP, security changes
- Impact on Domain Controllers hardly measurable
  - Little network traffic
  - No DC performance impact
- Creates special container when finished successfully
  - CN=Windows2003Update,CN=DomainUpdates,CN=System,DC=<domain>

Issues With Schema Extensions

- Exchange 2000 schema present
  - Exchange 2000 schema extensions define two non-RFC conform attributes (secretary and labeledURI)
  - If Exchange 2000 schema extensions are applied before Windows 2000 InetOrgKit or Windows 2003 schema, attributes with mangled names are created
  - See KB article Q325379
- SFU 2
  - SFU 2 defines uid incorrectly
  - Adprep cannot extend unless QFE is applied
  - See KB article Q293783

Introducing The First Windows 2003 Server Domain Controller In Forest

- Once adprep has run, Windows 2003 Server Domain Controllers can join the forest
- Two methods
  - Upgrade existing domain controller (Windows 2000 or Windows NT 4.0)
  - Install 2003 Server as member server and run dcpromo
- Choose any domain to hold the first 2003 Server DC
- Upgrade of PDC performs special operations again
  - Creates group for Terminal Service, internal groups
  - Role transfer to 2003 Server DC triggers same operations
- Best practice
  - Install 2003 Server member server and promote to Domain Controller
  - Upgrade PDC to 2003 Server early in the process
    - Or transfer PDC role to 2003 Server DC, even if temporarily only

Domain Upgrade And DNS

First domain controller in Forest/Domain

- First Windows 2003 Server DC in a forest/domain creates application partition for forest/domain wide DNS data
  - Prerequisites
    - Domain Naming Master must be on-line
    - Domain Naming Master must run Windows 2003 Server
  - If creation of application partition fails
    - DNS manager can be used later to create partition

Domain Upgrade And DNS

Adding Windows 2003 Server domain controllers

- Additional Windows 2003 Server DCs request replica of
  - Domain wide DNS application partition
  - Forest wide DNS application partition
- DNS data needs to be moved to application partition manually
  - Motivation: Removes DNS data from GC
  - Once all DCs are running Windows 2003 Server, data should be moved
  - Easy through DNS manager

Introducing 2003 Server Domain Controllers

Best practices

- Easiest way
  - Upgrade Domain Naming Master first
    - Automatically creates application partitions
  - Additional DCs at leisure
    - Either upgrades or promoted 2003 Server member servers
- Safest way
  - Promote Windows 2003 Server member server to domain controller in a small domain
    - Creation of DNS application partitions will fail
  - When you feel confident, upgrade Domain Naming Master to Windows 2003 Server
    - Create DNS application partitions for forest and all domains that already have Windows 2003 Server DCs manually
- Either upgrade PDC or transfer PDC role to a Windows 2003 Server DC as soon as possible

Agenda

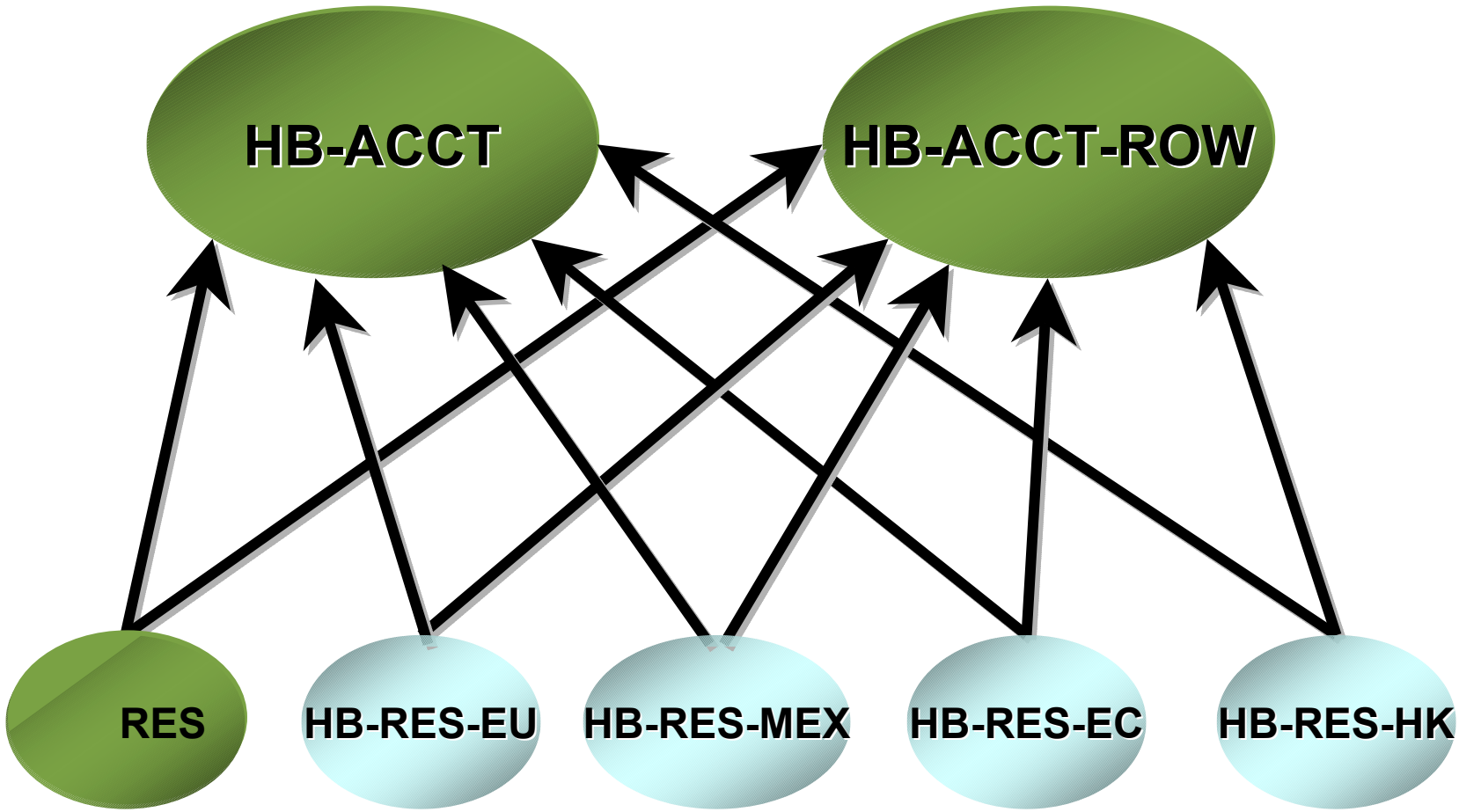
- Understanding Functional Levels
- Windows NT 4.0 to Windows 2003 Server upgrade
- Windows 2000 to Windows 2003 Server upgrade
- Domain restructuring with ADMT V-2

Migrating To Windows 2003 Server

- Most migrations from Windows NT 4.0 to Active Directory are a mix of in-place upgrades and restructuring
- See “Best Practice Active Directory Design for Managing Windows Networks” for more information
  - http://www.microsoft.com/windows2000/techinfo/planning/activedirectory/bpaddsgn.asp

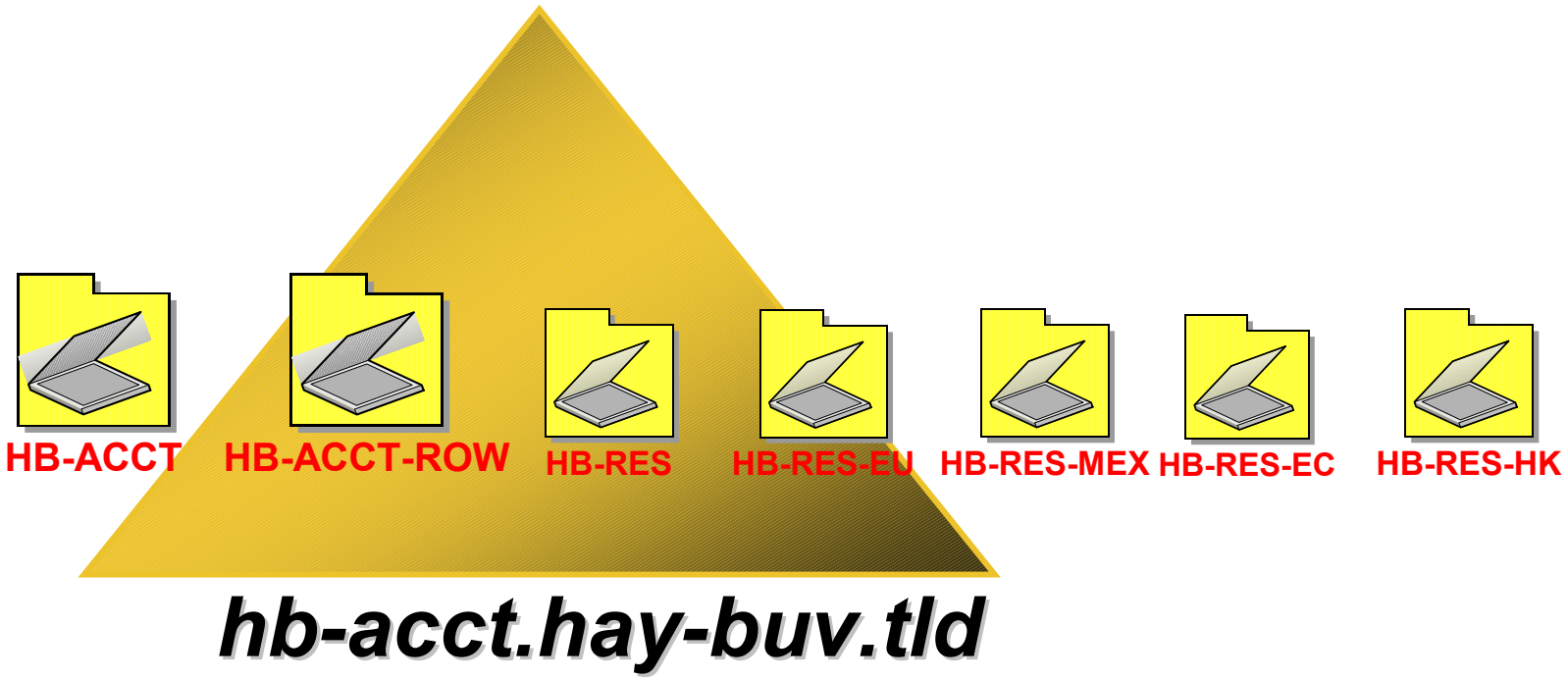
Hay-Buv Toys

Domain structure



Hay-Buv Toys

Post Migration Domain Structure



Restructure Activities

Activity	Part of
User migration	Account domain restructuring
Global Group migration	Account domain restructuring
Migrating user profiles	Account domain restructuring
Migrating Exchange mailbox access	Account domain restructuring
Migrating workstations	Resource domain restructuring
Migrating resources	Resource domain restructuring

ADMT V-2: New Features 1/3

- ADMT V-2 is part of Windows 2003 Server
  - Found in i386\ADMT folder on CD
- Inter-forest password migration
  - Source: Windows NT 4.0 (incl. syskey), Windows 2000, Windows 2003 Server
  - Target: Windows 2000, Windows 2003 Server
- Scripting interface
- Command line interface

ADMT V-2: New Features 2/3

- Migration delegation
- Supplying credentials
- Performance improvements
- Improved logging
- Account transition options
- Attribute exclusion list

ADMT V-2: New Features 3/3

- INetOrgPerson support
- Improved robustness of computer move operations
- Extensions for security translation
- Reporting Wizard
- New column in trust migration wizard to view trust properties

Summary

- Windows NT 4.0 to Windows 2003 Server upgrade very similar to Windows NT 4.0 to Windows 2000 upgrade
- Windows 2000 to Windows 2003 Server upgrade is easy and requires no planning
- ADMT V-2 makes restructuring easier

Interex, Encompass and HP bring you a powerful new HP World.