Active Directory Troubleshooting

Gary L. Olsen

Global Services Engineering

Hewlett -Packard

Gary.olsen@HP.com

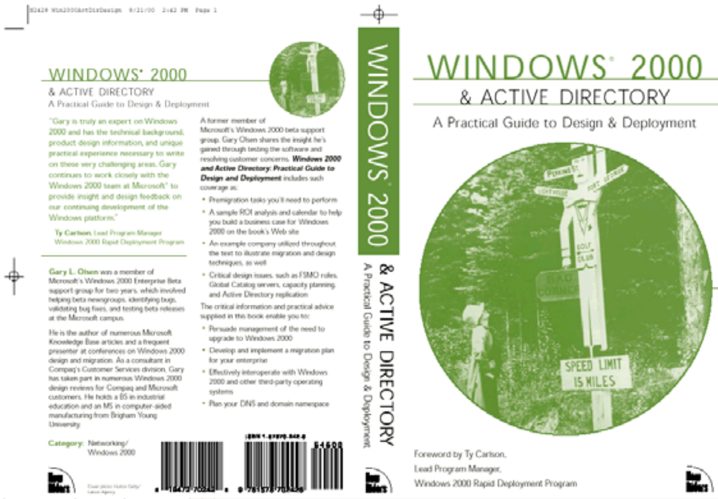
Books

Windows 2000: Active Directory Design & Deployment

Author: Gary Olsen

Publisher: New Riders

ISBN: 1578702429



82429 Win2000ActDirDesign 8/21/00 2:42 PM Page 1

WINDOWS® 2000

& ACTIVE DIRECTORY

A Practical Guide to Design & Deployment

"Gary is truly an expert on Windows 2000 and has the technical background, product design information, and unique practical experience necessary to write on these very challenging areas. Gary continues to work closely with the Windows 2000 team at Microsoft" to provide insight and design feedback on our continuing development of the Windows platform."

Ty Carlson, Lead Program Manager Windows 2000 Rapid Deployment Program

Gary L. Olsen was a member of Microsoft's Windows 2000 Enterprise Beta support group for two years, which involved helping beta newsgroups, identifying bugs, validating bug fixes, and testing beta releases at the Microsoft campus.

He is the author of numerous Microsoft Knowledge Base articles and a frequent presenter at conferences on Windows 2000 design and migration. As a consultant in Compaq's Customer Services division, Gary has taken part in numerous Windows 2000 design reviews for Compaq and Microsoft customers. He holds a BS in industrial education and an MS in computer-aided manufacturing from Brigham Young University.

A former member of Microsoft's Windows 2000 beta support group, Gary Olsen shares the insight he's gained through testing the software and resolving customer concerns. ***Windows 2000 and Active Directory: Practical Guide to Design and Deployment*** includes such coverage as:

- Premigration tasks you'll need to perform
- A sample ROI analysis and calendar to help you build a business case for Windows 2000 on the book's Web site
- An example company utilized throughout the text to illustrate migration and design techniques, as well
- Critical design issues, such as FSMO roles, Global Catalog servers, capacity planning, and Active Directory replication

The critical information and practical advice supplied in this book enable you to:

- Persuade management of the need to upgrade to Windows 2000
- Develop and implement a migration plan for your enterprise
- Effectively interoperate with Windows 2000 and other third-party operating systems
- Plan your DNS and domain namespace

Category: Networking/ Windows 2000

Cover photo: Hulton Getty/ Liaison Agency

WINDOWS® 2000 & ACTIVE DIRECTORY

A Practical Guide to Design & Deployment

WINDOWS® 2000

& ACTIVE DIRECTORY

A Practical Guide to Design & Deployment

Foreword by Ty Carlson,
Lead Program Manager,
Windows 2000 Rapid Deployment Program

Windows Server 2003 on ProLiant Servers

Authors: Gary Olsen, Bruce Howard

Publisher: New Riders

ISBN: 0131467581

Publishing Date: August, 2004

Topics

- **CLASS EXERCISES!**
  - Troubleshooting Basics
  - Troubleshooting DNS
  - Troubleshooting Replication
  - Troubleshooting DCPromo
  - Troubleshooting Group Policy

Troubleshooting Basics

Define the Problem
Work the Problem
Collect Data
Action Plan

Define the Problem

Is there one?

- Define the Problem
  - Events are NOT the problem!
  - What exactly is failing?
- Define the Scope
    - One or multiple Machines
    - One or more users
    - Single or multiple sites?
    - Single or multiple DCs? (check logon server env. Variable)
    - Members of same or multiple groups?
    - Group Policy applied (event 1704 in app log)
    - Time of day

Work the Problem

Is there one?

- Impact to the business
  - Urgency
  - Resource allocation
- After Defining the Problem, are there events in the event log related to the failure and time of failure?
- When did you notice it? What conditions?
  - Tie the times to the events, other log entries
- Can the problem be replicated?
  - Start narrowing the variables
  - Identify a savvy user with the problem who can help

Collect Data

- MPSReports
  - Free download (see slide notes)
  - All Event Logs in .txt, evt format
  - Netdiag, DCdiag, Net Accounts, Net Share,
  - Repadmin
  - DCpromo Logs
  - GPOtool, GPresult
  - Run it on all affected machines
- Other
  - Verbose Logging
  - Get status report from Replication Monitor

The Action Plan

- Define the Problem
  - Talk to all admins involved
  - Who is affected? (computers, users)
  - When? Is it reproducible?
  - Area
    - Replication
    - Security
    - Name Resolution
    - Group Policy
    - FRS/DFS
- What data needs to be collected?
- Analyze the Data
  - Errors, warnings, etc
  - Solution
    - Google
    - www.eventid.net
    - Microsoft KB
- Test Solutions

Action Plan Example

Overview: Determine cause of hang of ATL-DC1

Summary:

- analyzing perfmon logs
- implemented contingency plan
- identified support path

Action: Perfmon log analysis.
Why: to compare baseline (current) with Monday’s hang events
Priority: Medium
When: March 25
Who: Jim Shoos, Don Juan
Status: In progress

Action: Crash dump analysis.
Why: determine cause of Monday’s hang
Priority: Medium
When: March 27
Who: Jack Sprat
Status: In progress

Troubleshooting DNS

Basics
Configuration Issues
Quick Checks
Common Problems
Problem Solving Exercises

DNS Basics

- Understand DNS
  - www.microsoft.com/dns (DNS Center)
- Analyze the DNS infrastructure
  - Diagram
  - Details (delegation, forwarding, etc)
- Netlogon registers DNS records
  - Net start Netlogon & Net stop Netlogon
- Zone must contain _msdcs, _sites, _tcp, _udp sub zones for SRV records

DNS Resolver Configuration

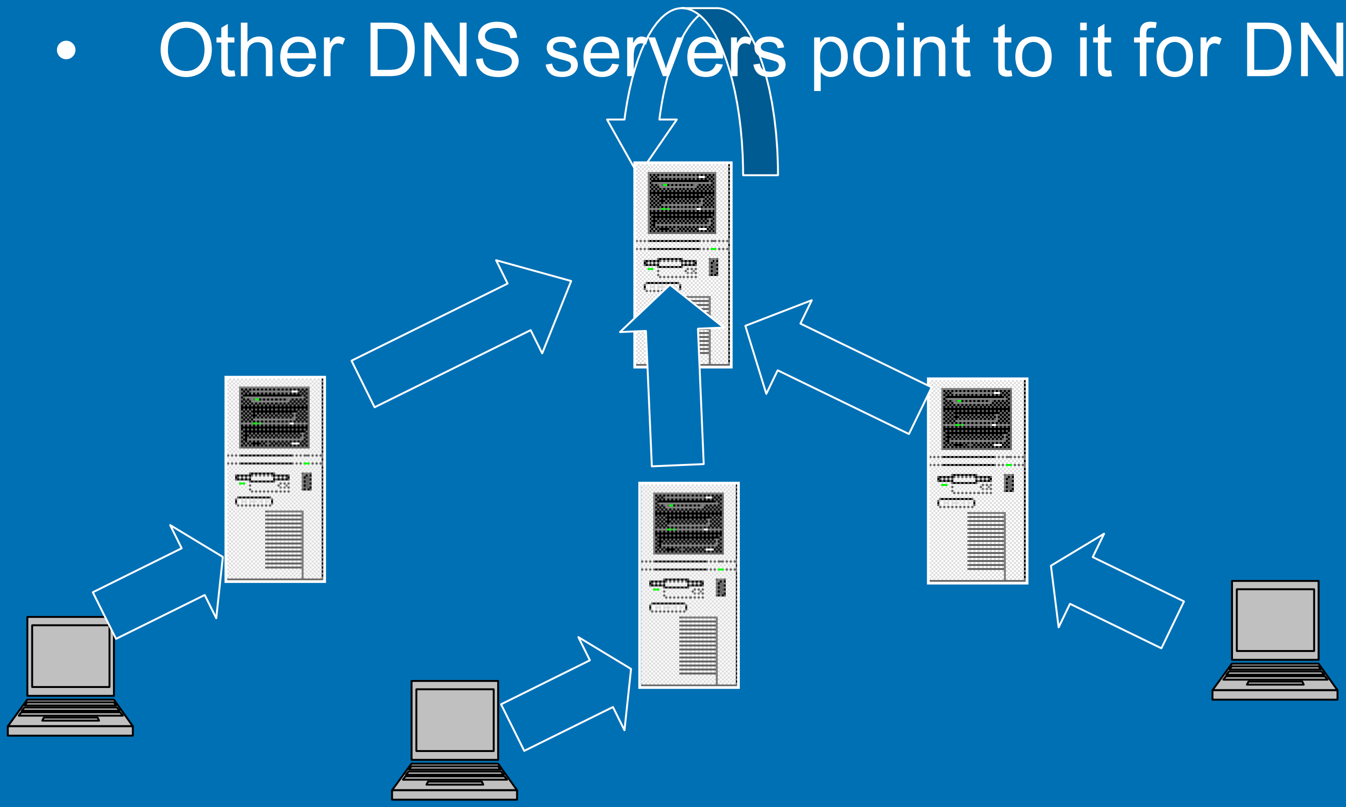
- Workstations, Servers, DCs point to NS for their domain
  - No reason to point to other name servers like ISP, other internal NS, as “additional DNS servers”
- Std primary zone name server – points to self for DNS
- ADI Zone
  - Only one NS points to self for DNS
  - Other NS point to single “primary”

DNS Server Configuration

- Server Properties
  - Forwarding
  - Zone Transfers
    - Restricted Servers
  - Enable Scavenging
- Delegation
  - Correct server, IP address?
- Resolver (Tcp/IP Properties)

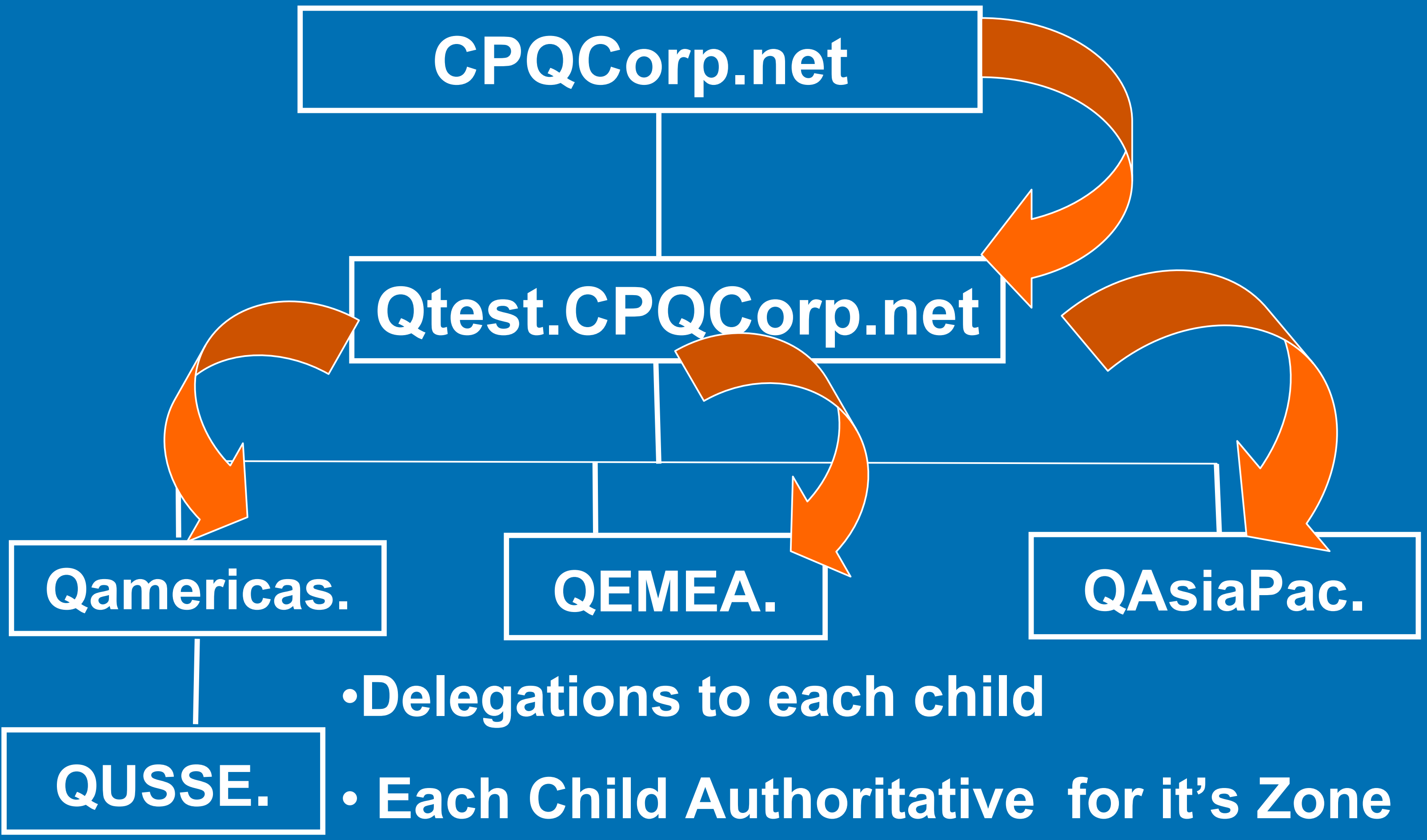
ADI Server Configuration

- Best Practice: Select single ADI DNS Server as the “Primary”.
  - Primary is only one pointing to itself for DNS
  - Other DNS servers point to it for DNS



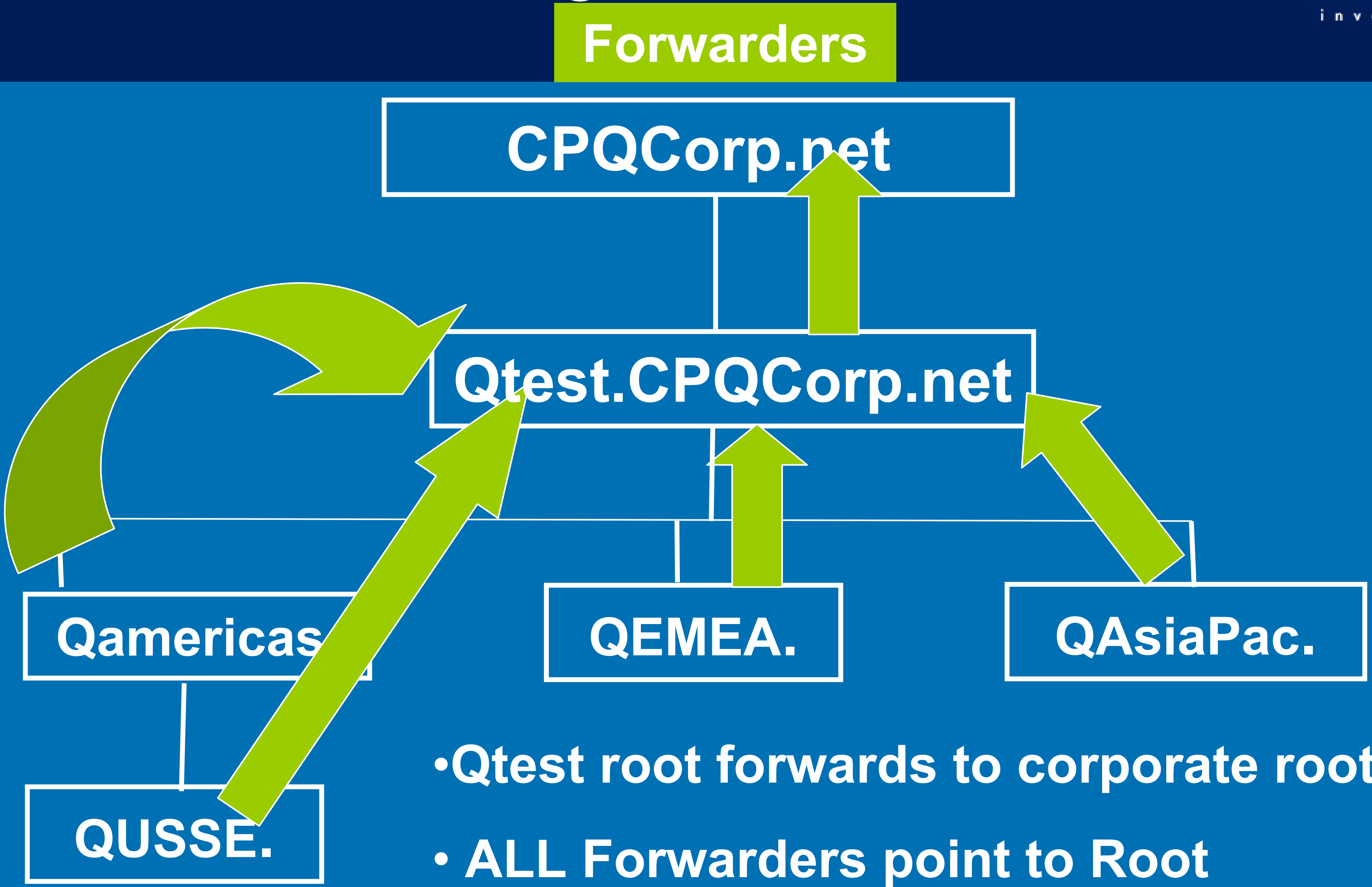
Qtest DNS Configuration

Delegations



- Delegations to each child
- Each Child Authoritative for it’s Zone
- ADI – 2 DNS Servers per Zone

Qtest DNS Configuration



- Qtest root forwards to corporate root
- ALL Forwarders point to Root
- “No Recursion” box checked

Quick Checks

- Access to Internet is different issue
- Clear client and server cache
- Check TCP/IP properties
- Check the DNS topology
  - ADI Zones
- _msdcs zone in root domain only
  - Cname Records
  - GC Records

Quick Checks

- Use Monitor tab in DNS snap-in
  - Test Recursive, simple queries
- Ping
  - Domain name
  - Server Name, address
- NSLookup

  ```
  nslookup gc._msdcs.qtest.cpqcorp.net
  ```
- Delete bad records, restart Netlogon svc

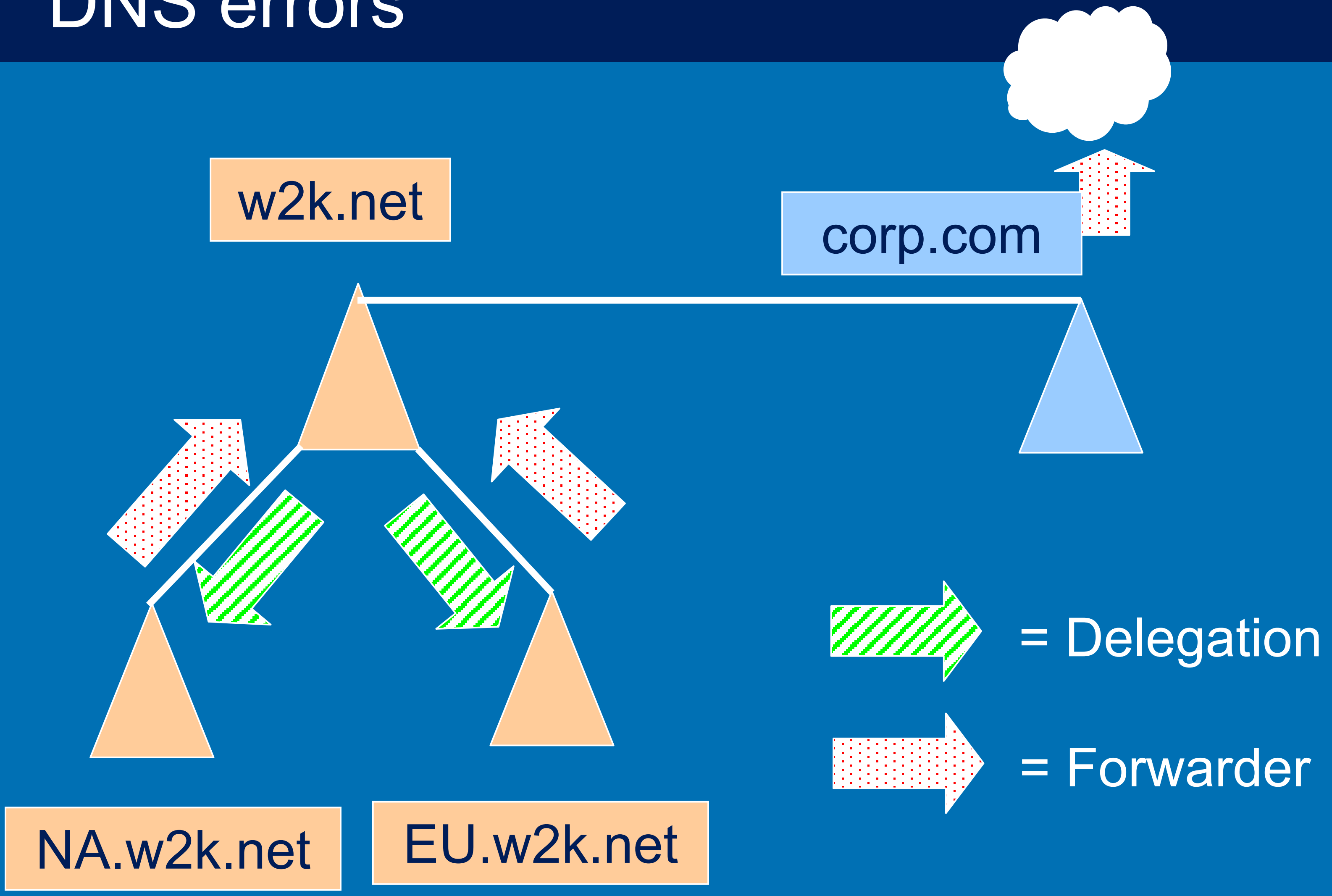
Common Problem: Missing sub zones for SRV records

- First DC creates subzones for SRV records
  - _msdcs, _Sites,_TCP,_UDP
- If they aren’t there…
  - Check Tcp/ip properties for DNS server
  - Dynamic Updates on
  - Physical connectivity to DNS server
- Bonus Question: What if you delete these zones?

Problem: Promotion of 2nd DC fails: Unable to contact domain

- Just promoted a new DC to create a new forest, company.com.
- Promoting 2nd DC in that domain yields an error saying it can’t contact the domain.
- How do you troubleshoot this?

Problem: Replication Broken in child domain DNS errors



w2k.net

corp.com

NA.w2k.net

EU.w2k.net

= Delegation

= Forwarder

Troubleshooting AD Issues

Tools
MPSReports
Tips
Account Lockout
Problem Solving

XP and Windows 2003
Remote Desktop Resource Redirection

- Client Resources Available when using Terminal Services Remote Desktop
  - **File System** – Local drives and Network drives on Local Machine available on Remote machine
  - **Audio** – Audio streams such as .wav and .mp3 files can be played through the client sound system.
  - **Port** – Applications have access to the serial and parallel ports
  - **Printer** – The default local or network printer on the client becomes the default-printing device for the Remote Desktop.
  - **Clipboard** – The Remote Desktop and client computer share a clipboard
  - **Terminal Services Virtual Channel Application Programming Interfaces** (APIs) are provided to extend client resource redirection for custom applications.

Windows XP as a Tool!

- Adminpak for Win2K
- Adminpak for Windows 2003
- GPresult.exe
  - RSOP, ACL Filters, Policy Priority List,
- Group Policy Management Console
  - Save GPO settings, User application
- Repadmin (new features)
- Remote Desktop

NTDSUtil (Windows 2003)

- Authoritative restore
  - Roll AD back to previous date
  - Entire AD, tree or object
  - Improved in Windows Server 2003 (with LVR)
  - DSRM Mode
- Domain management
  - Create Application Partitions
  - Pre-create domains
- Metadata cleanup
  - Remove Server, domain, site objects
- Roles
  - FSMO Management: See, change all roles
- Semantic database analysis
  - Can repair checksum, inconsistency errors
  - DSRM mode
- Set DSRM Password or account password

ADSIedit.exe Demo

- GUI much like Users & Computers snap-in/Advanced features.
- Graphical view of AD.
- Like LDP.exe but:
  - Easier to browse.
  - Can modify attribute values
  - **Shows ALL attributes**
- Don’t confuse with Users & Computers!

LDP.exe Demo

- Takes time to set up:
  - Connect
  - Bind
  - View – Tree
  - Enter DN to start (blank for default)
- Exposes attributes quickly, easy to see.
  - **Only lists DEFINED attributes**
- Faster than ADSIedit – no GUI to traverse.
- LDAP searches.
- Can delete and modify, but not as easy as ADSIedit.
- Can execute remotely.

MPS Reports

- Demo/Exercise – Using MPS Reports for AD Troubleshooting, Health Check

Active Directory Problem Diagnosis (Class exercise)

Tried to create a machine account – Error says it already exists, but can't see it in Users and Computers

Troubleshooting AD Replication

Golden Rule
Top 10 Things that Break Replication
Quick Checks
Tools
Common Problems
Problem Solving Exercises

Golden Rule of Replication Troubleshooting

Always Assume that…

No two domain controllers ever have the same AD information at the same point in time

Top 10 Things That Break Replication

10. Failure by System Architect to Design the topology properly
    - This isn’t rocket science!

9. Failure by Administrator to understand Replication

8. Failure by Administrator to monitor AD

7. DNS problems
   - Duplicate connection objects
   - Bad Cname record
   - SRV Records not registered

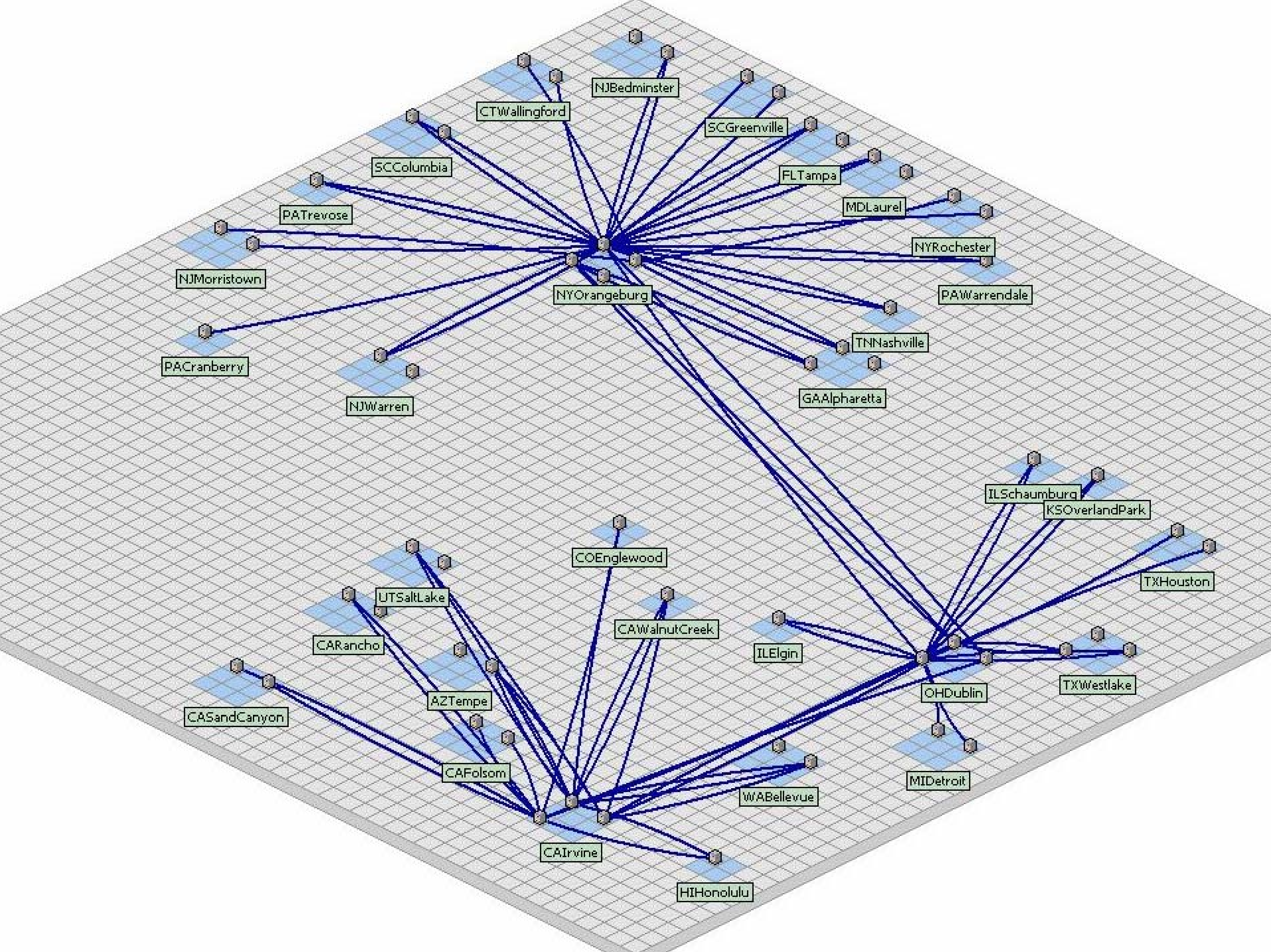
6. KCC doesn’t clean up (by design in Windows 2000)

Top 10 Things That Break Replication

5. Orphaned objects, Lingering Objects
4. Poorly routed, IP address changes
3. Messing with schedules, costs, etc.
2. Physical connectivity fails
1. Topology misconfigured
   - Poor design & implementation (see #9,10)
   - Failure to reconfigure DefaultIPSiteLink

Quick Checks

- Who isn’t replicating with who?
- MPS Reports (DS)
  - Repadmin
    - /Showreps (Win2K)
    - /replsum bydest bysrc /sort:delta
  - Event Logs
- Map out topology (HP OpenView)


NJBedminster
CTWallingford
SCGreenville
SCColumbia
FLTampa
PATrevose
MDLaurel
NYRochester
NJMorristown
NYOrangeburg
PAWarrendale
TNNashville
PACranberry
NJWarren
GAAlpharetta
ILSchaumburg
KSOverlandPark
COEnglewood
TXHouston
UTSaltLake
CAWalnutCreek
CARancho
ILElgin
TXWestlake
OHDublin
AZTempe
CASandCanyon
CAFolsom
MIDetroit
WABellevue
CAIrvine
HIHonolulu

Quick Checks

- Force Replication (snap-in)
  - Returns different error
- Create user, site on broken DC
  - See if Inbound/outbound replication working
- ReplMon – Status Report
  - Not included in MPS Reports

Check Cname DNS Records

- In root _msdcs zone (only), alias record mapping DC's FQDN to its server GUID.
  - Only one record per server.
    - Delete duplicates.
  - Match GUID in alias record to GUID reported by Repadmin /showreps.
  - If in doubt, delete DC's Alias record(s) and re-start netlogon on broken DC to re-register .
  - Ping <guid>._msdcs.domain.com

Common Replication Problems

- Event 1311
  - Physical
    - GC or DC can’t be contacted (see event 1722)
    - Network Failure
    - Improper routing
    - Changes in routing, addressing, etc.
  - Logical
    - Sites w/o site links
    - Site Link Bridges covering dial up networks
    - Site Links not Interconnected
      - Site link A-B and C-D (no common site)
    - Preferred BHS offline

Common Replication Problems

- Logical (cont'd)
  - BHS swamped
    - Undersized
    - Too many satellite sites to single BHS (fixed in W2k3)
    - Site Link Schedule
  - DNS Lookup Failure
  - KCC didn't clean up properly (Windows 2000)
- 1311 Repair
  - Look at the topology (HP OpenView)
    - Review the design and implementation
    - Poor design = lots of 1311s!
  - Are 1311's forest wide, domain wide, or site specific?
    - Repadmin /istg

Common Replication Problems

- Logical (cont'd)
  - BHS swamped
    - Undersized
    - Too many satellite sites to single BHS (fixed in W2k3)
    - Site Link Schedule
  - DNS Lookup Failure
  - KCC didn't clean up properly (Windows 2000)

- 1311 Repair
  - Look at the topology (HP OpenView)
    - Review the design and implementation
    - Poor design = lots of 1311s!
  - Are 1311's forest wide, domain wide, or site specific?
    - Repadmin (see Repadmin slide)

Common Replication Problems

- 1311 Repair
  - Look at the topology (HP OpenView)
    - Review the design and implementation
    - Poor design = lots of 1311s!
  - SLB only in fully routed networks
  - Preferred BHS: Just say NO! (or upgrade to w2k3)

Common Replication Problems

- 1772 – RPC Server is unavailable.
    - Physical connectivity.
    - DNS.
- DefaultIPSiteLink
    - Failure to treat this as a normal site link after topology is implemented
        - All Sites in here + in other Links (forgot)
        - Treat it as any other link
        - Rename, don’t delete… just in case
    - Causes Replication to break, poor performance
    - Test later… ☺
- Time Skew (must be within 5 minutes
    - W32tm –sync (Windows 2000)

      /config /syncfromflags:DOMHIER (Windows 2003)

“Lingering Object” Problem

- The problem
  - Replication broken or DC/GC offline >tombstonelifetime (TSL)
  - Loose behavior (Windows 2000 pre-sp3)
    - Allows old object to be propagated back to the AD
    - Security Problem (possibly)
    - Kills replication – chokes on orphaned objects
    - GC: propagates read-only objects (can’t delete)

“Lingering Object” Fix

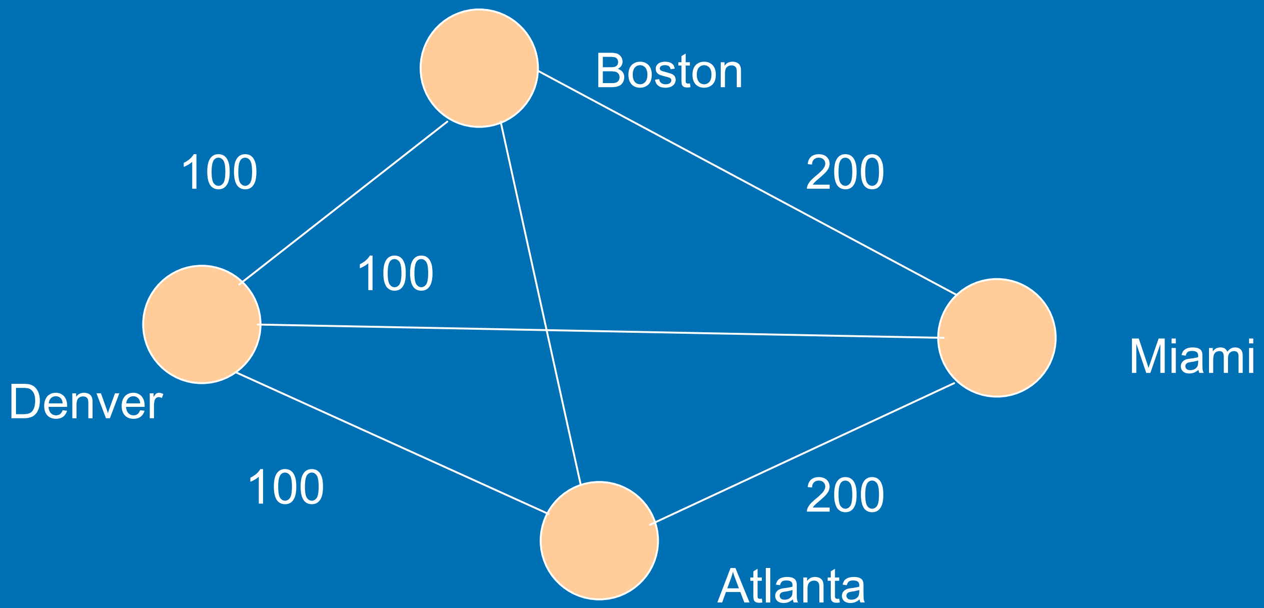
- The Fix:
  - Tight behavior (default in Windows Server 2003 clean install)
  - Stops replication until the object is deleted.
  - Q317097
- Cleanup:
  - Repadmin /removelingeringobjects
    - See Repadmin /experthelp

If all else fails, try demoting…

- Normal or Manual Demotion of a DC then repromote to clean up problems
  - Microsoft loves this!
  - Only if problem is isolated to one DC.
  - If replication isn’t working, demotion won’t work.
  - Can manually demote a DC in Win2K SP3 and Windows 2003.
    - **DCPromo /forceremoval** Then clean up the AD
    - **KB 332199**

Replication Problem Diagnosis (Class exercise)

- Problem 1: Takes twice as long to replicate from Denver to Atlanta as from Denver to Miami. Network bandwidth not an issue.



DCPromo Troubleshooting

Basics
Quick Checks
Tools
Common Problems
Problem Solving Exercises

DCPromo Basics

- 1st DC in Forest doesn’t need DNS
  - DNS failure will show up with #2 DC
  - DNS “_” zones must exist
- DCPromo will configure DNS
  - First DC in Forest
  - W2k: NO! W2k3: Yes!
- W2K33 – Nice DNS check
- DCPromo isn’t successful until SYSVOL and Netlogon shares are created
  - No Sysvol share = Replication failure

DCPromo Basics

- Able to contact a functional existing DC.
  - DNS must be working
  - Dcpromo /replicationsourceDC=
  - NLTest /test:DCPromo (tests DNS)
- Creates/moves Machine acct (DC1$)
- UserAccountControl Attribute set
  - 4096 (1000 hex) = Workstation/Server
  - 532480 (82000 hex) = DC

Quick Checks

- DNS Set up properly?
  - TCP/IP properties set to correct DNS
  - "_" zones exist
- Proper Credentials?
- Is the DC a DC?
  - Inbound/Outbound Replication
  - SYSVOL and NetLogon shares
    - If no, then no Outbound Replication
  - UserAccountControl = 532480 (82000 hex)

DCPromo tools

- %windir%\debug
  - DCpromo.log (appended)
  - DCpromoui.log (renamed)
- Set verbosity on dcpromoui.log
- Netdiag /v
- DCDiag /v
- Directory Service Event Log

Common Problems

- Missing Sysvol and NetLogon shares
- KB 257338 good but…
  - Create Manual connection object
    - Force Replication
    - Works well for any connection failure
  - Force KCC to “Check Replication Topology”
- Repadmin /add and /sync
  - Adds a low level link and syncs across it
  - Works very reliably

Common Problems

- Errors accessing the machine account (DC1$)
  - Q250804
  - If server is in a workgroup, join the domain, then DCpromo (cuts the troubleshooting in half)
    - Account is moved.
  - Error: DC1$ not found, access denied, etc.
    - Credentials of account running Dcpromo
    - Source must have security policy applied to itself.
    - Q250874
    - Dcdiag /test:MachineAccount
/test:FixMachineAccount
/test:RecreateMachineAccount

Poor WAN Performance

- Install From Media (W2k3)
  - Source Replica AD from Media in DCPromo
  - GCs or DCs (Replica only).
  - No initial replication from a DC.
  - After initial load, replicates changes.
  - Unattended Answer File Support:
    - ReplicateFromMedia
    - ReplicationSourcePath
- Media useful life < 60 days (or TSL)

DCPromo Problem Diagnosis (Class Exercise)

- Attempting to promote 1st DC in a remote site – fails with specified domain does not exist or cannot be contacted
  - RPC Server Unavailable

Group Policy Troubleshooting

Basics
Quick Checks
Tools
Common Problems
Problem Solving Exercises
Resources

Quick Checks

- Policy isn’t getting applied
  - Computer, user in domain or OU policy is defined for?
  - ICMP disabled or blocked in the network
  - Filtered, Overridden, Blocked, disabled?
  - Not refreshed yet?
    - GPUpdate (replaces secedit /refreshpolicy)
  - FRS or Replication Problem
    - Look for event 1704

New! Gpresult.exe

- Use the XP/2003 version
  - Run on XP client in the domain
  - Built-in
  - Gpresult /V (verbose)
- Returns:
  - Filtered GPOs (and reason)
  - Security Details
    - Account policies
    - User Rights
- Remember
  - Policy is cached – reboot / login to clear
  - Note who authenticating server is
    - Environmental Variable “logon server”

New! GPMC

- Group Policy Management Console
  - Free Download
- Manage all Policies in domain
  - See all options: No Override, blocking, etc
  - Applied GPOs / Denied GPOs (and why)
- Save GPO settings, User Applied Settings
- Modeling (“what if scenario”)

Common Problem

- Need to restore Default Domain, Default Domain controllers policies
- Best Practice – Don’t mess with these 2 policies
- If you do…
- DCGPOFix
  - Replaces Default Domain Policy
  - Replaces Default Domain Controllers Policy
  - One or both
  - Wipes out old settings like EFS –

Security Problem Diagnosis (Class exercise)

Problem: Set Password Length to 6, History to 24. However, when user changes password, it forces length of 8 and History of 5.

- 4 sites, 30 DCs - Affects all users and admins
- Checked all GPOs – none have 8/5 set
- Noticed 2 default domain policies
- 16 GPOs at domain level
- Default Domain policy lowest priority
- Users OU, Computers OU

Group Policy Resources

All Group Policy Resources: http://www.microsoft.com/gp
Server 2003 Group Policy Infrastructure

http://www.microsoft.com/downloads/details.aspx?FamilyId=D26E88BC-D445-4E8F-AA4E-B9C27061F7CA&displaylang=en

Troubleshooting Group Policy:
http://www.microsoft.com/downloads/details.aspx?FamilyId=B24BF2D5-0D7A-4FC5-A14D-E91D211C21B2&displaylang=en

Administering Group Policy with GPMC:
http://www.microsoft.com/windowsserver2003/gpmc/gpmcwp.mspx

Questions?

Gary L. Olsen
Consultant
Global Services Engineering
Hewlett -Packard
Gary.olsen@HP.com