



POWER IS NOTHING WITHOUT CONTROL

Microsoft

**TechNet & MSDN
Roadshow**



Active Directory Group Policy – Winning Tips and Tricks

Yousuf Bismilla

Technology Solutions Professional



Basic Agenda

- Planning / Building / Testing / Deploying
- Specific Group Policy “Features”
- Troubleshooting



Common GPO misunderstandings

- By default, how often does Group Policy initiate a refresh after a user has logged on?
 - Every 90 mins plus a random delay of up to 30 minutes (not plus or minus 30 mins)
- When policy applies, The version number between the AD and Sysvol parts of the GPO need to match in order for GPO to apply.
 - It depends! This changed between Windows 2000 and Windows XP / Windows Server 2003. With Windows XP and Windows Server 2003 it no longer matters that the AD and SYSVOL version numbers match. GP will still apply.



Planning OU Design

- Create separate OUs for computers and users
- Segment machines/users into roles by OU; Examples
 - Servers: Exchange Servers, Terminal Servers, Web Servers, File and Print, etc
 - Workstations: Desktops; Laptops, task stations etc.
 - Domain Controllers: Leave in Domain Controllers OU (with Default Domain Controllers Policy GPO linked)
 - Users: IT Staff, Engineers, Shop Floor, Laptop Users, etc.
 - By default, all new accounts are created in cn=Users or cn=Computers (cannot link these to GPO's). However, if you have a Windows Server 2003 domain
 - Run "RedirUsr.exe" and "RedirCmp.exe" in your domain to specify the new default OU's in which all new user / computer accounts will be created
 - Allows you to manage new accounts through Group Policy when you don't specify an OU at account creation1
- Limit who can create / update / link GPOs (delegation)



Planning

GPO Design

- “Normalize” GPOs – review for common settings; See Group Policy Common Scenarios ² for examples
- GPO naming conventions – make it consistent and easy to interpret
 - Simply use a clear name to describe intent of the GPO
 - One approach Microsoft uses internally. 3 token string – scope (end user, worldwide, IT), purpose and who manages. Example: “WW-Outlook-OTG”
 - How significant is the number of GPOs applied?
 - Myth
 - Performance is significantly improved with fewer GPOs applied to each computer or user
 - Facts
 - GPO contents are far more important in relation to performance than the number of GPOs (check out the “FindGPOsByPolicyExtension” script)
 - 999 is the maximum number of GPOs applied (after scoping) to a computer or user – but if you have that many you have bigger problems anyway!



Planning

GPO Design

- Avoid cross-domain GPO links – GPMC scripts help deploy and maintain consistent GPOs across domains
- Use Enforce/Block Inheritance, Loopback Sparingly
- Use WMI Filters (XP and WS 2003 only) where the “lifetime” of the filter is well defined; For example...
 - Microsoft OTG team needed to implement IPsec but only on machines with adequate NIC support
 - Created a GPO and linked a single WMI Filter (the WMI Filter checked for right NIC card support)
 - Able to implement immediately rather than wait for all machines to have right NIC card support
 - WMI Filter removed once IPsec project complete
- Keep in mind, Windows 2000 doesn't evaluate WMI filter – GPO will be applied
- Keep It Simple; Don't over-engineer!



Planning: Deployment Test, Stage, And Production

- It's a "good thing" if you: Test -> Stage -> Test -> Deploy -> Validate
- For significant functional changes, consider a pilot.
 - Don't limit the pilot to just IT Staff – they often know how to workaround/resolve issues!
 - Some GPMC features are specifically focused on testing/staging/piloting/deploying GPOs³
 - Group Policy Modeling (more elegant face on RSoP Planning)
 - Backup/Copy/Import (including migration tables)
 - Specific "sample" scripts - particularly CreateXMLFromEnvironment and CreateEnvironmentFromXML (optionally include users and groups)
 - Documentation: HTML or XML Reports



Planning

Disaster Recovery

- GPMC Backup / Restore handles GPO as a logical entity – AD and Sysvol
- Automate GPO backup using GPMC scripts - BackupAllGPOs or BackupGPO
- If you care, secure your backup location; If you don't care, why?
(consider the impact of a GPO linked to the domain)
- Regularly test GPO restore in your environment – RestoreAllGPOs or RestoreGPO
 - Think about building/rebuilding your staging environment



Planning

Disaster Recovery

- Be aware of what is NOT included in a backup of a GPO and plan accordingly
 - IPsec Settings, which live in CN=IP Security, CN=System,DC=xxxx (AD backup handles this); The GPO includes just the link to this data
 - WMI Filter (only the filter link is backed up); The filter itself is stored in AD so your AD backup covers this
 - GPO links from sites, domains or OUs, since they are not an attribute of the GPO (again, AD backup covers this)
 - Don't rely on DCGPOFix (last resort tool!) DCGPOFix returns default GPOs to the clean install state (not an upgrade) and they are unlinked; Use your own backup instead



Planning

Group Policy Dependencies

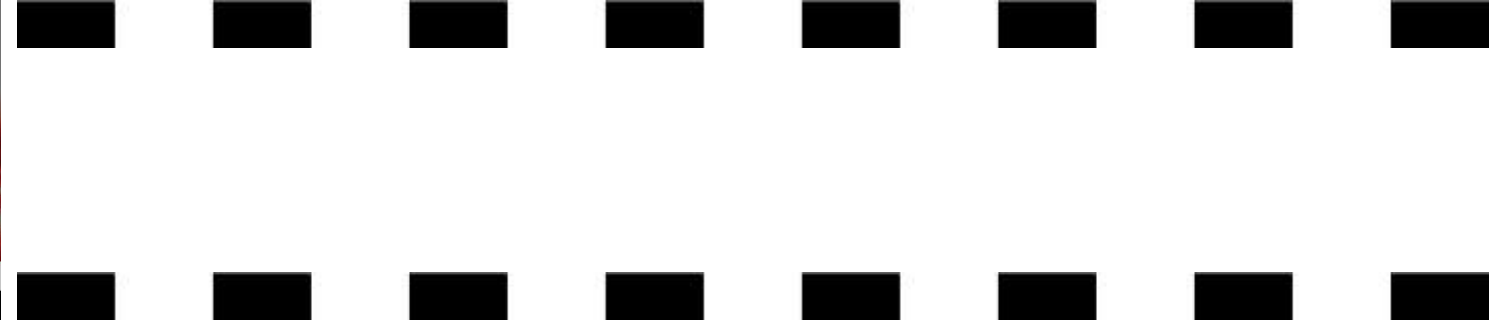
- DNS: Many “Group Policy problems” turn out to be related to DNS misconfiguration ⁴
- File Replication Service (FRS) ⁵ in multi-DC environment
 - Use Sonar for quick feedback on an unmonitored FRS system
 - Use Ultrasound for monitoring and alerts (requires supporting infrastructure such as a DB)
- Don’t touch the Policies directory in Sysvol (including playing with ACLs) – manage through supported tools only; If you plan to delete Sysvol – well, don’t!



Planning

Group Policy Dependencies

- ICMP, at network routers or in TCP/IP configuration (clients or DCs)
 - Used to validate connectivity to a DC and for slow link detection (uses Ping)
 - Policy not applied if client cannot reach DC
 - If you absolutely must disable ICMP, disable slow link detection; But then a “fast link” is assumed – consider impact on software installation and folder redirection
- With no connectivity to a DC at logon (i.e. a remote machine) policy will not process, unless you check the “Logon using dial-up connection” check box at the logon prompt
 - Will force update of user and machine policy



● DEMO



Windows 2000 Domains

Fixing Mismatched ACL's

- In a Windows 2000 domain created prior to SP4, GPO ACLs in AD and Sysvol are slightly mismatched
- Mismatch relates to the permission inheritance flag in an Access Control Entry (ACE)
- Mismatch exists on both the Default Domain Policy and the Default Domain Controllers Policy GPO's
- GPMC will prompt you to clean up when you touch the GPO; Do this!



Domain Upgrades

Upgrading To Windows Server 2003

- W2K domain to WS 2003 upgrade can potentially cause significant FRS replication traffic
 - Cross-domain Group Policy Modeling requires ACE on GPO's (read access for Enterprise Domain Controllers)
 - ACE is OK for new GPO's created in WS 2003 domain – problem exists for GPO's existing before an upgrade from a W2K domain
 - ADPrep /DomainPrep adds the ACE to all existing GPO's
 - ...and results in FRS replicating all modified GPO's through the domain; Can be a problem with large Sysvol and/or slow links
- To actively manage this replication use either GrantPermissionOnGPO (one GPO at a time) or GrantPermissionsOnAllGPO's; Allows you to decouple fixing the ACLs from the domain upgrade
- So, what are we doing?...
 - WS 2003 SP1 will NOT update the GPO's by default (a /GPPrep switch is added to ADPrep to allow the admin to force ACL update)



Group Policy “Features”

- Administrative Templates
- Security
- Machine and User Scripts
- Folder Redirection
- Resultant Set of Policy (RSOP)
- GPMC Scripting



Features

Administrative Templates

- What is an .adm file (UI vs registry.pol)
- "Recommendations for Managing Group Policy Administrative Template Files" (KB 816662)⁸
 - Operating System/Service Pack Releases
 - "Sysvol Bloat"
 - Multi-language Scenarios
 - Policy Settings To Manage .adm Files (read from Sysvol/write to Sysvol)
- From WS 2003 .adm releases are always a superset of previously released .adm files (i.e XP SP2 will include all policies in Windows Server 2003 plus new policy settings)
- Identify differences in .adm files using Admx.exe (Resource Kit Utility)
- All historical .adm files to be available online (one package for each OS/SP plus another for all OS/SPs)
- **Never** edit OS-shipped .adm files (system, inetres, wuau, wmplayer, conf)
- Note: <http://support.microsoft.com/default.aspx?kbid=842933>
"The following entry in the [strings] section is too long and has been truncated" error message when you try to modify or to view GPO's in Windows Server 2003, Windows XP Professional, or Windows 2000



Features

Security Settings

- Why don't we just set the highest security settings and be done? Because stuff breaks!
- In XP SP2 and WS 2003 SP1: "Dangerous" settings warnings
 - Example: "Allow Log On Locally"
 - Security extension (in GPEdit) adds a dialog box warning, pop-up confirmation and a link to relevant KB article⁹
- Domain Level Policies¹⁰
 - Account Policies
 - Rename or Disable Admin/Guest Account
 - Kerberos
- From W2K SP4 and XP SP2, you can add a domain group to a local group on a computer (uses Member of)¹¹.
 - Note: This should not be confused with Restricted Groups. Group membership is cumulative across multiple GPO's, Rrestricted Groups are not.



Features

Security Settings

- Avoid modifying the Default Domain and Default Domain Controllers GPO's; Except...
 - Some apps may expect settings to be set in the Default Domain/Domain Controllers GPOs
- User Rights and Password Policy With Applications installed on DC's
 - Application may update Password or User Rights policy
 - Security detects this and updates Default Domain Controller GPO (replicated to all DC's)
- Keep Domain Controllers Consistent
 - Keep DCs in the Domain Controllers OU
 - Do not use security filtering to filter policy settings on GPO's linked to DCs



Features

Machine/User Scripts

- Async logon/Logoff scripts finish in a non-deterministic order; Don't rely on one script completing before another
- Startup scripts run in the security context of the computer (requires access to script and referenced resources)
- Computer needs access to scripts and referenced resources over network at boot time
 - If script uses only local machine resources then you can copy scripts to local hard disk and reference accordingly in the GPO (consider use of environment variables such as %windir% for machine differences)
- User scripts need admin or granted rights if updating HKLM
- Two parts to processing scripts in GPOs
 - Processing of the GPO: event source = UserEnv
 - Running of the script: event source = UserInit (this one is more common if events are logged)



Features

Folder Redirection

- Do not pre-create folders (ACL issues)
- If server is Windows 2000, do not redirect folders to same machine used for Roaming User Profiles (fixed in Windows Server 2003)
- Do not redirect Application Data folder (particularly if logged on from multiple computers)
 - Exclusive locks
 - Absolute paths
 - Network latency
- You cannot redirect to a mapped drive (folder redirection occurs before mapping of drives)



Features

RSoP

- No Group Policy Results data available for
 - IPsec, Wireless, and Disk Quota
 - Windows 2000
(but you can simulate using Group Policy Modeling)
- Group Policy Modeling can only simulate the following (does not query target machine)
 - Slow links status
 - WMI filters
 - Loopback
- Also, Modeling doesn't know about the LGPO



Features

GPMC Scripting

- Consider the “sample scripts” as building blocks, as well as samples for GPMC API. Think of them as 32 tools to start you off!
- Comparing intended versus actual policy is not easy today – consider “diff’ing” XML versions of Modeling reports against Results reports (see GPMonitor for diff feature between refreshes)
- Integrate the generation of HTML or XML reports into your documentation system



Features

Miscellaneous ...

- Wireless: Need to be on wired network to get certificates for wireless policy (for 802.1x)
- GPMC: Drag a GPO across domains to an OU or domain and you get a cross-domain link (not a copy of the GPO); Instead, drag to Group Policy Objects node (note: No links will exist at this point)



Troubleshooting

- Know your reporting options
 - Group Policy Modeling (think proactively!)
 - Group Policy Results
 - Event Log (exposed through GPMC)
- Know your tools
 - With Operating System: GPUUpdate
 - WS 2003 Resource Kit: GPOTool, GPMonitor
 - Download Center: GPIInventory
- Know your log files
 - UserEnv (Core Engine), WinLogon (Security), FDeploy (Folder Redirection), Appmgmt.log (software installation), Gpmgmt (GPMC), GPedit (GPEdit), GPText (CSE-specific)
- Consider the methodology described in the Group Policy Troubleshooting Whitepaper ¹²
- Consider the Group Policy Management Pack (GPMP); MOM snap-in to monitor the health of Group Policy on WS 2003 Servers; Available from Microsoft.com
- Also see session ADM396



Troubleshooting

- Using the Local GPO (LGPO)
 - A good option if you don't have access to change GPOs in a domain (not all settings will be available – software installation and folder redirection, for example)
 - Updating the LGPO on a domain-joined PC has no impact when using cached credentials
- Read the Explain Text for Admin Templates and Help for Security Settings
- Remember the /force switch
- If you move a user/computer to a new OU, the change will not take place immediately (GetUserNameEx caches the location of a user/computer for 30 mins); Reboot/Logon to resolve
- Consider using a Virtual PC - especially helpful for tattooing security settings; Undo when done!



What's New In XP SP2?

Full list of new Administrative
Templates Policy Settings at:

<http://go.microsoft.com/fwlink/?linkid=22031&clid=0x409>



What's New In XP SP2?

Windows Firewall

- Domain and Standard Profiles (with and without connectivity to DC)
- Much more granularity
 - Turn firewall on/off
 - Open specific ports
 - Define list of allowed (listening) apps
 - Remote administration exception
 - File and print sharing exception
 - UPnP framework exception
 - Prohibit notifications
 - Allow Logging
 - Prohibit unicast response
 - Allow local port/program exceptions - merging policy with preferences
- Use these policy settings with caution – defaults are there for a reason!!!



Microsoft[®]

© 2004 Microsoft Corporation. All rights reserved. This presentation is for informational purposes only.
MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY.

Microsoft[®]