Global Information Assurance Certification Paper

Management Challenges of Windows 2000 Group Policy
Mark Sanders
December 13, 2001

Introduction

Group Policy is the primary tool for change and configuration management (CCM) in Windows 2000. It carries out its functionality through the use of Group Policy Objects (GPOs). GPOs leverage Windows 2000 Active Directory (AD) to allow administrators to control the behavior of their servers and workstations. Group Policy Objects can contain hundreds of settings ranging from user rights to system services, and can be applied in a hierarchical fashion to Organization Units (OUs) in AD.

Although these very granular policies can be easily created, the tools provided by Microsoft to maintain and troubleshoot Group Policies are less than adequate. There are however third party tools available, such as FAZAM 2000, which help with some of the features which are native GPO tools are lacking.

Native Group Policy Management Tools

Windows 2000 provides the following native tools for managing and troubleshooting the application of GPOs in an enterprise.

GPResult

This group policy results tool displays the policies that have been applied to the computer on which the command was run on, as well as the policies that have been applied to the user that is currently logged on. The /c and /u switches can be used to display the basic computer or user policies, while the /v and /s switches expand the level of detail of the policy results.

According to Microsoft's website, http://www.microsoft.com/windows2000/techinfo/reskit/tools/existing/gpresult-o.asp, the basic level of group policy results include the following:

- Operating System
- Type (Professional, Server, Domain Controller)
- Build number and Service Pack details.
- Whether Terminal Services is installed and, if so, the mode it is using.
- User Information
- User name and location in Active Directory (if applicable).
- Domain name and type (Windows 2000 or Windows NT).
- Site name.
- Whether the user has a local or roaming profile and location of the profile.
- Security group membership.
- Security privileges.
- Computer Information.

- Computer name and location in Active Directory (if applicable).
- Domain name and type (Windows 2000 or Windows NT).
- Site name.

In addition, the expanded group policy results include the following:

- The last time policy was applied and the domain controller that applied policy, for the user and computer.
- The complete list of applied Group Policy Objects and their details, including a summary of the extensions that each Group Policy Object contains.
- Registry settings that were applied and their details.
- Folders that are re-directed and their details.
- Software management information detailing assigned and published applications.
- Disk quota information.
- IP Security settings.
- Scripts.

GPOTool

This group policy verification tool is used to test the status of GPOs on domain controllers (DCs). Running the tool without switches displays a list of the Group Policy Objects by their globally unique identifiers (GUIDs) and the status of each. The /verbose switch displays the friendly name of the GPO, its created and modified dates, version IDs, and machine and user Group Policy Extension GUIDs. Gpotool.exe is especially useful for verifying properties such as replication of Group Policy Objects between domain controllers, because it reads the GPO instances from each DC in the domain and runs a recursive comparison of the content. It can be used to display information such as functionality version and extension GUIDs, as well as search GPOs based on friendly name or GUID.

Security Configuration and Management Snap-in

From Microsoft's website, http://www.microsoft.com/ntserver/techresources/security/SecurConfigToolSet.asp, the Security Configuration and Analysis snap-in provides administrators with a single graphical utility that can be used to configure and analyze virtually every aspect of a system that relates to security.

The snap-in can first be used to analyze a local system against a pre-defined security template. The results of this analysis are stored in a security configuration database. Once this is done, the database can be opened and viewed to see the differences in the policy defined in the template and the policies applied to the system.

This analysis can be used to verify that the settings in the policy are actually being applied to the local system. This will not always be the case, especially if there are a hierarchy of GPOs being pushed down by Active Directory to the local system, since generally the last setting applied wins out. For this reason, it is important to be able to determine a Resultant Set of Polices of a particular system, rather than just the comparison of one template to the effective policy settings.

Issues with Native Management Tools

The tools provide with Windows 2000 provide some management and troubleshooting features, but there are also several important features that seem to have been left out.

Documentation of GPO Settings

Each Group Policy Object has over 680 computer and user settings, including:

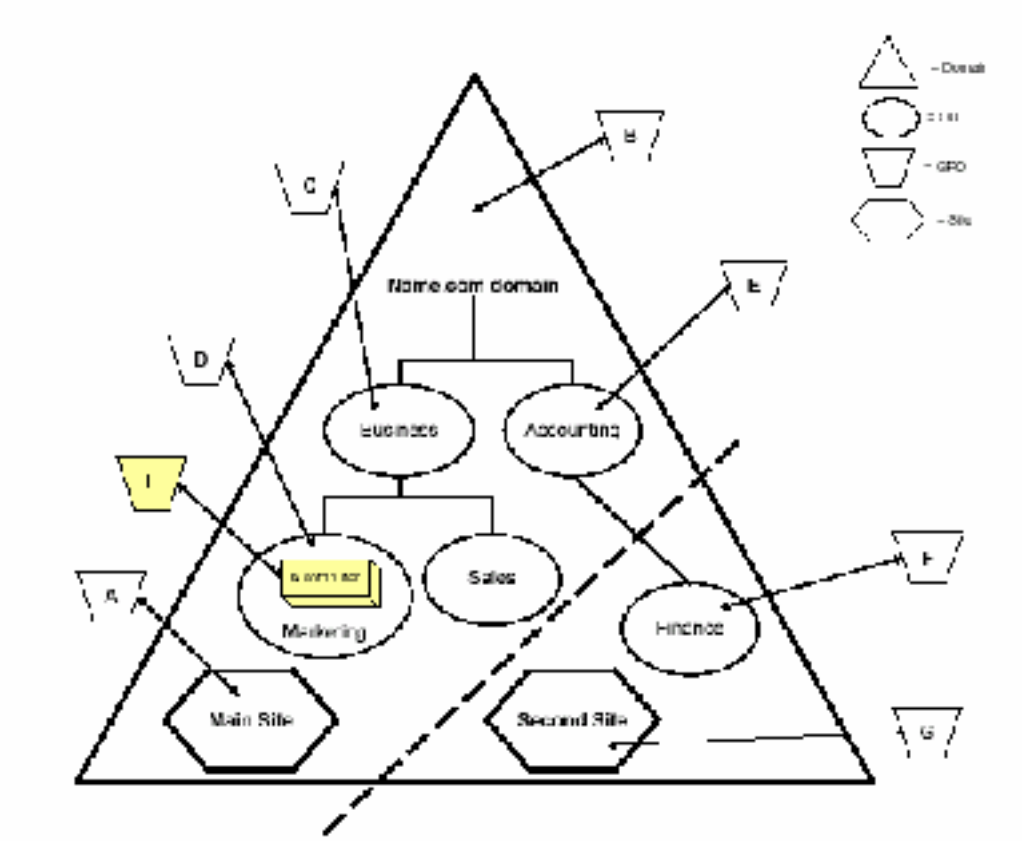
- Account Policies
- Local Policies
- Event Log Policies
- Restricted Groups
- System Services
- Registry Permissions
- File System Permissions

Although it is fairly easy to view the settings of a GPO with native Windows 2000 tools, there is no simple way to export them into a report. The only mechanism for doing this is by saving each subsection of the policy off individually with the Security Configuration and Management Snap-in pasting them together in a text document or spreadsheet. Not only is this a very tedious process when dealing with numerous GPOs, the process only works for the standard policy settings and not for Registry or File System permissions. Therefore, it is impossible with the native tools to easily and accurately track the settings contained within each GPO.

Resultant Set of Policies (RSOP)

As stated from Full Armor's website, http://www.fullarmor.com/pdf/EliminatingGPMgmtChallenges_v11_010119.pdf, Group Policies are a collection of numerous computer and user settings. They can be applied alone or in combination at several different levels within an organization: across an entire domain, to individual organization units (OUs) within the domain, or even to specific portions of the physical network (known as sites). Since policy objects can have their own access control lists (ACLs), it is possible to assign policy to specific groups in the organization.

A resultant set of policies (RSoP) is the effective policies which a specific user at a specific machine will receive. Since policies can be applied at many different levels of OUs in Active Directory, it is very important to know exactly which policy settings may be overwritten by other GPOs. This is based on the LSDOU (Local, Site, Domain, OU) hierarchy of policy evaluations used by Windows 2000. The figure below, taken from the Full Armor website, illustrates the hierarchical nature of Group Polices in Active Directory.



Based on this figure and the formula Local + Site + Domain + OUs, a user in the Marketing OU would receive a RSoP of L + A + B + (C+D), while a user's in the Finance OU would be (none) + G + B + (E+F).

While the Security Configuration and Management Snap-in can compare one policy to that of the effective policies on a system, it cannot determine the RSoP on an OU. For both planning and troubleshooting GPO issues, a quick way to view or analyze RSoPs is an operational necessity.

GPO Management

Although GPResult and GPOTool provide ways to view policy attributes of a local system, neither will work to determine the state of GPOs on a remote system. In an enterprise environment, it is essential to be able to monitor and troubleshoot Group Policy issues remotely.

With over 680 settings, Group Policy Objects could potentially take months to develop, and the ability to backup and restore Group Policy Objects is an essential feature. This can also be helpful while migrating GPOs from a test domain to a production domain. However, Windows 2000 only allows for backing up and restoring of the entire Active Directory.

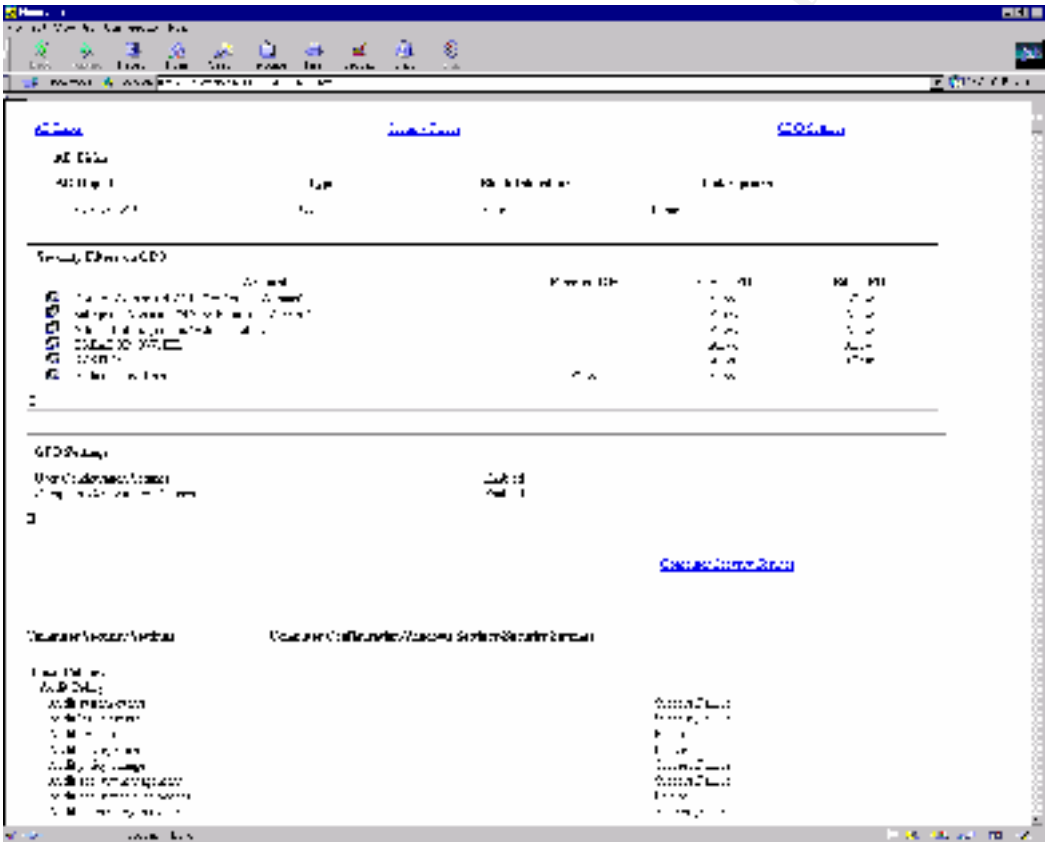
FAZAM 2000

Third party products are available to enhance the native Windows 2000 group policy tools. One in particular, which is actually endorsed by Microsoft, is Full Armor's FAZAM 2000 (Full Armor Zero Administration). Their product was designed to complement and extend Microsoft's native policy management tools to cover the previously mentioned issues.

Documentation of GPO Settings

FAZAM 2000 provides extensive reporting capability of GPO settings. Each setting of a Group Policy Object that has been set is displayed on the FAZAM report, including settings made in the Administrative Templates, Registry, and File System subsections. They contain descriptive information about policy settings that have been enabled or disabled and the actual registry key names and their values, respectively. The reports can also be easily exported to a MS Access database, where settings can be queried or compared, or as an HTML file.

The following figure is an example of a GPO report exported as an HTML file:



Resultant Set of Policies (RSOP)

FAZAM allows for the use of RSoP. This becomes essential for administrators to carry out policy enforcement and management tasks. From a planning perspective, FAZAM provides a way for previewing the result of a set of Group Policies to a user or computer before they are actually applied in Active Directory. Natively, the policies must first be applied to AD before

the effective settings can be verified. This inability to plan the application of multiple policies before they are added to AD would likely result in additional time and effort required to fix the problems afterwards.

From a troubleshooting perspective, the RSoP is an effective tool for help desk use as well. This would allow for the help desk personnel to determine exactly what policies have been applied to a particular system that may be causing problems due to conflicting GPO settings.

GPO Management

As stated from Full Armor's website , http://www.fullarmor.com/pdf/Man_Enterprise_Pol_FAZAM2000.pdf , FAZAM 2000 Remote Diagnostics feature provides the ability to connect and carry out diagnostics on a remote machine. On connecting to the remote machine, the FAZAM diagnostics console interacts with a client agent to provide information on GPOs that were downloaded and applied on that machine by virtue of machine and user policies. The Remote Diagnostics feature displays the GPO information for not only the current user logged on to the machine, but for all user accounts that have logged on from that machine as well.

FAZAM also offers backup and restore functions for GPOs. These functions include backing up and restoring the following:

- GPO settings
- Links to AD objects
- Security information

Conclusion

Although the native Windows 2000s Group Policy tools offer some great features to manage Group Policy Objects, there are many limitations with the native tools used for administering the GPOs. These limitations mainly consist of GPO management features, reporting features, and ability to provide a resultant set of policies. Therefore, though the use of some Windows 2000 third party tools, such as FAZAM 2000, administrators can be better equipped to manage Group Policy in their enterprise.

Realizing this, Microsoft is now incorporating a reduced-functionality version of FAZAM 2000 on the Windows 2000 Resource Kit, and has plans to incorporate the full version in future releases of Windows.

References

'Gpresult.exe: Group Policy Results' Microsoft website
http://www.microsoft.com/windows2000/techinfo/reskit/tools/existing/gpresult-o.asp

'Gpotool.exe: Group Policy Verification Tool' Microsoft website
http://www.microsoft.com/windows2000/techinfo/reskit/tools/existing/gpotool-o.asp

'Understanding Microsoft Security Configuration Tool Set' Microsoft website
http://www.microsoft.com/ntserver/techresources/security/SecurConfigToolSet.asp

'FAZAM 2000, Reduced-Functionality Version' Microsoft website
http://www.microsoft.com/WINDOWS2000/techinfo/reskit/tools/existing/fazam2000-o.asp

'Group Policy and Security' Windows 2000 Magazine website
http://www.win2000mag.com/Articles/Index.cfm?ArticleID=9169

'Eliminating Management Challenges" Full Armor website
http://www.fullarmor.com/pdf/EliminatingGPMgmtChallenges_v11_010119.pdf

'Designing Group Policy' Full Armor website
http://www.fullarmor.com/pdf/DesigningGroupPolicyWP.pdf

'Managing Group Policy' Full Armor website
http://www.fullarmor.com/pdf/Man_Enterprise_Pol_FAZAM2000.pdf

Jennings, Roger "Admin 911 Windows 2000 Group Policy" Berkely, CA. McGraw-Hill, 2001

Last Updated: September 20th, 2017

Upcoming Training

Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS New York SEC401*	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Oct 03, 2017 - Nov 14, 2017	Mentor
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VA	Oct 14, 2017 - Oct 21, 2017	Live Event
SANS Tokyo Autumn 2017	Tokyo, Japan	Oct 16, 2017 - Oct 28, 2017	Live Event
CCB Private SEC401 Oct 17	Brussels, Belgium	Oct 16, 2017 - Oct 21, 2017	
Community SANS Omaha SEC401	Omaha, NE	Oct 23, 2017 - Oct 28, 2017	Community SANS
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201710,	Oct 23, 2017 - Nov 29, 2017	vLive
San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
Community SANS Vancouver SEC401*	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
Community SANS Colorado Springs SEC401**	Colorado Springs, CO	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Dec 04, 2017 - Dec 09, 2017	Community SANS