Global Information Assurance Certification Paper

Challenges Associated with Windows 2000 Group Policy Object (GPO) Management

SANS Security Essentials GSEC Practical Assignment

Version 1.4b – Option 2

Author: Henry Kiiskinen
ID: henryki001
Location: SANS Biscayne Bay

Submission Date: June 10, 2004

Table of Contents

1.0 Introduction

I work for a large financial institution. We have over the last two years implemented a Windows 2000 Active Directory within our organization. Several divisions of the company had a business requirement for the implementation of Windows 2000 Active Directory. Each of these divisions of the company expressed a desire to participate in a single forest. One division of the company chose to implement their own forest. The business goals of the Windows 2000 implementation project were:

- Provide the strategic standards necessary to implement Windows 2000 Active Directory services.
- Provide a flexible platform that is cognizant of the diverse business requirements.
- A solution that improves our Total Cost of Ownership (TCO)

Due to the diverse requirements of each division, we realized that we had some significant challenges associated with the implementation and management of Group Policy Objects (GPO). I will focus on the issues we experienced related to the management of GPO's. There is a great deal of emphasis in the Microsoft documentation on how to implement Windows 2000 GPO's but not enough discussion about the pitfalls. I am hoping that our experience with GPO's will clarify some of the not always obvious problems that may be encountered with GPO management.

2.0 Before

Our Windows NT 4.0 environment was not a single Master Domain model. We had multiple domains scattered across hundreds of servers and multiple business units. Most of the domains were supported within each business unit with no communication between domains. Therefore, each division of the company had implemented different standards for Windows NT 4.0 servers. Many trusts between domains were required to provide access to required information. These trusts were created and maintained manually.

The solution to this problem was to implement a Windows 2000 Active Directory environment. We worked closely with Microsoft and IBM to implement a secure solution. IBM was responsible for the support of our NT 4.0 domain infrastructure. Microsoft acted as a consultant in the development of the Windows 2000 Active Directory. My department was the domestic division's security department and my security team would be responsible for the maintenance of the Windows 2000 Active Directory (AD).

It was obvious from the outset that management of Group Policy Objects was a critical component of a secure solution. Microsoft recommended that the planning phase of the development of GPO's be a critical phase of the project. Microsoft warned us that the implementation of the Active Directory had to be executed correctly the first time as it would be difficult to change at some later stage.

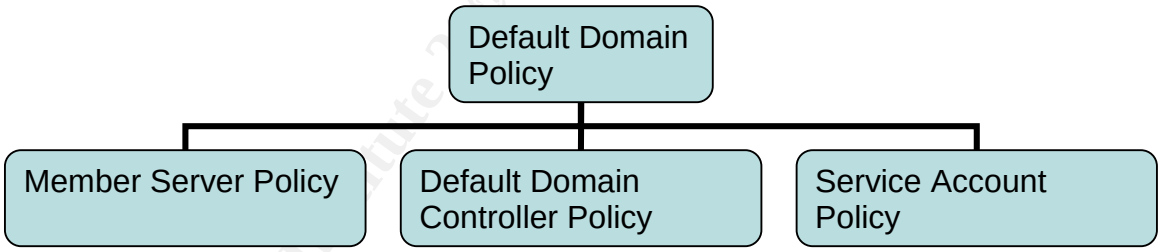
3.0 During

We created a committee consisting of our own security department, our architecture team, IBM and Microsoft to develop a strategy for GPO deployment. This committee was also responsible for the evaluation and definition of settings within GPO's.

One of the first activities of the committee was to design the domain and organizational unit (OU) structure of the Forest. This is necessary in order to be able to design GPO's as they apply to each domain and OU. GPO's can be used to control the access for AD objects such as users, workstations and printers.

3.1 GPO Structure

Group Policies and their settings are complex and very granular. It can be very confusing to determine which policies and settings are required for your environment. We took a staged approach to the implementation of Group Policies and started out with only those policies that we felt were essential. This staged approach allowed us to implement corporate wide policies such as password length and event log sizes from the outset. See the example below.



We only enabled those policies and settings that we defined as essential. We can look at the Default Domain Policy settings:

- Account Policies
- Password Policy
- Account Lockout Policy
- Kerberos Policy
- Local Policies – Applied at the Domain Controller level
- Audit Policy
- User Rights Assignment
- Event Log

- Settings for event logs

It is always possible to enable additional or specific policies and settings at the domain and OU level.

3.2 Default Behavior of GPO Settings

It is critical to understand that if a particular setting is not enabled in a policy, the setting is not necessarily disabled. The default behavior of GPO settings must be considered when you make the decision to use the default value for a particular setting. In order to avoid unexpected results we reviewed every setting and its default behavior for every active policy. This is a difficult and tedious exercise but essential.

For example:

Windows Settings >Security Settings >Local Policies > Security Options

Clear virtual memory pagefile when system shuts down

The default setting is DISABLE[1]. If it is your company's policy to clear the pagefile at shutdown for security reasons then you must enable this setting. This is a simple example of the kind of results that could happen if the default behavior of a setting is not understood.

3.3 Group Policy Management Authorization

Management of group policies is a critical security function. Group policies can be used to ensure that the users and machines on your network remain in a secure configuration after deployment. All Group Policy settings require careful planning and authorization. It is highly recommended that the only individuals authorized to make GPO changes are experienced security officers with a good technical knowledge of Windows 2000 Active Directory. Unless a security officer is aware of the potential impact of a GPO there is a risk of causing disruption to the user community or potential damage to AD objects.

Our company has very strict change control guidelines. The members of our Change Control Review Board include operational departments as well as

---

1 Microsoft. "Microsoft Knowledge Base Article – 320423"

URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;320423**, November 21, 2003**

business line owners. A good change control process eliminates the possibility that a policy is implemented without the knowledge of all areas that might be affected. Our domain and OU level policies must be reviewed, scheduled and authorized by this change control process.

There are additional concerns for Root level Group Policy changes. Root level policy changes affect all domains, sites and OU's. Therefore we have implemented an Active Directory Forest Change Review Committee. This committee is chaired by our Windows Architecture team as they have Active Directory architecture responsibilities across all domains. This committee must be convened for all changes to the Root including hardware upgrades and AD Schema changes as well as GPO changes. This level of authorization is in addition to the normal change control process.

3.4 Group Policy Migration

3.4.1 Migration Environment

The development, UAT and production environments each have their own domain. The domain structure of each of these environments reflects the production domain structure. They are not necessarily identical but close enough that the OU structure can be duplicated. If the OU structure is not duplicated then you risk not understanding how Group Policy settings are inherited through all of the OU's. The risk that this presents is that you could encounter unexpected results when the Group Policy is promoted to production.

3.4.2 Migration tools

Microsoft has developed a new Microsoft Management Console (MMC) snap-in that simplifies the management of Group policies. The Group Policy Management Console (GPMC) allows for:

- A user interface (UI) that makes Group Policy much easier to use.
- Backup/restore of Group Policy objects (GPOs).
- Import/export and copy/paste of GPOs and Windows Management Instrumentation (WMI) filters.
- Simplified management of Group Policy-related security.
- HTML reporting of GPO settings and Resultant Set of Policy (RSoP) data.
- Scripting of policy related tasks that are exposed within this tool (not scripting of settings within a GPO).

A white paper is available from Microsoft discussing the above bullets and the use of GPMC[2].

The most important GPMC feature for us was its ability to migrate GPO's from one domain to another. As I have already explained our development, UAT and production environments all reside in their own domains. There is no simple means of migrating GPO's from one domain to another. GPMC resolves this issue.

By connecting a workstation to one domain and backing up a Group Policy to a central location, it is then possible to migrate the same Group Policy to another domain by connecting that workstation to the new domain and importing the backed up Group Policy. This same process can be repeated for as many domains as required.

3.4.3 Group Policy Creation

In our environment IBM is responsible for the creation of Group Policies based on requirements agreed upon by IBM, the business line owner and our security team. IBM creates the policies in a development environment. IBM creates the Group Policy using the Microsoft Management Console on the development environment. It is very important to understand that the development environment is managed by IBM. IBM uses this environment to develop and test changes to group policies and how they will affect applications. The development environment is a near copy of the User Acceptance Testing (UAT) environment. There are some differences due to limited budget for hardware, network and software licensing.

3.4.4 User Acceptance Testing

When IBM has successfully tested the Group Policy in the development environment it can then be migrated to the UAT environment. All change control requirements, as stated above (3.3 Group Policy Management Authorization), must be satisfied before a Group Policy can be migrated to UAT.

The Windows 2000 security team is responsible for migration of the Group Policies from the development environment to UAT. The security team ensures

2 Microsoft. "Administering Group Policy with the GPMC,,

URL: http://www.microsoft.com/windowsserver2003/gpmc/gpmcwp.mspx, December 11, 2002

that the following precautions are taken prior to implementation of the Group Policy into the UAT domain.

- The policy satisfies the user requirements. This is a manual check to ensure that the settings are correct.

- No additional settings changes have been made other than what was requested and authorized.

- Take a backup of the policy to be promoted. This backup must be stored in a secure location to ensure that only the authorized security team can make changes to GPO's.

GPMC is then used to migrate the policy from the development domain to the UAT domain. At this point our UAT group is responsible for ensuring that the GPO has no negative effect on existing application functionality. Their sign off of a successful test cycle is required before deployment to production can be initiated.

It is important that the group responsible for defining the GPO requirements perform testing at this time. This group of testers is not necessarily part of the UAT group. Their sign off is required to ensure that the GPO meets all requirements.

3.4.5 Production Implementation

When the UAT group and any other testing groups have signed off on the success of their testing, it can be migrated to the production environment. All change control requirements, as stated above (3.3 Group Policy Management Authorization), must be satisfied before a Group Policy can be migrated to production.

The GPO that was backed up prior to promotion to the UAT environment is the same policy that is migrated to the production environment. This ensures that only authorized changes are promoted to production. The security team is responsible for migration of the GPO to production using GPMC.

3.5 GPO Hazard Avoidance

There are a number of hazards associated with Group Policy Objects. Some of these are documented by Microsoft but many are not documented. I will provide some information on some that we encountered and try to provide solutions where possible.

3.5.1 GPO Optimization

It is critically important to understand that the configuration of Group Policies can have an unacceptable impact on login performance. There are several factors that can contribute. We found that during our pilot testing of one particular domain that the reboot and login times were significantly increased. Microsoft recommended that we look at our GPO configuration with emphasis on the following items.

- Nested GPO's (many layers of GPO's)
- Proliferation of GPO's

We had created a GPO each time we saw a need for a policy. Generally it takes more time to process many small GPO's than a few larger GPO's. In researching this paper I found a Microsoft Knowledge Base Article that discusses some techniques for avoiding this issue[3].

We reviewed all existing GPO's to determine if some of them could be combined into one larger GPO. We have also performed an evaluation of each new GPO requirement to determine whether it could be incorporated into an existing GPO. This helped minimize any impact that the processing of GPO's had on system startup and login times and also simplified GPO management.

An additional benefit of minimizing the number of GPO's was to simplify problem determination when a GPO was suspected of causing a problem. Fewer GPO's simplifies the process of determining the effective GPO's that apply to a given user or computer.

3.5.2 Effective GPO Settings

Organizational Unit design is the most important factor in determining which GPO settings are effective for a particular Active Directory user or computer. Careful OU design can prevent many problems in determining which GPO settings are effective for users and computers.

The default behavior of GPO's is that they are inherited. However there are some factors that can be used to control which GPO settings are applied to a particular local computer, site, domain or OU.

The Block Inheritance option of a Group Policy will prevent Group Policy settings defined in parent containers from being applied to child containers. The Enforced option (formerly No Override) prevents lower level OU's from blocking inheritance. If both of these options are set then the Enforced option takes

[3] **Microsoft. "How To: Optimize Group Policy for Logon Performance in Windows 2000"**
URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;315418&Product=win2000**, September 22, 2003**

precedence. It is recommended that when creating an OU structure, it should be designed to limit the use of blocking inheritance. Blocking inheritance prevents the default application model for Group Policy from taking place. This makes it very difficult to troubleshoot problems associated with group policies[4].

It is possible to scope a Group Policy by using security group filtering. This is an effective method of ensuring that a group of users do not get the Group Policy applied to them that would normally be applied to users in the container. The procedure for accomplishing this can be found at this link[5].

The risk associated with this procedure is that if the security group is moved or added to another group this group can unexpectedly have a different effective Group Policy. This impact can be compounded if there are many layers of security groups and group policies linked to many containers. I would recommend that this feature only be used if absolutely required. If it is required, the potential for risk can be reduced by ensuring that the security group used for filtering has the "Make Member of" rights assignment disabled. This ensures that the group cannot be added to another group.

3.5.3 Tattooing

It is important to understand that not all GPO settings can be removed by removing the Group Policy. Some settings as defined below are persistent. In these situations you must understand the implications of applying a Group Policy. It may be necessary to take a backup of the affected component.

For Windows Server 2003 and Windows XP, security settings might persist even if the setting is no longer defined in the GPO that originally applied it. This occurs under the following conditions:

- The setting was not defined for the local computer at the time that the policy setting was applied.
- The setting is for a registry object.
- The setting is for a file system object.

Windows 2000 security settings may persist even if the setting is no longer defined in the GPO that originally applied it. This occurs under the following conditions:

---

[4] **Komar, B., (2001) Designing Microsoft Windows 2000 Network Security, Microsoft Press**
[5] **Microsoft. "How to: Administer GPO Properties in Windows 2000",**
URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;322176&Product=win2000**, October 30, 2003**

- The setting has not been defined for the local computer at the time that the policy setting was applied.
- The setting is for a registry object.
- The setting is for a file system object.
- The setting is for a service.
- The setting is for a Restricted Groups policy.
- The setting is an Event log setting.

All settings that are applied through local policy or a GPO are stored in a local database on your computer. Whenever a security setting is modified, the computer saves the security setting value to the local database. The database retains a history of all the settings that have been applied to the computer. If a policy defines a security setting and then no longer defines that setting, the setting reverts to the previous value in the database. If a previous value does not exist in the database, the setting remains defined as is. This behavior is sometimes called *tattooing*. Any other settings that persist maintain the values that are applied through the policy until that setting is set to a different value[6].

[6] **Microsoft. "Microsoft Windows Server 2003 Deployment Kit", URL:** http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/deployguide/en-us/Default.asp?url=/resources/documentation/WindowsServ/2003/all/deployguide/en-us/dmebg_dsp_rjnt.asp**, date not available**

4.0 After

4.1 Where Are We Today

We currently have a Windows 2000 AD Forest with a Root domain and 4 child domains. Each domain is used by different business lines for managing users and computers. Two of these domains are Citrix implementations. The Root domain and 3 of the child domains are managed by one security department centrally. Some privileges such as password resets, adding computers to the domain and group memberships are delegated to local administrators and password resets are delegated to the Helpdesk.

The fourth child domain is managed by a separate security department within the business line that owns the domain. This security department manages the domain centrally for all domain and OU level functions such as group policies. There are several data centres in geographically remote locations that manage users, computers, groups and group memberships in a distributed manner.

This fourth domain has a very complex structure due to the geographical locations and unreliability of network links. There are domain controllers in every branch office so that domain authentication is possible even if the network is not available. There are almost 200 domain controllers in this domain. This also necessitates a complex Group Policy structure as each of the branch offices has at least one Group Policy. In total this domain has almost 500 group policies. The complexity of managing this many domain controllers and group policies is significant. This complexity can be illustrated by a simple example. Changes in domain Group Policies can only be replicated to the remote domain controllers in an overnight window.

There is also a business line that has a separate forest. They have very specific requirements for tolerance and flexibility of change. Discussions have been held to look at the issues related to one forest rather than multiple forests but at this time they will remain in their own forest. There are significant benefits to a single forest versus multiple forests. There is a good Microsoft paper that discusses the issues of multiple forests[7].

---

7 Microsoft. "Multiple Forest Considerations in Windows 2000 and Windows Server 2003" URL: http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/directory/activedirectory/mtfstwp.mspx, April 8, 2004

4.2 Active Directory Review Task Force

We are currently involved in an Active Directory Review. This is an evaluation of every domain, including Root and the separate forest, to identify weaknesses. We have looked at every domain using the following categories:

- Governance - Review of controls for management of the domain
- Security Administration and Lockdown - Review of administration procedures and domain lockdown
- Logging, Backup and Retention - Review of logging, backup processes and retention periods
- Reporting - Review of reporting processes

We developed a scorecard rating for each domain under the four categories above with ratings from:

- Green - No issues
- Light Green - Minor issues (low priority)
- Yellow - Medium issues (medium priority)
- Orange - Serious issues (high priority)
- Red - Immediate action required

Each department responsible for their respective domains provided issues and how they felt they should be rated. Each of these issues was discussed by the task force to obtain agreement of the rating and determine if these same issues existed in the other domains.

The task force detailed each issue and provided a recommendation for a solution. The task force found that almost all of the issues for a given domain applied to all domains. There were some issues that were specific to a single domain. Each security department that was responsible for the management of their respective domains was asked to put in place project plans for dealing with the issues. This is the current stage of the task force review.

The mandate of the task force is to deal with all of the identified issues until they can be rated at an acceptable level. The task force will then meet on a regular basis to discuss new issues, audits and share information.

4.3 Microsoft Active Directory Review

The scope of this review is defined as follows.

- AD health check

- Domain controller deployment
- Group Policy deployment
- Inclusion of additional domains in future

Microsoft recommends performing a periodic health check of your AD to ensure that it remains secure, in compliance with corporate policies and conforms to Microsoft best practices[8]. Microsoft has been engaged in a statement of work to perform a detailed review of the health of the Active Directory. They will be using scripts and manual checks that they have developed.

The health check findings will be reported to the AD Review Task Force. The findings will be evaluated for their level of risk. Based on the determined risk there will be an action plan developed to deal with the findings based on priority.

4.4 Reporting

One of the areas that the AD Review Task Force identified as a weakness in every domain was reporting. In order to address the reporting issue we have obtained bv-Control for Windows and Active Directory in order to be able to create the types of reports required. The requirements for most of the reports were common to every domain. Some of the report requirements are as follows.

- Report(s) showing new users added, users deleted, users disabled and users enabled.
- Report(s) showing GPO adds, changes, deletes.
- Report(s) showing changes to GPO links.
- Report(s) showing effective settings for group policies.
- Report(s) showing differences between two different group policies.
- Report(s) showing the last login for users more than a predefined number of days old.
- Report(s) showing all unsuccessful Kerberos and NTLM login attempts.
- Report(s) showing changes to critical system registry entries.

Bindview Professional Services were engaged to provide us with onsite development of customized reports based on the provided requirements. The engagement was able to address each of the report requirements. Some of the requirements were satisfied with a report and others had to be dealt with a report in combination with a management process. For example the information to determine who implemented a GPO change is not available from Microsoft. We

[8] **Microsoft. "Best Practice Guide for Securing Active Directory Installations and Day-to-Day Operations: Part I" URL:** http://www.microsoft.com/technet/prodtechnol/windows2000serv/technologies/activedirectory/maintain/bpguide/part1/adsecp1.mspx**, February 28, 2004**

developed a report to determine that a GPO had changed and then in combination with the change management and powerful privilege id activation process we were able to determine who made the change.

Some of the benefits of these products are as follows[9].

- Auditing and documenting the compliance of corporate policies
- Identifying and resolving security holes by assessing risks and closing security holes across workstations, servers and users
- Locating missing patches
- Managing the configuration of servers to ensure that appropriate hot fixes and service packs are loaded
- Monitoring and reporting on event logs

We are currently in the process of developing a common set of reports for two of our domains. Once these reports have been developed they will be deployed on all domains. There are requirements for unique reports that are specific to a domain. These reports are also under development.

4.5 Summary

We feel we have a secure AD environment but like most projects it was implemented with aggressive timelines. This often necessitates the implementation of a solution that, although it may be secure, has some weaknesses that could not be addressed as part of the project. I highly recommend performing an AD Review as we did and I am sure you will find some surprises.

We performed this AD Review before our internal auditors commenced any audits of AD. When the audit was performed we had already identified almost all of the findings that they documented. The project plans in place to deal with these issues were already in place or under development as a result of the AD Review and therefore went a long way to assure the auditors that we were aware of the issues and had an action plan in place.

The reporting issue cannot be dealt with existing native Windows 2000 AD tools. It is necessary to look at alternative solutions available from other vendors as well as Microsoft.

[9] **Bindview Corporation. "bv-Control for Windows and Active Directory",**
URL: http://www.bindview.com/Products/VulnMgmt/AssesmentandSecurity/bv-Control_Windows.cfm**, May 27, 2004**

5.0 References

**1 Microsoft. "Microsoft Knowledge Base Article – 320423"
URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;320423, November 21, 2003**

**2 Microsoft. "Administering Group Policy with the GPMC"
URL: http://www.microsoft.com/windowsserver2003/gpmc/gpmcwp.mspx, December 11, 2002**

**3 Microsoft. "How To: Optimize Group Policy for Logon Performance in Windows 2000"
URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;315418&Product=win2000, September 22, 2003**

4 Komar, B., (2001) Designing Microsoft Windows 2000 Network Security, Microsoft Press

**5 Microsoft. "Microsoft Windows Server 2003 Deployment Kit",
URL:
http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/deployguide/en-us/Default.asp?url=/resources/documentation/WindowsServ/2003/all/deployguide/en-us/dmebg_dsp_rjnt.asp, date not available**

**6 Microsoft. "How to: Administer GPO Properties in Windows 2000",
URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;322176&Product=win2000, October 30, 2003**

**7 Microsoft. "Multiple Forest Considerations in Windows 2000 and Windows Server 2003"
URL:
http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/directory/activedirectory/mtfstwp.mspx, April 8, 2004**

**8 Microsoft. "Best Practice Guide for Securing Active Directory Installations and Day-to-Day Operations: Part I"
URL:
http://www.microsoft.com/technet/prodtechnol/windows2000serv/technologies/activedirectory/maintain/bpguide/part1/adsecp1.mspx, February 28, 2004**

9 Bindview Corporation. "bv-Control for Windows and Active Directory"

URL:
http://www.bindview.com/Products/VulnMgmt/AssesmentandSecurity/bv-Control_Windows.cfm, May 27, 2004