GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Group Policy Security Risks and Best Practices

Jenko Hwong
GIAC GSEC Practical (v1.4c)
October 11, 2004

Abstract

A good deal of information exists about the content or settings of Group Policy including the base security settings, often delivered in the form of security hardening guides and security template .inf files. Work by SANS, NSA, and other security organizations have resulted in certificate courses such as the Windows 2000 Gold Standard Certificate (GGSC). However, less has been written about real-world experiences with Group Policy and security issues due to the design and architecture of the Group Policy infrastructure itself. With the complex, scalable architecture of Active Directory and the hundreds of settings in Group Policy, it is easy for users to leave security holes in their environment or worse, cause user or application downtime.

This paper explores some advanced security topics related to Group Policy, such as:

- How can users start to cope with the complexity of Group Policy?
- What are some real-world experiences, pitfalls, and best practices?
- What should Active Directory or Group Policy administrators be aware of, from a technical design or architecture perspective in order to secure their Active Directory/Group Policy environments better?
- What are possible attack points in the Group Policy infrastructure?
- How can one mitigate risk with such a critical infrastructure?

and recommends best practices for mitigating risk with the Group Policy infrastructure.

ABSTRACT 1

1. GROUP POLICY OVERVIEW 4

1.1. INTRODUCTION 4
1.2. FUNCTIONALITY 4
1.3. TARGETING 4
1.4. USER AND APPLICATION AVAILABILITY IMPACT 5
1.5. ARCHITECTURE 5
Data/Functional Flow 6
GPO Data Storage 6
Local Policy 7
Authentication 7
Access Control 7
Encryption/Privacy 7
Data Integrity/Signing 8
Auditing 8
1.6. SECURITY IMPLICATIONS 9
Security Filter Design Means Policies Widely and Easily Readable 9
Default Domain Policy 9
Storage Design Can Cause Inconsistent Data 9
Replication Can Cause Inconsistent Data 9

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Domain Scope and Domain-Specific Settings Increase Administration Overhead *10*
Centrally Managed or Centrally Screwed-Up *11*
Disconnected and Legacy Clients are Trouble *11*
Local Policy is Difficult to Manage *11*
1.7. REAL WORLD 11
Who's Doing What *11*
Pitfalls *12*

2. VULNERABILITIES AND ATTACK POINTS 15

2.1. GPO SETTINGS 15
Password/Account Settings *16*
Services Running *16*
Restricted Groups *16*
Login Locally *16*
Security Options (LAN Manager Hashes) *16*
IPSec Policies *16*
Renamed Administrator Accounts *16*
File, Registry, and Service ACLs *17*
2.2. GPO CONFIGURATION 17
Incorrect Delegation/ACLs *17*
AD Properties *17*
Domain Trusts *17*
Group Membership *17*
Computer Accounts *17*
DNS and Service Endpoint Registrations *18*
2.3. COMMON SYSTEM SERVICES 18
FRS *18*
Active Directory Replication *18*
LDAP *18*
Client Authentication *18*
GPO Download *18*
WMI *19*
Active Directory Services *19*
TCP *19*
2.4. DOS 19
Replication Traffic *19*
Exclusive Read Lock in W2K sp2 ..... *20*
GPO Configuration—Performance Impact *20*
2.6. MAN-IN-THE-MIDDLE 20
2.7. BUFFER OVERFLOWS 20
2.8. SUMMARY 21

3. BEST PRACTICES 21

3.1. GET AND STAY INFORMED 21
3.2. PROCESS AND PROCEDURES 22
3.3. CHANGE AND CONFIGURATION MANAGEMENT 22
Versioning and Documentation *23*
Backup/Restore - Disaster Recovery *23*
Change Management *23*
Auditing Trails *24*
Validation and Consistency Checks *24*
Related Security Topics *24*
Ideal Solutions *25*
3.4. VULNERABILITY SCANS AND VALIDATION/HEALTH CHECKS 25
3.5. DISASTER RECOVERY 25
3.6. DELEGATION/ACL MANAGEMENT 25

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

3.7. TROUBLESHOOTING 26
Identification 26
Analysis 26
Response 26
Related Security Topics 26
3.8. AUDITING AND MONITORING 26
Microsoft Audit Collection System (ACS) 27
Third-Party Approaches 27
Ideal Solutions 27
Related Security Topics 27
3.9. INCREMENTAL APPROACH 27
4. CONCLUSION **28**
REFERENCES **29**

Trademarks

Microsoft, Windows 2000, Windows 2003, Windows XP, Group Policy, GPMC, Group Policy Editor, ACS, Audit Collection System, and Ultrasound are registered trademarks of Microsoft Corporation. FullArmor, FAZAM, FAZAM 2000, and FAZAM Auditing are registered trademarks of FullArmor Corporation. NetIQ, NetIQ Group Policy Administrator, and NetIQ Group Policy Guardian are registered trademarks of NetIQ Corporation. Quest is a registered trademark of Quest Software Inc. Bindview is a registered trademark of Bindview Corporation. All other product names mentioned herein are trademarks or registered trademarks of their respective owners.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

1. Group Policy Overview

1.1. Introduction

Windows 2000 introduced Active Directory (AD) as a new architecture for centrally managing users, computers, and configuration settings in a Windows environment. A key component of Active Directory is Group Policy, an infrastructure to manage over 1000 various security, application, and user settings from a central location.

The goal of Group Policy is to improve security and reduce cost of ownership by allowing for centralized update and management of these settings, yet allowing replication of these settings across the largest enterprise networks for high scalability and fault tolerance.

Group Policy was designed to be the central store for configuration information, and more and more Microsoft and third-party products can be configured through Group Policy.

1.2. Functionality

Group Policy settings are divided into user and computer sections and only the appropriate sections are applied depending upon if the target is a user or computer object (with the exception of loopback processing).

Group Policy covers a range of functionality: password and account policy, OS auditing, network and security options, public key encryption, registry settings, group policy infrastructure behavior, software distribution, restricting which software can run, Internet Explorer settings, IPSec policies, restricting group membership, file, registry, and service ACLs, folder redirection, user rights for OS operations, Start Menu, Control Panel, and Desktop configuration.

There is also an Administrative Templates section to each Group Policy Object (GPO) that includes registry settings—this is an extensible area of Group Policy and is a source of ongoing additions to Group Policy functionality. As an example, Windows XP SP2 includes new settings to control the Windows Firewall—these are distributed as new administrative templates with underlying registry settings.

1.3. Targeting

GPOs must be applied or targeted to users or computers using one or more of the following methods:

- Linking to an AD container (i.e. domain, site, OU)
  The GPO will apply to any user or computer objects contained within the container (or its sub-containers). Link information is stored in the gpLink property of the AD container.
- Security Filtering
  This involves setting Read and Apply DACLs (Discretionary Access Control Lists) on a GPO to determine which user/group or computer accounts will

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

receive a GPO. The GPO DACLs may also be referred to as GPO delegation rights as they are also used to delegate administrative control over GPOs.

- WMI Filtering
  This is a new 2003/XP feature allowing a GPO to be targeted based on the results of a WMI query against the target computer (thus utilizing WMI information such as hardware, OS, or application state).

AD linking is the most common method, followed by security filters. WMI filters are not common due to performance issues and limitations in functionality (only one filter can be used per GPO).

1.4. User and Application Availability Impact

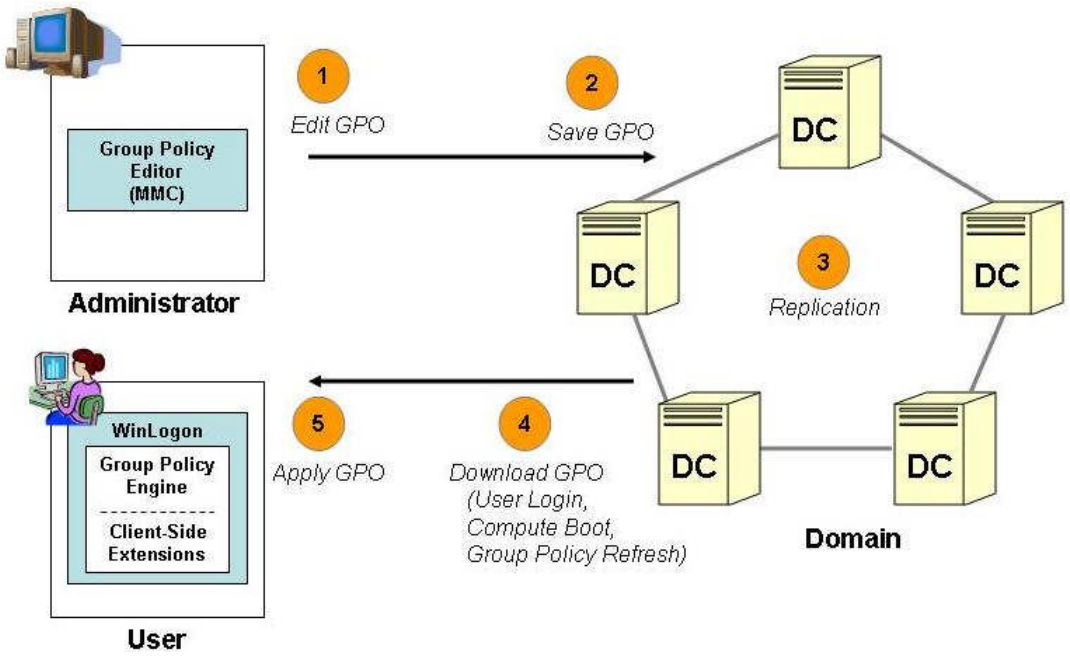
The majority of Group Policy settings relate to security in some fashion. GPOs can be used to install applications, grant users appropriate rights, give them access to services and applications to do their jobs, and implement security policies such as strong password strength. Group Policy can have a tremendous impact on users' availability of applications or data. It is easy to grant any domain user access to any file, service, or registry key on any computer. Setting the wrong permissions in a GPO can easily result in a user being unable to login to her computer in the morning.

1.5. Architecture

The Group Policy architecture uses the multi-master domain controller replication model of Active Directory to distribute the Group Policy settings throughout the enterprise and includes a client-side pull model for actually downloading GPO settings in order to apply the functionality. The major components are displayed in the following high-level architecture diagram[1]:

[1] "Group Policy Collection," Components.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



Data/Functional Flow

1. Edit GPO: The Windows or Active Directory administrator will use the Group Policy Editor to edit Group Policy settings on a domain controller. The Group Policy Editor can be accessed as an MMC snap-in or can be launched from tools such as Active Directory Users and Computers, Group Policy Management Console (GPMC) or 3rd-party products such as FullArmor's FAZAM 2000 or NetIQ Group Policy Administrator. The GPO's settings are read from a domain controller.
2. Save GPO: After applying changes within the Group Policy Editor, the changes are written back to the domain controller (DC).
3. Replication: Active Directory Replication and the Filesystem Replication Service (FRS) propagate the GPO changes to every DC in the domain. Both AD and FRS replication utilize the RPC Endpoint Mapper (TCP 135) and a dynamic port (by default) for replication.
4. Download GPO: The new GPO settings are downloaded by the client-side extensions (CSEs) that run within the winlogin process during user login, computer boot, or the periodic group policy refresh cycle.
5. Apply GPO: The new GPO settings are applied by the individual CSEs and affect user and computer behavior.

GPO Data Storage

Understanding a GPO's data storage is crucial to understanding the security and manageability issues surrounding a GPO. A GPO is stored partially in AD and partially as text-readable files on the file system. The AD portion can be browsed with Active Directory Users and Computers (ADUC) and contains settings information such as folder redirection references, IPSec Policies, and Wireless settings (Windows 2003). The majority of settings are stored as files on the filesystem on the SYSVOL share of

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

each domain controller. GPOs are assigned unique ids (GUIDs) at creation time and the AD containers for the GPO and the top-level folder for the GPO on SYSVOL are named after the GUID.

Local Policy

The Group Policy Editor can also be used to edit on each machine the local security policy object (LGPO), which contains a subset of the security settings found within a GPO. The local policy object information is stored in:

```
%SYSTEMROOT%\system32\GroupPolicy
```

The local and group policy settings are merged during runtime following LSDOU ordering i.e. Local-Site-Domain-OU with Local having lowest precedence.

Authentication

Authentication is based on standard Windows domain authentication. Any security implications depend on the authentication scheme used by Active Directory (by default Kerberos).

Access Control

Authorization and access control follows the standard Windows model. DACLs set on the GPO will be implemented as specific permissions on the underlying data storage objects for the GPO (AD containers and file system objects). For a GPO to be applied to a user, the user must have both Read and Apply permissions on the GPO. By default, Authenticated Users have Read and Apply permissions on the Default Domain Policy, since its purpose is to set domain-wide policy.

GPO DACLs are not inherited from the parent container or object, because inheritance would change the DACLs and drastically affect the availability or access to a GPO—causing in the worst case, denial-of-service for user functionality. Specifically, the GUID containers in AD (underneath the Domain>System>Policies containers) and the GUID folders on SYSVOL (under the Policies folder) will have inheritance blocked.

In the Windows security model, Domain Administrators (DAs) and Enterprise Administrators (EAs) can always take ownership of a GPO and re-edit the ACLs. This makes it more challenging to restrict access and maintain integrity of GPOs, especially in large enterprises where Domain Administrators group membership may be extensive. Since inheritance is not enabled for GPO objects, re-ACLing GPOs is a non-trivial task for organizations with a large numbers of GPOs since every GPO must be re-ACLed separately.

Encryption/Privacy

There is no encryption of a GPO's data, so having Read rights on a GPO allows one to browse all settings as well as AD properties. Some of the GPO data may be stored in binary format (e.g. registry settings in the registry.pol file), but the data is not encrypted.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Data Integrity/Signing

Since Windows 2000, SMB signing is available for all packets in a session but this is not enabled by default due to the performance overhead.

Auditing

There are no specific GPO auditing features built into Windows 2000 or 2003. However, auditing can be enabled for directory access of AD containers and object access for file system objects. Specifically, SACLs (System Access Control Lists) can be specified on the AD Policies container with ADUC and on the SYSVOL Policies folder with the File Explorer using the Auditing tab in the Security Properties, or can be specified at the GPO level using a GPO administration tool such as GPMC.

Low-level events will then be logged in the domain controller's Security Log, containing the GUID of the object modified, the low-level operation performed (read, write, modify attribute), the timestamp, and user performing the operation. This level of auditing helps identify which GPO has been modified by when and by whom, but does not provide a lot of information as seen in the following 560 audit event:

```
Event Type:       Success Audit
Event Source:     Security
Event Category:   Object Access
Event ID:         560
Date:             10/11/2004
Time:             8:55:07 AM
User:             W2K3\Administrator
Computer:         W2K3DC-JH
Description:
Object Open:
      Object Server:    Security
      Object Type:      File
      Object Name:      C:\WINDOWS\sysvol\domain\Policies\{31B2F340-
                        016D-11D2-945F-00C04FB984F9}\MACHINE\Microsoft\
                        Windows NT\SecEdit\GptTmpl.inf
      Handle ID:        1700
      Operation ID:     {0,1499490}
      Process ID:       4
      Image File Name:
      Primary User Name: W2K3DC-JH$
      Primary Domain:    W2K3
      Primary Logon ID: (0x0,0x3E7)
      Client User Name: Administrator
      Client Domain:    W2K3
      Client Logon ID:  (0x0,0x16E0FE)
      Accesses:   DELETE
                  READ_CONTROL
                  SYNCHRONIZE
                  WriteData (or AddFile)
                  AppendData (or AddSubdirectory or CreatePipeInstance)
                  WriteEA
                  ReadAttributes
                  WriteAttributes
      Privileges: -
      Restricted Sid Count:   0
      Access Mask:      0x130196
```

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

1.6. Security Implications

The architecture and design of the Group Policy infrastructure has several implications on security that are discussed in more detail in this section.

Security Filter Design Means Policies Widely and Easily Readable

Confidentiality of GPO settings is generally weak because:

- a user must have read access to a GPO in order to have its settings apply
- security filters are not used frequently so most GPOs are readable by Authenticated Users
- GPO data is not encrypted

The defaultSecurityDescriptor attribute for the groupPolicyContainer class in the AD schema will set read access by Authenticated Users by default in newly created GPOs. Administrators have to be disciplined to accurately manage and restrict security filters. An attacker can use GPO settings as reconnaissance for secondary attacks across the network.

Default Domain Policy

The Default Domain Policy by definition will apply to (and hence be readable by) Authenticated Users. Further, the GPO infrastructure will only apply account and password settings if a GPO is linked to the domain, meaning that the domain-wide security policies for account/password settings will be set in the Default Domain Policy (or its equivalent domain-linked GPO). Imagine that one of the first steps an attacker performs when gaining unprivileged access to a network is to read the Default Domain Policy and analyze it offline. If other GPOs are linked to the domain and used instead of the Default Domain Policy, this can be gathered by reading the gpLink property of the Domain container in AD.

Storage Design Can Cause Inconsistent Data

The storage design of Group Policy is complex and can affect the integrity of a GPO. Storing a GPO's data in both AD and on SYSVOL makes it difficult to have atomic write transactions that leave GPOs in a consistent state. Errors such as missing files and folders, misapplied DACLs, and incorrect version numbers (between AD and SYSVOL), are common in large enterprises. These types of errors result in a corrupted GPO that will not be applied. Imagine editing the Default Domain Controller Policy, writing it out, having some corruption be introduced, and not realizing that it wasn't being applied! Although Group Policy management tools are becoming better at providing error-checking and validation of GPO settings, this level of implementation complexity makes security very difficult.

Replication Can Cause Inconsistent Data

The replication of GPO data will almost assuredly introduce corrupted GPO data at some point in a large enterprise. There are two replication cycles (each on their own schedule) for AD and FRS, meaning there are time windows where a GPO is only partially replicated. The versioning scheme of GPOs ensures that GPOs do not apply if data is out-of-sync, but if one of the replication cycles fails, there is no built-in facility to restore state and integrity. How would a user even know a replication cycle has failed?

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The functionality is quite immature when compared to database transaction integrity with 2-phase commit and ACID properties.

In addition to separate replication cycles, FRS itself has had reliability problems that have caused replication corruption of SYSVOL. It is not uncommon to find that ACLs on SYSVOL objects have not replicated consistently across all domain controllers. Other times, actual objects may be corrupt or missing. Microsoft has addressed some issues with various FRS hot fixes,[2,3,4,5,6] but problems still remain and are encountered by large customers. The ongoing development of FRS monitoring products such as Ultrasound and the AD Management Pack for Microsoft Operations Manager, highlight the importance of monitoring the health of a complicated infrastructure such as AD and FRS replication.

Domain Scope and Domain-Specific Settings Increase Administration Overhead

GPO settings are replicated only within one domain. What happens if you want to apply the same settings to more than one domain? Although it is possible to link a GPO to AD containers in a different domain than where the GPO exists, there are two problems with this that make it impractical: 1) performance issues and 2) domain-specific information. A GPO linked to different domain than the client's can increase boot and login time significantly, so cross-domain GPO links are not recommended. The alternative of copying GPO settings between domains creates additional management overhead but generally is considered the lesser of two evils. The second issue is that GPOs often reference domain-specific settings: folder redirection and software distribution reference DFS shares, registry/file/service ACL settings reference domain accounts, and the GPO itself is linked to a specific container in its domain. This means that simply copying a GPO to another domain (or even cross-linking it) can result in meaningless settings and unintended results. GPO administration tools have designed migration features to help map this domain-specific information during the copying process.

Complicated Architecture Means Lots of Failure Points

The Group Policy infrastructure not only has a complicated data storage mechanism, complex replication issues, but also has a complex data flow. Failures can occur at multiple points, including the initial editing of a GPO setting on a domain controller, the replication of that GPO across all domain controllers in the domain (including both AD and SYSVOL portions), the replication or migration of a GPO to other domains, the client download of the GPO data over the network, and the actual application of the GPO settings to the user or computer. This makes troubleshooting and auditing more difficult and increases the management costs for organizations trying to leverage Group Policy functionality.

---

[2] "FRS Does Not Replicate Files or Folders If the System Account Does Not Have Full Control of the Directory Tree."
[3] "Improvements in the Post-Service Pack 3 Release of Ntfrs.exe."
[4] "Issues that are fixed in the post-Service Pack 3 release of Ntfrs.exe."
[5] "Improvements in the Post-SP2 Release of Ntfrs.exe That Is Packaged with an Updated Ntfs.sys Driver."
[6] "Ntfrs.exe Does Not Clean Up the Staging Folders on Members with No Outbound Partners in Windows 2000"

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Centrally Managed or Centrally Screwed-Up

The ease of central administration and management of Group Policy also carries an ability to make mistakes across the enterprise. A decentralized model is not necessarily better, but organizations do need to implement various controls and processes to maintain availability of resources and maximize user productivity. It is too easy to lock users out of a computer using Group Policy with a few clicks.

Disconnected and Legacy Clients are Trouble

Group Policy applies to managed computers currently joined and connected to the domain. In the absence of being connected to the domain e.g. mobile clients, cached policy settings and the local policy object will apply. Non-domain i.e. workgroup computers and legacy computers (pre-Windows 2000) cannot gain the benefit of Group Policy and present additional challenges in terms of what security or configuration policy actually is in place. Attempting to enforce a consistent policy in a large Windows environment is a challenge.

Local Policy is Difficult to Manage

Management of local policy is difficult because traditionally, there has not been a way to centralize updates and easily distribute changes. Most organizations do not even attempt to use it beyond the initial ghosting/imaging process for new computers. Some companies (FullArmor) have recently extended into this area by allowing local security and registry policy to be managed with forms of executable policy files, but the distribution of actual settings to the client will remain a challenge, just as in software distribution. Ideally, a defense-in-depth strategy would utilize local policy as one of the last lines of defense and to also ensure that disconnected clients have managed security policy in place.

1.7. Real World

Who's Doing What

Many organizations have migrated from Windows NT and legacy desktop clients to Windows 2000/2003 domains and Windows 2000/XP clients. Other organizations are still in the midst of migration and are still using Windows NT servers for legacy applications. For those organizations who have implemented Active Directory, many do not fully use Group Policy functionality. These organizations may only use the two default policies, the Default Domain Policy and Default Domain Controllers Policy, often with default settings. Other organizations have just started to use Group Policy, focusing on some basic security settings such as the account and password settings and registry (through Administrative Templates) settings to control widely-used applications such as Internet Explorer or Microsoft Office. Many folks who have been on the cutting-edge of implementing Group Policy (back to 2000 and 2001) have made many mistakes, learned much, and found bugs and limitations in the infrastructure. For the most part, awareness of Group Policy functionality has penetrated many organizations since 2002 and 2003, especially given Microsoft's introduction and launch of GPMC in 2003.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Since 2000, several vendors (FullArmor, NetIQ, Quest, and Bindview to name a few) have provided Group Policy administration tools. Initially, this was to address the lack of any Group Policy management functionality in Windows 2000 (there was only the Group Policy Editor, but no capability for RSoP, reporting, backup/restore, and copy/paste). Later these vendors expanded into various AD management functionality as well as extending Group Policy management into areas such as change management.

At the same time, most organizations still struggle with management of Group Policy on a large-scale, because it is a complicated infrastructure with rich functionality and configurability. Not only are users inundated with over 1000 total settings (a challenge by itself to just understand the functionality), they must also deal with how to apply and use that functionality (e.g. how many GPOs to create, division of settings among GPOs, design of AD OU structure in order to support policy, use of GPO loopback, whether and how to use security filters and/or WMI filters, performance considerations for how many GPOs are linked/filtered to each user/computer, what level of hardening guide to implement, orphaned/unlinked GPOs, tattooing of some GPO settings after the GPO is unapplied, backup policy, change management, etc.). When you add to this the level of complexity in the architecture and the possible security issues that arise in a large environment such as corrupted GPOs or misapplied ACLs, then the problems can appear overwhelming.

Many customers may not be aware of the scope of their problems due to their ignorance about:

- the state of their environment
- how much they lag in best practices
- how insecure their organization can be with mismanaged Group Policy
- how much better their organization can perform with better managed policy

In this respect, the state of Group Policy is not that different from general security awareness and best practices. There is still a fair amount of: “What about Group Policy? We don’t have any problems with Group Policy.” Yet an audit of the AD and Group Policy environment often reveals a myriad of misconfiguration, unapplied policy settings, conflicts, and data corruption.

Pitfalls

Group Policy is difficult. There is a lot of information to learn (over 1000 settings), complicated infrastructure to manage, and a lot of discipline required to be effective.

As with many Windows interfaces, changing a setting can be as easy as one-two-three, click. This can have disastrous effects because the Group Policy Editor makes live changes immediately upon clicking the OK or Apply button.

When Windows 2000 was first released, an administrator at one of the world’s largest software companies was editing the Services ACLs in the Group Policy Editor. By default on Windows 2000, every service’s DACL list included only the Everyone group, meaning all users (even unauthenticated ones) were allowed to run and change state of

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

every service. Practicing the principle of least privilege, the administrator proceeded to delete the Everyone ACE (two button clicks) for each service but failed leave any access rights at all. Within minutes, empty DACLs for all services were replicating throughout the domain and soon after, computers were downloading these settings and applying them. No users (not even administrators) could login to the computers affected and not even new Group Policy settings could be downloaded. Over 100 computers had to be reformatted. To be fair, later versions of Windows have changed the default ACLs, and GPO administration tools are now much better at validating such kinds of errors, but point-n-click administration can still easily affect a large number of users or computers in the enterprise.

ACLs can be dangerous in other ways. With Group Policy, you could easily remove all ACLs for the root of the system drive e.g. C:\. After these ACLs take effect and you logout of the machine, no one, not even administrators will be able to log back in. The login process itself requires access to files.

To further complicate matters, some GPO settings "tattoo" or permanently change settings, even after the GPO is unapplied! Although there are standard practices for ensuring that registry-based policy settings do not tattoo, there are still a number of GPO settings that do tattoo such as file/registry/service ACLs. There is no way to go back to your old settings. Note that the fundamental issue here is that for a setting to be reversible i.e. unapplied when the GPO is removed from the target, the old value must be saved or available. Standard registry-based policy achieves this by storing GPO settings in a different section of the registry than local preference settings. The same applies for security settings in local security policy objects vs. GPOs – they are stored in different areas. However, ACLs are attributes of the file system and there is no design mechanism in place to rollback ACL changes.

Some GPO settings sound extremely useful, such as Restricted Software Settings. However, upon further review, one finds out that the implementation may have caveats such as a dependency upon a file path. Not only may this be easy to bypass (by renaming and/or moving software), it may be difficult to implement since knowing all file/executable dependencies of third-party software may be difficult or impossible.

Many users may not realize that multiple GPO settings are often required to ensure that a policy is fully implemented. Account aging and password history both require multiple settings to be configured; otherwise no effective policy is actually set. Although the Group Policy Editor does a good job of warning users about the multiple settings that need to be set and although most third-party products use the Group Policy Editor, the user still has the burden to understand all settings and ensure they are set properly.

In other cases, multiple settings are required to ensure that the primary setting is not changed. As an example, it is not enough to configure security zones in Internet Explorer, but end-users must be restricted from actually changing that setting in IE. This is often unclear when looking at the Group Policy settings and with some settings there are multiple access paths to changing the setting—all of which have to be locked down.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Beyond confusion about settings, Group Policy replication can provide challenges to users due to its complexity: GPOs stored in AD and SYSVOL, replicating on different cycles, with non-atomic SYSVOL replication composed of multiple file system objects. Because of this, FRS can cause corruption of GPO data or its ACLs, with the end-effect being that GPOs are not applied—they sit in some mal-formed state on some or all domain controllers.

Even worse, administrators can be completely ignorant of replication issues because there is no built-in GPO auditing/monitoring, and there are only weak tools for validating GPOs in a large-scale production environment. Imagine setting crucial security settings in a GPO for the domain controllers or Exchange servers, apply them, have them become corrupted during replication, the settings do not apply, yet never being aware of this. Imagine further, that you have 10 domains that require this same setting, so you copy/paste/migrate this setting nine more times. Regardless of whether replication problems arise or not, just knowing whether your 10 domains are in a consistent, valid state (or not suddenly) becomes an administrative nightmare.

The Group Policy Editor itself can present problems. With Windows 2000, the Group Policy Editor was the only method to look at GPO settings and required modify access in order to launch—there was no read-only mode. This made it impossible to practice the principle of least privilege and made it very easy to have unintended modifications of GPOs.

There is a also a bug in the Group Policy Editor where setting a Deny ACE on a GPO will incorrectly set the write synchronization bit in the security descriptor on the SYSVOL files of the GPO, causing the GPO to be unreadable. Since Deny ACEs are not commonly used, this may not occur frequently, but the effects can be enormous—GPOs will not apply. This bug was encountered while attempting to help a Fortune 50 company lock down access by re-ACLing GPOs and shows how security can be even more challenging when the implementation is complex (in this case, the underlying storage mechanism of using SYSVOL files).

Even if there are no corruptions or bugs in the Group Policy infrastructure itself, its complexities can make data integrity a challenge. Since AD is a multi-master replication model, there is not a single master DC—any domain controller can initiate replication. Although highly scalable, simultaneous changes on different DCs will cause conflicting updates. If Administrator Joe edits the minimum password length in the Default Domain Policy on DC 1 and Administrator Betty edits the same setting on the Default Domain Policy GPO on DC 2…does the last change win? It gets more complicated when the change is for different underlying objects in the GPO. What if Joe changes the minimum password length on DC 1 (GptTmpl.inf), but Betty disables the computer section (AD) and sets a registry setting on DC 2 (registry.pol)? Do the changes merge haphazardly or does one GPO copy win? In practice, the resulting state is unpredictable, and corruption is likely.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Besides issues related to management and process, there are problems in performance. DCs are part of the critical infrastructure that affects all users and computers. It is important to minimize the impact on DCs as much as possible. "Orphaned" GPOs are GPOs that are not linked to any AD container, meaning that they are useless because they will not apply. To minimize management overhead, they should be deleted. In the early days of Windows 2000, one large manufacturer had over 500 GPOs in their environment but nearly half of them were unlinked—they were afraid to delete them because it was unclear what their purpose was, who created them, and why. Imagine the space wasted on all DCs and the potential bandwidth impact should a trivial change ever be made (causing replication), not to mention the confusion and wasted time for the administrative team.

These administrative pitfalls raise additional concerns with auditing because there is no auditing specific to Group Policy. Although file system edits and AD updates can be audited, they are very low-level, identifying user and timestamp, but little about what exactly changed. The GPO GUID is usually identified, but which of the 1000 settings changed is not. This effectively makes native auditing useless for GPO change tracking.

One way to mitigate these problems would be to minimize who had update rights on GPOs to minimize these types of mistakes. However, scaling the management and administration of GPOs across a large enterprise often runs counter to centralizing the management to a few trusted parties. Having only a few administrators perform every GPO change for hundreds of GPOs for tens of thousands of users and computers globally will not scale, meaning that not a lot of policy will be implemented or that changes may take a long time—both end up decreasing security.

The Windows security management model makes it difficult for users to manage this. Since GPOs do not inherit ACLs from their parent containers/folders, there is no easy way to correct corrupted or misapplied ACLs across all GPOs, except for one GPO at a time. DAs and EAs can always take ownership and modify GPOs making it difficult to prevent access to GPOs in large organizations where there are many DAs. Auditing is weak, so incident handling is haphazard and disorganized. Even if you are able to start with a clean environment, managing GPO ACLs is worse than managing file system ACLs because there is no built-in reporting, it's difficult to validate your changes across DCs, and difficult to apply changes to multiple GPOs.

2. Vulnerabilities and Attack Points

Having discussed the functionality and architecture of Group Policy, we now look at how this might be exploited from an attacker's viewpoint. Although there have not been any publicized exploits specifically targeting the Group Policy infrastructure, it is only a matter of time before attackers become more knowledgeable and start to leverage the content and configuration of GPOs as reconnaissance for secondary attacks.

2.1. GPO Settings

Since GPOs are generally world-readable, this raises similar issues in password-cracking ass world-readable Unix password files. GPO security settings can be easily

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

dumped and analyzed offline to tailor or customized follow-on attacks. The two default policies have well-known GUIDs and are an easy starting point. Checking the gpLink and gpOptions settings for the domain and the Domain Controllers OU is also a good starting point as they will identify which exact GPOs are being applied to the domain and DCs, as well as whether inheritance/override is in place. Here are some other settings that may reveal useful information to the attacker.

Password/Account Settings

The minimum password length can be used to optimize password cracking programs by skipping the generation of shorter guesses. The account lockout policy can be used to tailor DoS attacks against accounts.

Services Running

Knowing which services are enabled is an easy way to target network attacks without actively scanning other hosts. This could be used to more stealthily attack additional hosts without raising as high a profile to any detection systems (IDS, sniffers) that may be deployed.

Restricted Groups

If set, Restricted Groups often will include privileged groups such as the Administrators group. This information can be used to target password cracking on privileged accounts. This information could also be obtained from AD queries, but this is one more source of data.

Login Locally

Knowing which accounts have rights to logon locally is useful for an attacker attempting to gain remote access. By analyzing those GPOs that apply to sensitive servers (e.g. Exchange Servers), targeted password-cracking attacks or privilege exploits could be performed on a subset of accounts.

Security Options (LAN Manager Hashes)

Many miscellaneous security options exist including the setting of the LAN Manager authentication level and anonymous enumeration of SAM info (null sessions). Some of these options can serve as the basis for password-cracking or DoS exploits.

IPSec Policies

If IPSec is being used for packet/port filtering, then this information is akin to having knowledge of firewall/router rules, and can be used to target attacks more specifically and with less chance of detection.

Renamed Administrator Accounts

Although administrator accounts have well-known SIDs, knowing that they have been renamed can be useful depending upon the particular attack vector—in those cases where login with reference by account name is done (interactive login or via API).

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

File, Registry, and Service ACLs

If any file or registry ACLs are explicitly set to protect sensitive files, attackers can target the particular accounts that have privileges. Ultimately, the list of accounts referenced can be useful as a target list for cracking.

2.2. GPO Configuration

In addition to the content or GPO settings themselves, the configuration of the Group Policy Object provides additional information useful to the attacker.

Incorrect Delegation/ACLs

Analyzing the ACLs for both the AD and SYSVOL portions of a GPO may help gain unauthorized write access to the GPOs or may identify security holes if the GPOs are not being applied. ACL security holes could be exploited to allow GPO update privileges to non-privileged accounts, corrupt or delete GPOs, modify GPOs to introduce vulnerabilities, corrupt application data, or create DoS situations.

AD Properties

The gpLink and gpOption properties of the AD containers can also be helpful in understanding where GPOs are being applied and with which options. If modification rights exist on the gpLink property, GPOs could be relinked or unlinked, effectively removing their policy settings from the environment. Access to the gpOption property could be used to modify inheritance and override settings with the effect of changing the effective policy settings that apply to a user or computer. In practice, AD ACLs are not prone to corruption like file system objects under FRS, so ACL security holes in AD are less likely.

Domain Trusts

Querying for domain trust information is useful in order to identify other domains that can be queried and attacked. A rough analogy would be discovering the network prior to or after a traditional network exploit. Trust information helps identify the logical topology of Active Directory, ultimately identifying potential attack vectors and additional targets.

Group Membership

AD can be queried directly for group membership. This allows one to understand the delegation model and the list of privileged accounts, allowing for targeted attacks for password-cracking and ability to understand impact and value of gaining access to various privileged accounts.

Computer Accounts

AD also contains a list of all domain-joined computer accounts and their organization into OUs. For example, the Domain Controllers OU will typically contain all DCs. This is a form of host discovery but through a different reconnaissance vector that typically has a lower profile to detection systems since only one DC needs to be queried for this information, as opposed to active network discovery that scans each IP device. Often other servers may be identified by name or OU, so other critical servers may be identified for focused attacks.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

DNS and Service Endpoint Registrations

Both DNS and Service Endpoint registration information is stored in AD and includes server and port number information. This can help identify services running on non-standard ports and focus network attacks without having to actively port scan.

2.3. Common System Services

Group Policy utilizes common Windows services to perform domain controller replication of its data and to expose query interfaces for information. These services and the ports and protocols they use expose potential attack vectors.

FRS [7]

FRS uses the RPC Endpoint Mapper (TCP 135) and a dynamically assigned port to replicate SYSVOL portions of GPOs. To replicate through firewalls, a static port can be configured using a registry key[8].

Active Directory Replication

AD replication also uses the RPC Endpoint Mapper (TCP 135) and a dynamic port for replication of the AD portion of the GPO. Similarly, static ports can also be configured using a registry key.

LDAP

LDAP queries are required to obtain GPO information stored in AD including: GPO data, gpLink, and gpOption information. LDAP runs on the following ports[9]:

- TCP 389 (LDAP)
- TCP 636 (LDAP SSL)

Windows 2000 had an exploit with non-privileged users being able to change other users' passwords over an LDAP SSL connection[10], and although this has since been patched, the serves to reinforce the axiom that the surface area exposed to attack is proportional to the number of ports left open. Group Policy inherits much from the AD infrastructure, and administrators should be aware of these dependencies.

Client Authentication

TCP/UDP 88 is used for Kerberos authentication and is another requirement for healthy AD and Group Policy.

GPO Download

Clients will download GPO data using LDAP and SMB (TCP 445/139). Attacks against these ports can pose difficult issues for customers who are trying to protect or quarantine at the same time as use Group Policy functionality. Sasser attacked SMB

[7] "Description of the FRS Replication Protocol, Notification and Schedule for DFS Content."
[8] "How to Restrict FRS Replication Traffic to a Specific Static Port."
[9] "How to Configure a Firewall for Domains and Trusts."
[10] "Microsoft Security Bulletin MS01-036."

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

port 445 and was one of the viruses that highlighted the tight dependency of many Windows functionality on a few common system ports. [11,12]

WMI

WMI is used for RSoP logging mode (diagnostics on clients), Windows 2003 RSoP modeling (with GPMC), as well as WMI filters for targeting/application of Policy. It relies on DCOM and hence utilized the RPC Endpoint Mapper (TCP 135).

Active Directory Services

In addition, several additional services are required for healthy operation of Active Directory which does affect availability of Group Policy functionality since it is the same underlying infrastructure that provides both capabilities:

- **Global Catalog**
  TCP 3268 (LDAP GC)
  TCP 3269 (LDAP GC SSL)
- **DNS**
  TCP/UDP 53
- **WINS**
  TCP/UDP 1512 (WINS resolution)
  TCP/UDP 42 (WINS replication)
- **NTP**
  UDP 123

2.4. DoS

Certainly explicit denial of service attacks can be launched against the common core services listed in section 2.3. One could attack the domain controllers directly and attempt to create DoS situations such as a flood of simulated logins or reading of SYSVOL shares. However, the scalability of DCs in general are quite good (e.g. 10 to 20 high-end quad-proc Xenon servers with 1 GB+ RAM and high-speed networking can support tens of thousands of users), so a high-level of client activity would be required to significantly affect performance. Since domain controllers are typically exposed only on internal-facing LANs, the probability of traditional DoS/DDoS attacks may be less likely, however it is useful to understand the potential attack vectors.

Replication Traffic

A subtler attack might be to use the delegation rights on GPOs to cause excessive FRS replication activity by updating the SYSVOL share with minor updates to a large data file placed there by an attacker. This would require either write access via a privileged account or misconfigured ACLs that allow non-privileged write access to at least one GPO folder. An analogous hypothetical DoS attack against Active Directory was described by Aaron Sullivan in a January 2002 SecurityFocus article.[13]

[11] "PSS Security Response Team Alert - Sasser Worm and Variants."
[12] Kington, Tristan.
[13] Sullivan, Aaron.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Exclusive Read Lock in W2K sp2

3apa3a@security.nnov.ru discovered a Windows 2000 sp2 bug where any user (non-privileged) could obtain an exclusive read lock on a file, preventing any other read access to it—this could even be launched via a network share[14,15]. The potential effect would be that Group Policy would not be applied. Though this has since been patched in Windows 2000 sp3[16], it does show that the complexity of and lack of abstraction of the storage mechanism for Group Policy data makes DoS exploits more likely.

GPO Configuration—Performance Impact

There are subtle misconfigurations in Group Policy that may lead to availability issues for users. Users might encounter degraded availability of service as long boot-up or login times. This can be caused by:

- Too Many Linked GPOs—causing long processing of GPO data
- Cross-Domain GPO Links—GPOs may be downloaded over slow links
- Bad Site Topology—when a local DC is not available in the site, GPO may be downloaded over a slow link
- Use of WMI Filters for targeting—the target host must be queried
- Use of large number of file or registry ACLs—increases disk activity as the ACLs are applied. This can be an issue with any very-hardened security template .inf files which include a large number of file/registry ACLs.
- Badly written boot/login scripts—which may incur a large overhead

The asynchronous/background processing of GPOs available in XP and 2003 clients can help alleviate login processing time, but creates a time window where policy has not been fully applied (potential security gap).

2.6. Man-In-The-Middle

Man-in-the-middle (MITM) attacks can be potentially launched because there is no encryption of GPO data and no signing by default. Although SMB signing is available as an option in Windows 2000 and XP for SMB data transfer (SYSVOL), there have been flaws detected in SMB signing in Windows 2000 and XP sp1.[17] Even if there were no exploits, "SMB Signing is disabled by default on Windows 2000 and Windows XP because of the performance penalty it exacts."[18]

2.7. Buffer Overflows

The risk of buffer overflows is tied to the standard system services used by the Group Policy Infrastructure as outlined in section 2.3. The primary ports are the RPC Endpoint Mapper (TCP 135), SMB (TCP 445/139), and LDAP (TCP 389). Any successful attacks against these specific ports would likely cause severe disruption in AD as well as other services.

---

[14] 3APA3A@security.nnov.ru.
[15] "Microsoft Windows 2000 Group Policy Evasion Vulnerability."
[16] "Microsoft Security Bulletin MS02-016."
[17] "Microsoft Security Bulletin MS02-070."
[18] "Microsoft Security Bulletin MS02-070."

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

2.8. Summary

It is a good idea to document the key technical dependencies of the Group Policy infrastructure and update appropriate incident-handling and BCP/DR plans to include procedures and service levels to address when any of these dependencies (e.g. common core ports and services) are exploited.

As an example, one large Fortune 50 company had an internal policy that shutdown access to port 135 on domain controllers in response to a worm that attacked the RPC Endpoint Mapper. One of the side effects was that Group Policy replication was prevented and policy updates were put on hold for over a week while the worm was being contained and eradicated. With some foresight and planning, perhaps a higher-level of service could have been achieved during this incident.

Although many of these vulnerabilities are not new and have mitigating factors that reduce their risk, there are several interesting points worth mentioning:

- Group Policy is a force-multiplier by design. Its intent is to allow easy, centralized management of security policy across the enterprise (i.e. a domain containing tens of thousands of users and computers). Any security breach of Group Policy can be multiplied greatly by a knowledgeable attacker.
- Group Policy presents an interesting opportunity for more passive reconnaissance—not completely, since GPO data must be read from a DC in the domain under attack, but it can be carried out with a much lower profile than active network scanning.
- Group Policy infrastructure is complicated. We've seen how this creates additional attack vectors, and ultimately it means that Group Policy is hard to secure in areas such as access control management, validation, auditing, and detection. For example, how would you even detect that an unprivileged account was reading all GPO data from a DC? What would be the signature? Unfortunately, there are no easy answers, but some of the best practices discussed in the next section provide some guidance for improving the situation.

3. Best Practices

Hopefully, you haven't been scared away from Group Policy. Its complexity will make secure management and productive use a challenge, but it is not impossible. Similar to other security domains, some knowledge and common-sense along with discipline and hard-work will help you improve continually in securing your Group Policy infrastructure. Ultimately, all of these best practices are about mitigating risk. You will observe parallels with general security practices: creating policies, procedures, and process, attempting to practice the principle of least privilege, and defense-in-depth.

3.1. Get and Stay Informed

Start with understanding the basic Group Policy concepts, architecture, and runtime behavior. Although a brief overview was provided in section 1 of this paper, excellent in-depth resources exist online including:

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- Microsoft's Group Policy Website[19]
- "The Definitive Guide to Windows 2000 Group Policy," by Darren Mar-Elia[20]

The next challenge is to understand the functionality of Group Policy settings. Material from the Microsoft website will help with this. However, the number of Group Policy settings increases with each service pack, so keeping abreast of new GPO settings is important, particularly the new ADM templates. For Windows XP sp2, the latest descriptions can be found in an Excel spreadsheet on Microsoft's website (search on: ADM reference)[21].

When in doubt, searching the web will provide a wealth of information on Group Policy functionality—part of the challenge is dealing with the information overload.

3.2. Process and Procedures

Managing Group Policy day-to-day is not that different from any IT roll-out process. Proper planning should be done with clear stages for:

- design (e.g. "how many GPOs with which settings?")
- implementation (e.g. changing GPO settings)
- testing of settings (e.g. in a test lab or using RSoP)
- deployment (e.g. application of settings to the production domains/forests)

Within this context, there is flexibility to adjust the process and procedures to the organization's environment. Small environments may not have a dedicated test environment, minimal bureaucracy, and a few administrators who perform all the work. Large environments may require strict change control procedures, have one or more testing environments, and delegate administrative responsibility for GPO changes across many administrative groups.

In addition to the basic design, develop, test, and deploy stages, be sure to cover incident-handling stages such as trouble-shooting, auditing/monitoring, and disaster recovery. When a critical incident occurs, this pre-planning will earn its return many times over.

Whatever the process, make sure that it is clear to all people involved, so that mistakes don't occur due to lack of clarity.

3.3. Change and Configuration Management

Because it is so easy to wreck havoc with Group Policy, it is strongly suggested that some level of change and version controls be put in place. The worst possible scenario would be to not know what changes have been performed or were supposed to be performed as the organization loses money because users cannot login or access their application data. This does not mean that you need an overly bureaucratic process or

[19] Group Policy Website. URL: http://www.microsoft.com/windowsserver2003/technologies/management/grouppolicy/default.mspx
[20] Mar-Elia, Darren.
[21] "Group Policy Settings Reference for .adm files included with Windows XP Professional Service Pack 2."

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

that expensive tools need to be purchased, but some thought should be given to what level of control and structure provide the greatest benefits.

Versioning and Documentation

At the core of change and configuration management is saving versions of the GPO data and documenting the changes. Each change applied to a GPO should be documented (requests and implementation, dates of change, and which person performed the change). Many large organizations have some software product that is used for either change requests (e.g. Remedy) or change logging but simple mechanisms such as spreadsheets or paper and pencil are better than nothing.

Third-party products such as FullArmor's FAZAM 2000 (resold as NetIQ Group Policy Administrator) provide features to save administrator changes in a relational database along with change comments, much like source control configuration management products. The advantage is that the same product used to apply changes is also used to document and save versions, providing a more natural and optimized workflow than manual methods such as spreadsheet logging or separate Helpdesk products. Products that do provide this type of versioning functionality typically provide easy means to rollback to previous versions, as well as compare differences among versions.

Backup/Restore - Disaster Recovery

Regular backup of GPO data is crucial to disaster recovery, as well as ongoing change management. In the worst case, if a mistake occurs, a backup can serve as a way to go back to a better or well-known state. Backups are better suited for DR as opposed to rollback of changes during development because of the frequency of backups.

It is better to perform GPO-specific backups rather than rely on full system backups of the domain controller (which would include both AD and SYSVOL data stores) since a full system restore is not very granular and will restore other state that may have unintended side effects. In addition, the GPO state may be inconsistent in a full system restore depending upon when the backup was performed.

Backups can be performed automatically via scripts (GPMC, FullArmor FAZAM 2000 are all scriptable) and can be scheduled to occur regularly.

Treat backups as seriously as any other crucial data in the enterprise and include procedures to validate backups by checking random, selective restores.

Change Management

Change management typically involves a broader workflow and process among multiple users and roles. Defining who is responsible for which parts of daily GPO management (specification, change requests, design, implementation, test, rollout) as well as support functions such as backup/restore is important.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Decide which tools and procedures are required for change request/tracking as well as communication among the various users (e.g. manual email, change product generated alerts, etc.).

The best approach will depend on the organization and its existing people and processes. Home-grown tools and processes can be effective, if implemented clearly with all parties. FullArmor's FAZAM 2000 provides abilities to define different roles and permissions, as well as provides automatic email alerting, for the different users involved.

Auditing Trails

User-entered documentation of changes is good, but may not be enough because comments may be omitted or be incomplete. Having a more formal and automatic auditing of user actions is valuable for accountability, troubleshooting, and to ensure a base-level of documentation regardless of user actions. FullArmor's FAZAM 2000 provides an ability to log user actions in the Windows Application Log as one way to automatically create an audit trail.

Validation and Consistency Checks

Many users focus on the primary process of creating and deploying changes, while ignoring the secondary processes of troubleshooting, support, and incident-handling. We've seen that the Group Policy infrastructure can be very complicated, leading to potential security risks. While change management controls can help to minimize errors, having a good process for validation and consistency checks can help reduce a great deal of downstream wasted time and money by catching errors early.

The Windows Resource Kits include various command-line tools to check on the consistency of GPOs across domain controllers to help identify version skew due to replication errors (gpotool.exe).

There are also command-line utilities (gpresult.exe) RSoP reporting and RSoP logging diagnostics in GPMC or third-party tools provide an ability to check what settings should apply to a user/computer as well as what effective settings actually did apply on the end-computer.

More expensive monitoring solutions such as the AD Management Pack for MOM or other agent-based technologies can be used to check on errors in the AD infrastructure, such as replication problems. Since FRS problems have occurred in the past with large customers, specific replication-monitoring tools can also be deployed, such as Microsoft's Ultrasound (free).

Related Security Topics

All of the above topics relate to general security issues and concerns. Part of securing any environment involves minimizing mistakes from occurring (change management) and recovering from exploits (incident handling, backup/restore).

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Ideal Solutions

Rather than providing more complexity on top of a complicated infrastructure, ultimately the best solution would be for Microsoft to simplify the architecture and design of Group Policy without sacrificing functionality. The data storage implementation of Group Policy should be revamped in the next major operating system release (e.g. Longhorn or Blackcomb), which would make it a much more reliable infrastructure. This could involve storing all GPO data in AD, which would get rid of the corruption problems of FRS. A cleaner abstraction layer for all GPO read/write operations such as LDAP or ADSI would help to minimize problems in writing GPO data (today, GPO administration tools need to write multiple files to the SYSVOL share). If an intermediary service were provided to arbitrate all reads/writes, GPO-specific auditing could be provided. Today, it is burden of tool developers to provide auditing, which leads to complicated, non-standard and inconsistent solutions. However, changing the architecture so fundamentally would require today's GPO administration tools to be modified and present messy problems for mixed Windows environments (Windows 2000/2003/XP and the newer Windows OS) in terms of compatibility.

3.4. Vulnerability Scans and Validation/Health Checks

Validation checks are not just useful for checking that changes are appropriately applied, they can also be leveraged in a proactive manner to assess and root-out risk. By applying similar validation checks (on replication consistency of data and ACLs, on ACL settings, on Group Policy settings across forests), organizations can identify misconfigurations or mistakes before they affect users.

At the minimum, users should consider GPMC scripting or third-party product scripting, combined with ADSI VBScript to check on the state of the AD and Group Policy environment.

3.5. Disaster Recovery

The DR plan should be modified to include Group Policy, specifically. Backup and restores should be performed daily or as frequently as possible. Scripting in GPMC or third-party tools can help automate this process for all GPOs in the environment. Validation of the backups should also be done through at least some spot-checks, if not automatically by a script.

3.6. Delegation/ACL Management

Some AD products exist to manage ACLs in a more scalable manner, but even without these solutions, utilize the GPO ACL reports found in GPMC and third-party tools. Review these on a regular basis to ensure that nothing strange is observed.

You can modify the default security descriptor in the AD schema. This may reduce possible security breaches where ACLs are by default too broad.

Finally, having a scheduled script check for ACL consistency can minimize downstream effects of corrupt GPOs.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

3.7. Troubleshooting

Identification

Proper incident identification starts with auditing as described in section 3.8. In the absence of any GPO auditing information, an administrator generally will wait to hear from users or the internal IT Help Desk.

Analysis

Several techniques and tools are available for analysis of the situation depending upon the context. The primary symptom tends to be that a policy setting is not applying as expected to particular users/computers. The goal is to identify and isolate the cause to:

- client processing
- server processing
- incorrect settings

RSoP can be performed to determine if appropriate settings have reached a particular DC. Client diagnostics can be performed to verify whether policy settings have been applied correctly to the client. Note that RSoP Logging Mode in GPMC relies on newer client OSes (Windows 2003/XP); however remotely looking at a Windows 2000 event log can help identify errors in the Group Policy download process. These two techniques help isolate which part of the data flow has broken down (server or client processing).

If RSoP results indicate that the wrong settings are showing at the DC, then the settings can be double-checked by utilizing basic settings reports in GPO administration tools, advanced comparison/difference reports in third-party Group Policy administration tools such as FullArmor's FAZAM 2000, by checking change records in the change management tool/process, and checking any change audit logs kept.

If the settings appear correct, replication problems can be analyzed by checking the same GPO across different DCs for consistent settings and ACLs. This can be done using gpotool.exe from the Windows Resource Kit or by utilizing GPO settings reports from different DCs.

Response

Remediating GPO settings or replication problems usually means reapplying the correct policy setting, ACL, or AD attribute to a DC, and forcing a refresh on the client using gpupdate.exe or secedit.exe.

Related Security Topics

The techniques and tools used for troubleshooting are similar to those used for general GPO incident handling, whether it be for disaster recovery or exploit detection.

3.8. Auditing and Monitoring

Although native Windows auditing for Group Policy is weak, there are alternative approaches that should be considered.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Microsoft Audit Collection System (ACS)

The Microsoft Audit Collection System is currently in release candidate and likely to be released coincident with Windows 2003 sp1 in late 2004 or early 2005. It provides extremely scalable and secure centralized collection of Windows audit events, including secure encryption of events, separate audit roles to control access, a light-weight footprint, and ability to manage collect audit events from thousands of nodes with one ACS server and SQL Server database. ACS was designed to prevent attackers from erasing their tracks since the audit log data is immediately and securely sent to a central database—privileged admin users do not have the ability to intercept this data stream at any point. Some of the exciting capabilities include its ability to provide real-time subscriptions to the centralized data feed, its lightweight footprint, and that it will likely be built into Longhorn.

Third-Party Approaches

Historically, traditional approaches have included placing an agent on the domain controller in order to detect changes to certain objects and provide in-depth information. To date, there have been no good third-party solutions based on deploying agents to DCs, most likely because the OS support for auditing makes it difficult to gather useful information and because the impact on DCs can be severe enough that customers resist this deployment architecture.

A different approach, specific to GPO auditing was released by FullArmor Corporation in 2003—FAZAM Auditing (sold as NetIQ Group Policy Guardian) provides detailed change reports on any GPO change, storing old and new values in a SQL Server database. The information includes the exact GPO section and setting, old value, new value and provides much higher value than the 560/565/566 Windows audit events.

Ideal Solutions

If Microsoft ACS is built into Longhorn, then supporting reliable, centralized OS auditing will be much easier. This support will help detect and audit GPO changes, even though the event stream may still be cryptic and reflect the flawed data storage implementation of GPOs. Vendors will be able to focus more on adding advanced correlation and analysis on the event stream itself as opposed to the process of collecting events.

Related Security Topics

GPO auditing poses the same challenges and issues as security auditing. Having reliable, integral audit logs is a requirement for exploit detection. Knowledgeable attackers will attempt to cover their tracks by modifying audit logs.

3.9. Incremental Approach

Ultimately, Group Policy will never be simple due to its scope and magnitude in both functionality and scalability. However, by using an incremental approach to implementation, continuous improvement can be achieved while minimizing risk. An organization does not have to implement every setting in a GPO—settings can be learned and implemented piece-meal. Best practices can be implemented and refined in

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

small, iterative steps. Smaller steps means smaller missteps, and the good thing about Group Policy is that it can be easily divided into manageable pieces.

4. Conclusion

Over the next few years, knowledge of Group Policy will continue to grow, and Group Policy will be used to manage more and more functionality in the Windows enterprise. However, managing Group Policy on any scale will still remain a challenge.

Group Policy has unique security concerns due to its design and implementation, as well as its far-reaching functionality and content. Many of the security risks of Group Policy relate to its complicated data storage mechanism, its typically world-readable settings, and the reality that truly scalable architectures are complicated.

Ideally, several changes occur over the next few years:

- GPOs stored only in AD, not SYSVOL
- Better abstraction layer for reading and writing GPOs
- Better GPO ACL abstraction is provided
- GPO auditing provided in the operating system
- More best practices codified

In the meantime, a disciplined, iterative approach to Group Policy management can provide continual improvement and improve the security of the broader Active Directory environment. This will require a lot of hard work with a focus on better change management procedures, ability to audit changes, and supporting scripts and tools to continually validate and check on consistency in the environment.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

References

3APA3A@security.nnov.ru. “SECURITY.NNOV: file locking and security (group policy DoS on Windows 2000 domain).” 1 Dec 2001. URL: http://cert.uni-stuttgart.de/archive/bugtraq/2001/12/msg00080.html.

“Description of the FRS Replication Protocol, Notification and Schedule for DFS Content.” 20 Nov 2003. URL: http://support.microsoft.com/?kbid=220938.

“File Replication Service.” Part 3 Enterprise Technologies. URL: http://www.microsoft.com/windows2000/techinfo/reskit/samplechapters/dsdh/DSDH_FRS.doc.

"FRS Does Not Replicate Files or Folders If the System Account Does Not Have Full Control of the Directory Tree." Revision 2.1. 4 Nov 2003. URL: http://support.microsoft.com/default.aspx?kbid=319473.

“Group Policy Settings Reference for .adm files included with Windows XP Professional Service Pack 2.” Revision 1.1. 31 Aug 2004. URL: http://www.microsoft.com/downloads/details.aspx?FamilyID=7821c32f-da15-438d-8e48-45915cd2bc14&displaylang=en.

“Group Policy Collection.” URL: http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/techref/en-us/Default.asp?url=/Resources/Documentation/windowsserv/2003/all/techref/en-us/w2k3tr_gp_over.asp.

Group Policy Website. 2003-2004. URL: http://www.microsoft.com/windowsserver2003/technologies/management/grouppolicy/default.mspx.

“How to Restrict FRS Replication Traffic to a Specific Static Port.” Revision 2.0. 20 Oct 2003. URL: http://support.microsoft.com/?kbid=319553.

“How to Configure a Firewall for Domains and Trusts.” Revision 6.0. 5 Aug 2004. URL: http://support.microsoft.com/default.aspx?scid=kb;EN-US;179442.

"Improvements in the Post-Service Pack 3 Release of Ntfrs.exe.” Revision 2.2. 30 Jul 2003. URL: http://support.microsoft.com/default.aspx?kbid=811217.

"Improvements in the Post-SP2 Release of Ntfrs.exe That Is Packaged with an Updated Ntfs.sys Driver." Revision 2.2. 24 Mar 2004. URL: http://support.microsoft.com/default.aspx?kbid=321557.

"Issues that are fixed in the post-Service Pack 3 release of Ntfrs.exe." Revision 8.0. 5 May 2004. URL: http://support.microsoft.com/default.aspx?kbid=811370.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Kington, Tristan. “More on Sasser, IPSec Firewalls, and SMB.” 6 May 2004. URL: http://blogs.msdn.com/tristank/archive/2004/05/06/126963.aspx.

Mar-Elia, Darren. “The Definitive Guide to Windows 2000 Group Policy.” www.realtimepublishers.com, 2000.

“Microsoft Security Bulletin MS01-036: Function Exposed via LDAP over SSL Could Enable Passwords to be Changed." 28 Feb 2003. URL: http://www.microsoft.com/technet/security/bulletin/MS01-036.mspx.

“Microsoft Security Bulletin MS02-070: Flaw in SMB Signing Could Enable Group Policy to be Modified (329170).” 22 Jan 2003. URL: http://www.microsoft.com/technet/security/bulletin/MS02-070.mspx.

“Microsoft Windows 2000 Group Policy Evasion Vulnerability.” 5 Dec 2001. URL: http://www.securityfocus.com/bid/4438/discussion/.

“Microsoft Security Bulletin MS02-016: Opening Group Policy Files for Exclusive Read Blocks Policy Application (Q318593).” 9 May 2003. URL: http://www.microsoft.com/technet/security/bulletin/MS02-016.mspx.

"Ntfrs.exe Does Not Clean Up the Staging Folders on Members with No Outbound Partners in Windows 2000." Revision 3.1. 6 Nov 2003. URL: http://support.microsoft.com/default.aspx?kbid=322141.

“PSS Security Response Team Alert - Sasser Worm and Variants.” 12 May 2004. URL: http://www.microsoft.com/technet/security/alerts/sasser.mspx.

Sullivan, Aaron. “An Audit of Active Directory Security, Part Five: A Theoretical Attack on the Multi-Master Replication Scheme in a AD-Enabled Network.” 15 Jan 2002. URL: http://www.securityfocus.com/infocus/1535.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.