

Technical White Paper



Microsoft® IT
Showcase

Group Policy Object Infrastructure Management at Microsoft

Design, Troubleshooting, and Lifecycle
Management

Technical White Paper

Published: August 2007

Microsoft®

CONTENTS

Executive Summary	4
Introduction	4
The Microsoft Environment	6
Distributed, Large, Multi-Forest Deployment	6
Large Number of Group Policy Objects	7
Group Policy Supports Business Policies	8
Group Policy at Microsoft	9
Microsoft GPO Challenges	9
Group Policy: A Flexible and Extremely Powerful Tool	11
Group Policy Extensions	12
Group Policy Editor (GPEdit)	13
Individual Policy Settings	13
Target Container	14
Security Filtering and WMI Filters	14
Client-Side Extensions and GPO Service	15
Group Policy Management Console	15
Resultant Set of Policies Management Console	15
Replication Services for Group Policy Objects	16
GPO Design Strategies	17
Use Cross-Enterprise GPOs	17
Use Many Small GPOs	18
Plan for Potential Failed GPO Replication	19
Target Different Policy Settings to Different Groups	20
Link GPOs to Appropriate Containers	20
Filter by Security Group or WMI Queries	21
Consistently Name and Track GPOs	21
Evaluate Methods for Software Installation and Script Execution	22
Plan for Computers Leaving a Domain	22
Limit GPO Deployment Personnel	23
Group Policy Workflow Management	24
Roles and Responsibilities	24

GPO Change Management Process	25
Troubleshooting GPO Issues	30
Conflicting Policies	30
Replication Issues	30
Slow Link Issues	31
Best Practices	32
Conclusion	33
For More Information	34

Situation

Group Policy is a powerful technology for managing security and configurations of computers on a corporate network, allowing both broad global settings and finely tuned, targeted settings for specific classes of computers. Without a clear design strategy and management process, Group Policy can become complex and cause conflicts that could lead to loss of productivity.

Solution

Microsoft IT has developed a consistent Group Policy design practice and applied the Microsoft® Operations Framework (MOF) to manage more than 900 Group Policy Objects that are applied to 20 domains in six forests.

Benefits

- Reduced downtime due to conflicting Group Policy Objects.
- Increased productivity because classes of computers can be centrally configured across the enterprise.
- More consistent security measures, applied uniformly across the corporate network.

Products & Technologies

- Microsoft Group Policy
- Microsoft Active Directory
- Microsoft Group Policy Editor (GPEdit)
- Microsoft Group Policy Management Console (GPMC)

EXECUTIVE SUMMARY

The Microsoft Information Technology organization (known as Microsoft IT) uses Group Policy Objects (GPOs) to create user and computer policies that are deployed using the Active Directory® service. Group Policy and Active Directory work together to provide an effective framework for enforcing a wide range of security and configuration policies.

This paper is based on the experience and recommendations of Microsoft IT as an early adopter. It is not intended to serve as a procedural guide. Each enterprise environment has unique circumstances; therefore, each organization should adapt the plans and lessons learned that are described in this paper to meet its specific needs.

The purpose of this paper is to illustrate the experience of Microsoft IT in designing and managing GPOs. That experience shows that a robust, carefully planned change management system based on the Microsoft® Operations Framework (MOF) contributes to a highly manageable Group Policy infrastructure. Microsoft IT has developed a formal management process for testing and implementing GPOs. The result is a Group Policy framework that ultimately makes business operations more consistent and assists with regulatory compliance. The process flow has reduced disruptions, increased stability, and reduced human error.

This paper is written for enterprise technical decision makers, IT implementers, and architects who want more information about managing GPOs in a large corporate network. This paper does not include a detailed discussion of other management applications also in use at Microsoft, such as Systems Management Server 2003 (SMS 2003), Microsoft Operations Manager 2005 (MOM 2005), or other internally developed tools. For white papers with information about those applications, please visit <http://www.microsoft.com/technet/itshowcase>.

The essential enabling technologies described in this paper run on the Microsoft® Windows Server™ 2003 operating system—part of the Microsoft Windows Server System™ integrated server software—and the Microsoft Windows® XP Professional operating system with Service Pack 2. However, most of the technologies were developed when the infrastructure was based on the Microsoft Windows 2000 Server operating system, and they can be implemented on Windows 2000 Server SP 4 and Windows XP. Microsoft IT uses Group Policy to manage both servers and workstations throughout its corporate network. All of the technologies and deployments continue to mature, based on evolving security requirements, future strategic plans, and product-testing and validation requirements.

Note: For security reasons, the sample names of forests, domains, internal resources, organizations, and internally developed security file names used in this paper do not represent real resource names used within Microsoft and are for illustration purposes only.

INTRODUCTION

Securing and managing a corporate network can involve deploying many layers of technologies and processes. Likewise, establishing a controlled environment for financial or business systems generally involves setting up multiple systems that provide crosschecking of critical controls.

Microsoft IT uses several different systems to manage computers on the corporate network. SMS 2003 is used to roll out software updates, deploy antivirus software, and perform other tasks. MOM 2005 handles monitoring and security alerting. This paper focuses on configuration management delivered through a third system, the Group Policy functionality built into Active Directory in Windows 2000 Server and Windows Server 2003. One of the big benefits of Group Policy over the other technologies is that it is a common, unified framework for managing business policies across the various parts of the operating system and in many server and workstation applications.

The technical elements covered in this white paper include:

- **Microsoft IT environment.** An overview of the specific challenges and considerations of the corporate network that influence deployment decisions.
- **Technical overview of Group Policy.** Background information for the technology described in this white paper.
- **Description of the Group Policy implementation at Microsoft.** A look at GPO design considerations and the choices Microsoft IT made while developing the GPO infrastructure.
- **GPO workflow management.** How Microsoft IT uses the MOF to manage change requests for GPOs within the company.
- **Basic troubleshooting steps for Group Policy.** Steps to help resolve issues arising from GPO deployment.
- **Known issues and best practices.** Specific problems encountered and lessons learned while planning and deploying policies and settings across the enterprise.

Group Policy provides a powerful set of tools for managing many aspects of an enterprise network. It is fast to deploy, can scale up to the largest deployments, and can accommodate specific needs of small groups, all at the same time. However, the comprehensive nature of Group Policy also can lead to confusion about the best way to make use of it.

Every organization has a unique set of needs, priorities, and environmental factors, all of which lead to different network design strategies. The goal of this white paper is to provide insight into the decisions that Microsoft IT made while deploying Group Policy across its corporate network and to illustrate how it manages changes on a day-to-day basis.

THE MICROSOFT ENVIRONMENT

Microsoft IT has a variety of responsibilities. Its primary role is to provide IT services ranging from end-user support and telecommunications management to server and network operations to architectural design of future service offerings.

Microsoft operates in an extremely active and challenging security environment. Challenges include the following:

- Each month, Microsoft experiences approximately 100,000 intrusion attempts.
- Each month, Microsoft probes, scans, and quarantines more than 150,000 virus-infected e-mail messages.
- Microsoft has unique IT environments for product development, testing, and support, which require special security.

Group Policy provides an effective framework for managing and enforcing policies that help keep the corporate network secure, while providing the flexibility necessary to support a challenging environment.

Distributed, Large, Multi-Forest Deployment

Microsoft IT manages more than 300,000 computers and devices, serving more than 100,000 user and test accounts in more than 20 Active Directory domains in six Active Directory forests that are spread across more than 400 locations around the world. Microsoft IT supports 56,000 employees, 7,000 contractors, and 28,000 vendors, providing corporate network access 24 hours a day, seven days a week.

Many aspects of the Microsoft work environment are not typical of a large-scale enterprise. Some of the unique aspects of the desktop environment at Microsoft include:

- **Multiple computers per user.** Many Microsoft employees have two or more desktop computers in their offices. Often, one computer has a specific configuration, dedicating it to performing a given task such as developing Microsoft Office products, while another is reserved for standard network and e-mail access. The user may purposely have systems running different versions of Windows or Office to test for application compatibilities. Microsoft employees also use Microsoft Virtual PC 2004 to emulate several operating systems on one desktop computer.
- **Diverse desktop implementations.** The Microsoft staff represents all levels of technical computer skills within the company. Many employees are highly technology-literate and routinely explore the limits of the tools available to them. Many desktop computers have unique capabilities and software characteristics.
- **Frequently rebuilt computers.** To test software functionality, often many employees completely rebuild their systems, sometimes on a daily basis. Approximately 5,000 computers per month are rebuilt in the data center at the Redmond, Washington headquarters alone.
- **Diverse mix of approved software versions.** When Microsoft releases a new version of an application, departments across the enterprise—such as product development, product support, and sales—do not unilaterally install the software immediately. Like many other enterprises, departments and business units within Microsoft have a generous amount of latitude to choose the software versions that best fit their work models. For example, some departments run older versions of software to test version

interactions and backward compatibility. Development groups deploy multiple—sometimes up to six—builds of an operating system or an application into the desktop environment before release to manufacturing. Some testers install new software builds on a daily basis.

Microsoft Forest Structure

In Active Directory, a forest represents a security boundary. Each forest has its own Active Directory structure, and it can be effectively isolated from other forests.

Large enterprises might implement a multi-forest structure when there is a strong need for isolating groups of administrators from each other. Often multi-forest structures arise from mergers and acquired companies. The main drawback to having multiple forests is additional administrative cost involved in managing inter-forest trust relationships.

Microsoft IT manages six separate forests, each meeting different needs. There is a forest for testing new beta versions of Active Directory forest structures, and some forests are used strictly in labs. Other forests provide the ability to segregate external vendors from the main corporate forest and to contain external, publicly accessible servers. There are Active Directory forests on the corporate network that are managed by staff other than Microsoft IT (for example, the MSN and MSNBC organizations). Finally, a number of untrusted forests exist on the corporate network, but those are used for test purposes only and generally do not connect to IT-managed forests.

Microsoft Domain Structure

The pre-release (test) forests each have two or three domains, to provide a multitude of testing scenarios. None of the test forests is considered trusted. The main production forest has nine domains that are separated into geographic regions in order to keep replication as local as possible while maintaining an overall domain structure that is reasonable to manage.

Users and computers are put in separate organizational units (OUs). In production domains, each has 7 to 30 domain controllers (DCs). Sites with slower network links may have their own DC.

Microsoft gradually has been consolidating sites and domains, eliminating DCs and infrastructure servers, which has greatly reduced replication issues. Microsoft IT has found that the less complicated the forest and domain structure, the easier the entire network is to administer.

The Microsoft Identity Management Team, part of the Microsoft IT Information Security organization, is responsible for the Active Directory structure across the entire enterprise and for Active Directory–based identity and access management.

Organizational Units

A comprehensive OU structure has been deployed for all Microsoft IT data center servers. An effort is currently underway to create OUs, as appropriate, to better delegate certain tasks to local administrators. This effort is in its early stages and not yet fully deployed.

Large Number of Group Policy Objects

The Identity Management Team manages more than 900 individual Group Policy Objects and, more importantly, manages the global GPO approval and deployment process.

If the GPOs are not carefully managed, they can overlap and cause conflicting policies to be applied. Because individual settings in one GPO can contradict the values for the same setting in a different GPO, it is important to carefully track which GPOs are applied to which computers and users. When moving a computer to a different forest or moving a user to a different Active Directory organizational unit, care must be taken to prevent conflicting settings.

For example, Microsoft has a set of approximately 65 locked-down, kiosk-style computers in the lobbies of many of its buildings that employees use to check e-mail, access their workstations using Terminal Services, or perform other limited tasks. During one GPO deployment, these kiosks processed a Group Policy setting that effectively disabled a network configuration and thus kept the kiosks off the corporate network. Microsoft IT had to dispatch service technicians to every computer to make them operational again.

Another example of a GPO that interfered with business operations was the Service Pack 2 update to the Microsoft Windows XP Professional operating system. When Windows XP SP 2 was deployed internally at Microsoft, the Windows Firewall was automatically enabled, configured, and enforced by a GPO. Some of the policy settings deployed prevented testing groups from remotely managing their Windows XP SP2 computers. A special “firewall configuration” GPO had to be deployed to allow the relevant testing groups to remotely manage their Windows XP SP2 computers.

Centralizing the efforts of managing GPOs at Microsoft has lessened the potentially disruptive impact of GPO changes and has better aligned the technical network environment with the written business policies.

Group Policy Supports Business Policies

The Identity Management Team handles the approval and deployment of all GPOs at Microsoft, as well as the workflow for updating them. The underlying GPO policies come from a variety of groups, such as Corporate Security, Finance, Law and Corporate Affairs, and various business units or product groups within Microsoft.

For example, the Law and Corporate Affairs team might determine the minimum password length—required for user accounts—that complies with the business guidelines in all countries where Microsoft has employees. A single Group Policy Object setting can be used to enforce this global requirement. Alternately, the Finance department might require that certain event log entries (such as attempted access failures) must be recorded on all data center servers. Again, a single Group Policy Object setting can ensure the global enablement of this control.

Before defining and deploying a GPO, the originating (requesting) group must identify the underlying business policy it wants to enforce. The originating group needs to specify which people or computers should receive the policy and what settings the group wants to apply. The originating group also must provide business justification for the change. Creating these policies is not explicitly an IT function; many requests come from groups that lack IT knowledge and experience in configuring or testing Group Policy settings, linking to Active Directory contexts, or filtering to specific security groups.

The Identity Management Team has developed a process to handle GPO requests based on the Microsoft Operations Framework. The process determines necessary policy settings, identifies the targets for each GPO, checks for conflicts with existing GPOs, requires

approval for all policy additions and updates, and communicates GPO updates with other affected groups before deployment.

This process is discussed in more detail later in this paper, in the section titled “Group Policy Workflow Management.”

Group Policy at Microsoft

For Microsoft IT, the main benefit of Group Policy is the ability to easily apply consistent settings across all domain-joined computers, enforcing corporate security requirements, written business policies, and compliance requirements.

Among other uses, Microsoft IT uses Group Policy:

- To control password policy and auditing.
- To specify event log settings for particular computers.
- To support compliance with regulations such as the Sarbanes-Oxley Act or the Health Insurance Portability and Accountability Act of 1996 (HIPAA).
- To create a trusted network segment of authenticated computers using IP Security (IPsec) and deny untrusted computers access to corporate resources.
- To enable and configure the Windows Firewall service.
- To deny all computers that are not in a particular domain access to the source code repositories.
- To test new desktop configurations.
- To provide specific configurations to servers, reducing administration costs.
- To ensure that the SMS 2003 client is installed and running upon logon.
- To enable the help desk to offer remote assistance to client computers.
- To publish a limited set of applications.

Some GPOs are applied across the company, while others define policies for small groups of computers or users.

One of the ways that Microsoft IT enforces domain membership is by deploying IPsec policies through Group Policy. Only computers that have the correct IPsec policy applied will be able to communicate with other computers on the domain.

Note: For more information about the deployment of IPsec on the Microsoft Corporate Network, see “Improving Security with Domain Isolation” on the IT Showcase Web site at <http://www.microsoft.com/technet/itsolutions/msit/security/ipsecdomisolwp.mspx>.

Microsoft GPO Challenges

Based on the existing systems in use at Microsoft and a desire to minimize the impact on users during GPO updates, Microsoft IT has developed the following goals for GPO changes:

- Prevent GPO edits from being made in the production environment of Active Directory— all modifications to GPOs first must be done in an isolated environment and tested before they are deployed to the production Active Directory environment.
- Minimize the number of personnel authorized to edit GPOs, delete GPOs, or modify the security settings for GPOs.

-
- Effectively manage the administrative (*.ADM) template files to account for the various software versions deployed on the corporate network.
 - Avoid using scripts to manage and report because SMS 2003 already provides that functionality.
 - Cease GPO-based software distribution because SMS 2003 already provides that functionality.
 - Craft GPOs to effectively link to site, domain, or OU contexts in Active Directory, or filter to appropriate security groups as needed, to reduce the dependencies on per-GPO Windows Management Interface (WMI) query-based filtering.

Aside from these goals, there are a number of challenges involved with managing a corporate environment using Group Policy:

- Creating and managing reference *.ADM files when there are a variety of operating systems and server software versions. In most enterprises, the latest versions of an *.ADM file will have settings that work across versions of an application or operating system, but at Microsoft there are many interim beta versions that may have changing policy settings.
- Managing GPO access and restricting it to a small group—technically, any domain administrator can create and apply a GPO.
- Aggregating event logs to help administrators detect unauthorized modifications to GPOs.

These challenges can be addressed by having a clear Group Policy change management process, a single group responsible for managing the process, and tools that help do the job.

GROUP POLICY: A FLEXIBLE AND EXTREMELY POWERFUL TOOL

Within Active Directory, Group Policy provides a powerful system for enforcing specific configuration settings for sets of users and computers based upon their individual sites, domains, or organizational units. It is important to design any powerful system with care and forethought and to carefully manage changes to the system.

Group Policy is comprised of several different parts:

- Administrative templates (*.ADM files)—these files define the possible settings for a configuration item, such as minimum password age or required computer startup script.
- The tools used to create, modify, or delete Group Policy Objects.
- Policy settings, stored individually or in combinations in a GPO—each setting may have one or more values (ENABLED/DISABLED/TRUE/FALSE/AUTOMATIC/MANUAL, etc.) that are configured as appropriate for the business policy.
- The publishing point for each GPO, also known as the link information, indicating the site, domain, or OU to which a GPO is applied.
- The security filtering for each GPO, which enables an administrator to target each GPO to support specific security principles. The target can be a set of specific user or computer objects, a security group, or a well-known security principle, such as “Authenticated Users.”

Additional tools and service components for Group Policy include:

- The Group Policy Management Console (GPMC), a GPO management snap-in for the standard Microsoft Management Console (MMC).
- The Resultant Set of Policies (RSOP) tool, a GPO investigative snap-in for MMC.
- Gpresult.exe—a command-line GPO investigative tool.
- The Active Directory replication, for the replication of data stored for GPOs within Active Directory.

- The File Replication Service (FRS), for the replication of data stored for GPOs within the /Sysvol share.

Active Directory Forest

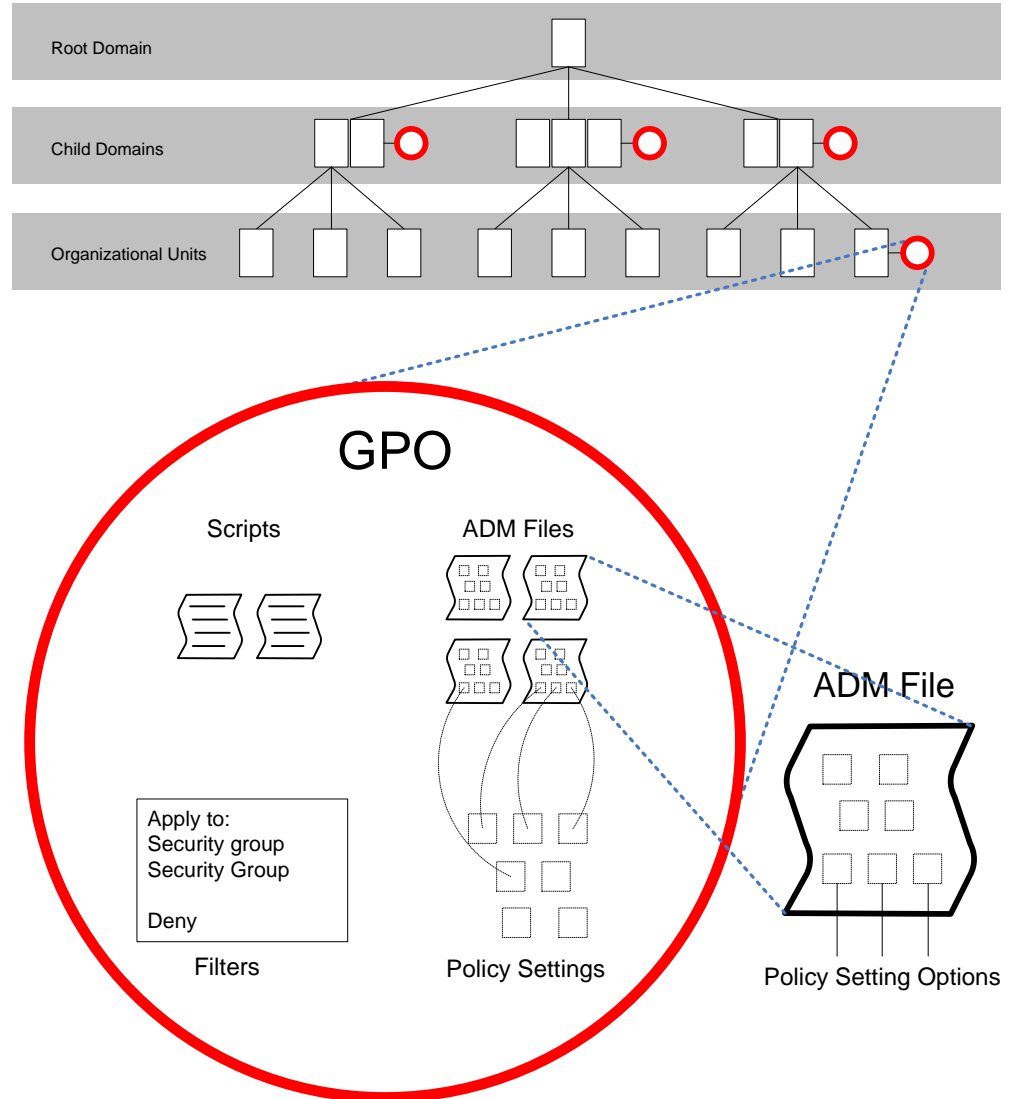


Figure 1. Relationship of various parts of Group Policy

Group Policy Extensions

Group Policy defines a number of extensions for managing individual policy settings. A GPO may specify settings for any of the following extensions:

- **Security.** The security extension contains policy settings for security-related settings, although these also can be defined in an administrative template.
- **Software installation.** The software installation extension can publish or force installations of various software applications.

-
- **Internet Explorer Maintenance.** The Internet Explorer maintenance extension provides a means for configuring everything from user interface settings to connection settings within Internet Explorer. These also can be defined in administrative templates.
 - **Scripts.** The scripts extension provides settings related to logon/logoff and startup/shutdown scripts deployed by Group Policy. It also runs the scripts included in the GPO at the appropriate time.
 - **Administrative templates.** Administrative templates provide complete customizability of Group Policy to meet the needs of the organization. Nearly any registry setting associated with a user or computer can be defined in an administrative template and made available as a policy setting. However, the templates shipped with Microsoft products are in a secure place in the registry and do not overwrite user preferences.

Administrative templates define the possible values for a policy setting, the registry location to use, the format and possible values for the setting, and default values, if appropriate. Developers can create administrative templates to go with their applications, and administrators can manage them using Group Policy.

Administrators can import an administrative template on a computer that is not even running the corresponding service, and they can create a GPO using options in the administrative template. For example, by importing an administrative template for Microsoft Office Word 2003, the administrator can create policy settings for Word 2003 without having it installed on the local computer. The Identity Management Team uses this technique to create many GPOs for applications that it never installs.

Group Policy Editor (GPEdit)

GPEdit is the main tool for editing a single GPO.

GPEdit provides an interface to manage the different parts of a GPO. A GPO can contain one or more extensions that define which settings are available. It also can contain any number of individual policy settings.

Individual Policy Settings

A GPO can have any number of individual settings that are set from the available policy settings. At Microsoft, GPOs tend to contain a small number of individual settings, typically 5 to 20. The Identity Management Team has found it easier to manage a large number of GPOs, each with a small group of settings, than to manage a few GPOs with a large number of settings. This approach maximizes flexibility in defining who gets a set of settings and minimizes the need for frequent changes of core policies.

There are approximately 1,950 individual policy settings available with the release of Windows Server 2003 SP1. Microsoft IT does not track or use all of these, but it does use policy settings available in other products. In all, the Identity Management Team tracks approximately 1,400 individual policy settings, spread across slightly more than 900 individual GPOs.

Examples of individual policy settings include:

- Require all passwords to be a minimum number of characters.
- Require that all passwords have complex formats, including characters and numbers.
- Pre-populate printer search location text.

-
- At user logon to the workstation, run a program that will launch the antivirus client inspector application.

Each of these is an individual policy setting, but they can all be grouped into a single GPO.

Target Container

A GPO is applied by linking the GPO to a target container defined in Active Directory, which may be:

- **A domain.** Many smaller businesses have a single domain for the entire business. Microsoft has split its corporate network into 20 domains, divided into specific business units or geographical regions around the world.
- **Any organizational unit defined in Active Directory.** Users or computers may be a member of a specific OU, such as Finance or Windows Development. The hierarchy of OUs is completely arbitrary, based on the Active Directory deployment of a particular network. OUs are used for computers within the Microsoft IT infrastructure, but not widely deployed for users. A separate project is underway to optimize the OU structure. The OU hierarchy should align with the administrative model of the enterprise.
- **A site.** A site generally corresponds to a block of network addresses or subnets that are typically of a consistent bandwidth. Most sites consist of all computers in a physical building, floor, wing, or group of buildings.

Security Filtering and WMI Filters

Any Group Policy Object can be filtered to apply to a specific set of computers or users by using a security filter or WMI query. The security filter may include or exclude users, computers, groups, or well-known security principles, and it can take the form of access control lists for fine-tuning to which computers or users a specific GPO is applied.

Filter lists can be useful for different purposes:

- Allowing only a specially authorized group to gain access to high-value resources.
- Applying a particular configuration only to computers running a specific version of an application via the use of a WMI filter.
- Testing major GPO changes on small security groups before wider deployment.

Filter lists can be defined in the GPO using GPMC.

While filter lists provide a great deal of flexibility, they also can consume many computer resources while processing if they use WMI filters. It is a good practice to group related sets of policy settings into GPOs that target the same users or computers and to use WMI filters sparingly.

For the most part, Microsoft IT has avoided using WMI filters. One instance where they were used was during deployment of IPsec for servers. Because each IPsec connection adds processing overhead, the IPsec deployment team wanted to install special LAN adapters optimized for IPsec on high-traffic servers before requiring those connections to be secured. The deployment team set up the IPsec GPO to have the correct settings and then used a WMI filter to prevent the settings from being applied unless the new LAN adapter was installed. Once team members had completed the rollout and all computers had been restarted, they removed the WMI filter.

Client-Side Extensions and GPO Service

The administrator applies the GPO in Active Directory. From there, each computer applies GPOs using its client-side extension on the following basis:

- When the computer joins the domain—either when it starts or when it connects to the network—it connects to Active Directory and looks for GPOs applied to the site, domain, and OU. Security group filtering happens on the client, after downloading all of the applicable GPOs.
- When a user logs on, the same process occurs, except with GPOs that are based on user templates instead of computer templates.
- At a random interval between 90 and 120 minutes (random to reduce load on the domain controllers), each client refreshes its GPO list, automatically getting any changed policy settings and new policies or removing deleted policy settings. These refresh times are configurable. Certain GPO settings, such as software installation and publishing settings, are only applied or refreshed during computer startup or user logon.
- DCs have their GPO lists refreshed by default every five minutes. These refresh times are configurable.

In Windows 2000, GPOs are processed synchronously—that is, each GPO is applied during the startup or logon sequence. In Windows XP, GPOs that install software, run scripts, or perform folder redirection are processed synchronously, but other GPOs by default are applied asynchronously, allowing the startup or logon process to complete before GPOs are fully processed. When a GPO is applied asynchronously, it is handled like a periodic refresh.

If a user disconnects from the network, the computer continues to use the previously applied settings, though startup and logon scripts only run when the computer is connected to the network.

The Group Policy engine (service) component is available on Active Directory DCs.

Group Policy Management Console

GPMC is an MMC snap-in used for managing GPOs. Administrators view, create, import, export, save, link, filter, and apply GPOs using GPMC. This interface can restore previous versions of a GPO if the administrator saved them first.

GPMC provides a summary view of GPOs in use in Active Directory, and it enables management of those GPOs. One of the great values of GPMC as a reporting tool is that it allows a user with read-only access to a GPO to view a report of the settings contained within a GPO. This feature can be used to give lower-tier support groups the ability to review GPO settings—in order to assist in troubleshooting—without giving them the ability to edit the GPO.

The GPMC installation folder also contains command-line management tools (scripts) that are useful for GPO analysis, archiving, bulk modification of GPOs, and reporting.

Resultant Set of Policies Management Console

The RSoP tool is an MMC snap-in for GPO management that provides an investigative tool to help users understand the cumulative set of policy objects that will be applied, in order, to a target computer and user.

RSoP is an effective tool for conducting “what-if” GPO scenarios for sample computer and user accounts.

RSoP can be run locally on a specific computer to generate the live resultant set of policy data for the computer and the user who is currently logged on, which makes it a useful troubleshooting tool.

Replication Services for Group Policy Objects

Group Policy Objects rely upon FRS for file synchronization of data stored on the /Sysvol share between each domain controller in each Active Directory domain. Thus, the health of FRS, which can be determined with the Ultrasound FRS monitoring tool, affects the health of Group Policy. If FRS is not replicating files properly, users can have a variety of hard-to-identify problems related to Group Policy.

Note: *The Ultrasound FRS monitoring tool is available online at <http://www.microsoft.com/frs>.*

Group Policy Objects also rely upon Active Directory replication for the synchronization of data stored within Active Directory between each domain controller in each Active Directory domain. It is important to monitor both FRS and Active Directory replication, since both can affect the health of Group Policy.

GPO DESIGN STRATEGIES

There is a wide variety of methods for designing Group Policy. Early documentation for Group Policy suggested it was better to put as many settings as possible in a single GPO to minimize the number of GPOs a client would have to download when connecting to the domain. In practice, however, the number of GPOs does not make a substantial difference in time it takes to log on—but the number of individual settings does have an impact.

There are several key design questions that must be considered when creating a Group Policy design strategy, including:

- What business policies need to be enforced with Group Policy?
- Is it better to have a few GPOs with many settings or many GPOs with few settings?
- How can different groups within a domain get different policy settings?
- Should GPOs be linked to a domain, an organizational unit, or a site?
- What is the best use for security group filtering or WMI filtering?
- How should GPOs be named and tracked?
- Should GPOs be used to install software and run scripts?
- What happens when a computer moves to another domain?
- Who has access to make changes to GPOs in Active Directory?

The answers to these questions will vary between organizations. Microsoft has chosen to use a centralized IT structure to manage GPOs, designating the Identity Management Team as the owner of Active Directory and GPO deployment throughout the enterprise.

Use Cross-Enterprise GPOs

Having the same GPO settings deployed to domains across the IT-managed enterprise simplifies administration and provides a high degree of consistency and compliance to security standards. Specific GPOs deployed to all IT-managed domains include:

- Default domain policy, the setup security standards and basic policies for the domain.
- Default domain controllers policy, which applies the baseline security settings for domain controllers.
- Restricted groups, to provide local administrator rights for security auditors.
- Network segmentation, to allow computers that are joined to the domain to gain access to domain resources and to block access to non-domain-joined computers.
- Folder redirection, to redirect a local My Documents directory to a server.
- Managed Desktop, which provides various Windows components and the configuration for the Microsoft Office Outlook® 2003 messaging and collaboration client.
- Application Publishing, which enables a user to install applications from a list of published applications via the “Add/Remove Programs” feature.
- Networking, which sets the preferred wireless SSID and sets the Windows Firewall.
- Remote Assistance, which enables the help desk to initiate Remote Assistance sessions without an explicit invitation.
- Startup script, which disables network browser service to save bandwidth and installs the SMS 2003 client.

-
- Logon script, which ensures that the antivirus client is installed and updates the signature file.

Other GPOs are used to give specific security groups access to high-value resources, such as the Human Resources database or the source code repositories.

A typical request might be to increase the isolation of the Microsoft Exchange Server 2003 communication and collaboration servers from the rest of the corporate network, or Microsoft IT may be asked to set specific policies on a Microsoft Office Sharepoint® Portal Server 2003 server. In general, Group Policy works well for locking down and managing configurations of servers in data centers. Before managing servers with Group Policy, each Microsoft data center managed all of its own servers, leading to inconsistent security across the enterprise. Group Policy helps assure an enterprise-wide standard for security and server configurations across data centers.

Many GPOs are built to accommodate particular testing scenarios, so that a specific set of computers can be configured in a non-standard way. In most cases, the rest of the corporate network does not trust these computers, and they can be effectively isolated while providing basic Internet access or access to other devices with the same policies.

A typical computer on the Microsoft IT network might have 14 GPOs applied, including GPOs containing computer settings and GPOs containing user settings.

Use Many Small GPOs

Microsoft IT has found several benefits to using many small GPOs:

- Easier to manage objects that remain stable.
- Easier to roll back individual policy settings if there is a mistake.
- Reduced effort and fewer errors deploying across domains because policies can be duplicated for multiple domains.
- Less load on DCs because clients can cache GPOs that have not changed and only download new or modified policies.
- Lower potential impact of file replication problems.

Easier to manage

It is much easier to make small, incremental changes by adding GPOs with one or two settings than to find and change settings in a single large GPO. Individual GPOs can be targeted or filtered to a specific set of users or computers, and they can be used to override a more general default policy.

For example, at Microsoft, IPsec is used to segment trusted computers from untrusted devices (i.e., computers that are not joined to an IT-managed domain) that may connect to the corporate network. All computers in the domain can be set to run in IPsec "require" mode, not communicating with any other computers that do not initiate requests using IPsec. However, in some cases, a computer will need to be configured to allow other computers to initiate requests not using IPsec. In this case, there is a separate IPsec "request" mode policy applied to the computer.

By breaking related policy settings into distinct groups, the Identity Management Team can put them in a GPO that makes them easier to deploy and manage.

Easier to Roll Back

When a new policy setting is requested for an area that already has a GPO, the Identity Management Team tends to create a new GPO for that setting, rather than adding it to an existing GPO. The reasoning is that if there is some unforeseen consequence of adding the setting, it is easy to delete the entire GPO from Active Directory and restore the previous configuration.

Reduced Effort and Fewer Errors

Because a GPO can be linked only to a domain, a site, or an OU, enterprises with multiple domains need to manage multiple sets of GPOs. By creating a GPO with a small number of settings, it is easier to duplicate it directly in other domains and avoid linking one GPO across multiple domain boundaries.

Microsoft uses a base set of GPOs across all of its production domains. These GPOs provide password policies, local administrator rights for a security auditing group, IPsec settings, and settings that create a mirror of users' My Documents directory on a server. The GPOs also turn on the Windows Firewall, enable the help desk to initiate a remote assistance session, run startup and logon scripts, and support several other policies. Many of the GPOs can be exported from one domain and imported directly into another domain.

Each domain gets a standard set of GPOs and then adds other GPOs as needed to meet more specific needs.

Reduced Load on Domain Controllers

By keeping GPOs relatively static, client computers do not have to process each GPO at every startup or logon. When the Group Policy client starts, it connects to the DC and gets a version identification of each GPO linked to its domain, site, or OU. If the version matches a GPO that the client already applied during a previous session, the client may not need to change existing setting, depending on the type of setting. If the version identification has changed, the client needs to download the new GPO from the DC.

By keeping most policy settings in static, unchanging GPOs, clients only need to download the new GPOs, minimizing startup times and reducing the load on DCs.

Lower Impact of File Replication Problems

For the same reason, keeping GPOs static reduces the need for replication across all of the DCs in a domain. Only new GPOs need to be replicated, increasing the chances that the core, unchanging policy settings are always available and in effect.

Plan for Potential Failed GPO Replication

Group Policy provides the ability to centrally define what happens to clients (both computers and users) at the edges of the network. What is defined centrally is replicated throughout the domain. Yet, replication is not 100 percent reliable. When designing GPOs, it is essential to consider the consequences of a particular GPO failing and what it would take to be properly updated during any particular startup.

For security-related policies, it may be useful to design policies that prevent access if the policy is not properly applied.

Many policy settings can be specified in several ways:

- Default (no policy specified)

-
- Enable, but allow user to override
 - Require a particular setting
 - Disable, but allow user to enable
 - Disable entirely

The options available for any particular registry setting are defined in the *.ADM template file and depend more on the application that is using the policy than anything else.

Target Different Policy Settings to Different Groups

When a particular registry setting is specified in more than one GPO, determining which one will take effect can be challenging. The Group Policy client follows a specific sequence when processing GPOs, but determining this sequence, especially when some settings contradict others, is an exercise best avoided entirely.

Microsoft IT avoids the issue of conflicting Group Policy settings by grouping similar policy settings together in a GPO. If a particular group of users needs to have different settings, Microsoft IT puts them in a security group (if the relevant group does not already exist) and creates two different GPOs linked to the same domain. One GPO is filtered to include the relevant security group(s), and the other is filtered to exclude the same groups.

Microsoft has a defined process that makes it easy for any employee to request the creation of a security group. After creating a group, the change requestor can ask the Identity Management Team for a custom GPO to provide the desired settings for that group.

Another way of addressing the same issue is to target a GPO to a specific OU. In certain cases, the Identity Management Team has set up an OU and linked a requested GPO to the OU. The majority of the time, however, Microsoft has tended to use security groups rather than OUs to apply specific GPOs to specific users. This reflects a challenging and heterogeneous computing environment. Microsoft's user base typically maintains multiple computers, runs varying operating systems, and frequently rebuilds its own computers. However, Microsoft is currently migrating towards a more managed and homogeneous computing environment. In tandem with this effort, the OU structure at Microsoft is being updated and optimized,

One benefit of using OUs over security groups is that Microsoft IT can delegate control over the GPO to the OU administrators, without granting them access to any other GPOs or users in the forest. This delegation of GPO control generally is used to give more freedom to particular labs.

Before granting modification access to specific GPOs, the Identity Management Team verifies that the settings do not conflict with other GPOs that are applied to the domain. The group grants the OU administrators the ability to modify—but not add or delete—GPOs for their OU only.

Link GPOs to Appropriate Containers

When a computer starts and connects to a domain, it asks Active Directory for a list of all GPOs that apply to its domain, OU, and site. The Group Policy client then checks for and downloads any new GPOs or new versions of existing GPOs.

The same basic process happens again when a user logs on.

-
- **Domain.** At Microsoft, most GPOs are linked to domains, mainly as a result of the Active Directory domain structure.
 - **OU.** The primary benefit of linking a GPO to an OU is that it is possible to delegate administrative access over that GPO to the OU administrators without granting them administrative rights to anywhere else in the domain. A secondary benefit is that clients will not download GPOs linked to other OUs, but they will download all GPOs linked to a domain, whether or not the clients apply those GPOs. Filtering occurs after downloading. Microsoft has a growing number of OUs, but unless there is a business need to delegate control over a GPO to an organizational unit, the Identity Management Team maintains centralized control over all of the GPOs.
 - **Site.** At Microsoft, GPOs are not linked to sites. A site corresponds to a specific sub-network and can be used to create specific GPOs for a lab.

Filter by Security Group or WMI Queries

After downloading all the GPOs linked to the domain, OU, and site of the computer and user, the Group Policy client examines each GPO for filtering settings. Each GPO may be filtered by security group or by a WMI query. Filters can be used to apply or exclude a particular GPO based on the result.

GPOs are downloaded to the client computer whether or not it is applied. Filtering happens after downloading. Microsoft IT has found the impact of this extra downloading to be negligible for security group filtering, especially when individual GPOs remain static for long periods of time and are cached on the clients. Microsoft IT uses security groups extensively to filter groups in and out of specific GPOs.

On the other hand, WMI queries can be time consuming because they need to be executed each time the GPO is applied. Yet, there are certain cases in which WMI queries are the best solution. For example, Microsoft “dogfoods” many of its products internally, using various beta builds of applications throughout the corporate network. Sometimes a problem is found with a specific version of a beta application. A WMI query can help the Identity Management Team target a specific build of an application for a particular set of policy settings.

Consistently Name and Track GPOs

Microsoft IT has found that a consistent naming convention for GPOs is essential to managing them effectively. Before deploying Windows Server 2003, Microsoft IT renamed the older GPOs. The naming convention is designed to easily identify key information about the GPO, such as its purpose and owner. . By using a consistent naming convention, Microsoft IT can find the owner of a particular GPO and have some sense of what the GPO is for and where it is applied.

The Identity Management Team owns all default GPOs, including those developed on behalf of requesting groups. Other internal IT groups also have expertise in their subject areas, and the Identity Management Team delegates GPO modification privileges to them.

Tracking changes to GPOs is also essential. The change management process is covered later in this white paper in the section titled “Group Policy Workflow Management.”

Evaluate Methods for Software Installation and Script Execution

Group Policy is capable of handling much more than just registry settings. A GPO can execute a startup, logon, logoff, or shutdown script. A GPO can publish software, making it available to install on demand, or it can force installation of software.

Microsoft has other systems that provide similar functionality. Microsoft IT uses Systems Management Server 2003 extensively to provide most software publishing and software update management and to handle tasks that might otherwise be done by using a GPO to call a script.

Microsoft IT uses Group Policy to require the SMS 2003 client to be installed and running on any computer that joins a managed domain. A startup script also disables the Computer Browser service to conserve bandwidth on the network.

Microsoft IT also uses a GPO to run a user logon script that verifies the presence of the corporate antivirus software and latest signature file updates; the script forces their installation if they are not present.

Aside from these minimal GPO scripts, Microsoft IT uses other deployment technologies to run scripts on computers for two primary reasons:

1. The systems were already in place and operating before Microsoft deployed Group Policy.
2. Forced installations of software through a GPO effectively can deny large numbers of users access to their computers, with no indication of what is taking place. Other tools provide ways of giving users some indication of the installation and its progress.

Software deployment through Group Policy has been tested within Microsoft. With larger software “push” installations, the installation must finish before continuing past the “Applying Group Policy” message when starting up or logging on to the local computer. Users did not know why it took so long to log on; many turned the computer’s power off and started it while disconnected from the network. At Microsoft, SMS 2003 has proven to be a more user-friendly way to forcibly install mandatory software and updates, and provide on-demand installation of approved business applications.

When using GPO to run scripts or force software installation, Microsoft IT recommends keeping the size of downloaded components to a minimum and properly notifying users about the reasons for longer logon times. Alternatively, there are other methods that can be used for the same tasks.

Plan for Computers Leaving a Domain

When designing GPOs, it is important to recognize what happens to policy settings when a computer moves to another domain or otherwise leaves the existing domain. Some policy settings remain in effect, while others revert to the previous value set by the user.

The behavior of Group Policy varies depending on whether the computer actually joins another domain, leaves the original domain, or is merely disconnected from the domain. It also varies depending on whether a given policy setting belongs to an application that is aware of Group Policy and how the *.ADM file was constructed.

- When a computer is part of a domain, it attempts to connect to a DC at startup and again when the user logs on.

-
- If a DC is not available, or the computer is not connected to any network, it starts in a disconnected mode and uses the previously applied security and policy settings.
 - When a computer leaves a domain, it removes the policy settings for Group Policy-aware applications. Settings that are not for policy-aware applications remain written in the registry and may need to be reset by a local administrator or a GPO on a newly joined domain.

In one instance, computers in a domain were being moved from one forest to another. The preferred method to accomplish this is to directly move each computer in the domain, but in this case, each computer was un-joined from the old domain and joined to the new domain. Because the Domain Name Service settings remained in the registry of each computer, and the local administrator passwords were unknown on some computers, users were locked out of their computers and the computers were unable to join the new domain. (Some group policy settings create registry settings that remain after the policy is removed. This is called *tattooing* the registry.)

Administrative templates configure specific settings in the registry, and they can be built to set any registry setting in the HKEY_LOCAL_MACHINE or HKEY_CURRENT_USER subtrees. However, there are specific branches in the registry used by applications that are aware of Group Policy. Setting a value in the policy branch of the registry enables the application to revert to a different user preference when the GPO is removed.

Applications that are not aware of Group Policy have no way to revert to a previous state. If an administrative template makes a registry setting outside one of the policy-specific locations, the user has to manually change that setting back after removing the GPO or moving the computer to another domain with a different set of GPOs.

Limit GPO Deployment Personnel

Because GPOs can have wide-ranging effects on a corporate network, it is essential to limit the number of administrators who have permission to deploy or change them. At Microsoft, only the Identity Management Team has authority to deploy new GPOs.

Any domain administrator has the necessary access rights to deploy a GPO. However, Microsoft has a strong business policy that specifically forbids unauthorized people from doing so, requiring them to go through the change request process established by the Identity Management Team. This group owns all GPOs and the Active Directory structure at Microsoft.

The group regularly reconciles the GPOs linked in Active Directory to the authoritative set that it maintains. If there are any unauthorized changes to the GPOs in Active Directory, it is treated as a security incident, and the source of the change is tracked down and educated appropriately. Enforcing this policy is an organizational issue, not a technical one.

In certain cases, the Identity Management Team delegates editing privileges for specific GPOs linked to an OU. The OU administrators can fine-tune specific settings within their GPOs. They do not get the ability to add or delete GPOs—only to edit the specific GPOs delegated by the Identity Management Team.

GROUP POLICY WORKFLOW MANAGEMENT

Given the large number of users, computers, and GPOs at Microsoft, implementing a sound process for managing updates to GPOs has been essential. Microsoft IT uses the MOF as the base for its core management processes. The Identity Management Team has adopted the change management process defined in the MOF to manage GPO change requests, testing, and implementation.

Note: *The Microsoft Operations Framework is documented extensively at the MOF Web site, <http://www.microsoft.com/mof>. The change management process deployed by the Identity Management Team is described at <http://www.microsoft.com/technet/itsolutions/cits/mo/smf/smfchgmg.mspx>.*

GPOs must comply with basic corporate security policies, and any GPO requests must be justified by appropriate business need. GPOs are reviewed and deployed on a weekly basis, and all regular GPO changes are deployed on the same day each week. The help desk is notified of new GPOs that have been released each week, and it has no need to guess whether any particular problem could be related to a GPO—if it is not on one of the GPO release days, it probably is not a problem related to a new GPO.

The Identity Management Team provides a service level agreement of 7 to 14 days from request, to review, to approval, to deployment, providing sufficient time to conduct multiple pre-deployment tests of the new or updated GPO policy settings.

Triage and emergency escalation criteria are explicitly defined, so that critical GPO changes can be made sooner. Cross-group communication is integrated into the process as other groups, such as Corporate Security, are notified of GPO changes.

The GPO change management process has reduced disruptions and reduced human error. Using a consistent, enforceable workflow makes GPO deployment more reliable and greatly assists with regulatory compliance.

Roles and Responsibilities

The Identity Management Team owns the GPO change management process. It manages, tests, and implements GPOs for a team or group that requests one. The Identity Management Team also ensures that GPOs are consistent across all domains, forests, and organizational units throughout the enterprise, and it manages the delegation of policies applied below the domain root.

The Identity Management Team uses a cross-IT notification process to notify other groups within Microsoft IT of upcoming policy changes to give them the chance to review the upcoming changes and provide feedback on those changes, if desired.

GPO Change Management Process

By having a consistent change management process, Microsoft IT can reduce the impact of deploying new GPOs and discover potential issues before a GPO is deployed companywide. The MOF-based process includes the following steps:

1. The client group (requestor) submits a request for a GPO change.
2. The requestor or Identity Management Team (change manager) opens a trouble ticket to track progress on the GPO.
3. The change manager evaluates the request to determine whether it is an emergency or a regular request and sets a schedule for the change request.
4. A member of the Identity Management Team is assigned to be the change owner, who assesses the settings required.
5. The change owner represents the requestor during the weekly GPO Change Review Board meeting, and the request is approved or denied.
6. The change owner and the requestor test the settings for effectiveness in a lab environment.
7. For changes that have an effect that is noticeable to users, the requestor and the change owner communicate the changes to users.
8. The requestor and change owner verifies deployment settings.
9. The change owner deploys the GPO, sometimes in phases, and archives both the previous and the new GPOs.

10. If any negative results appear, the change owner rolls back to the previous state, if necessary.

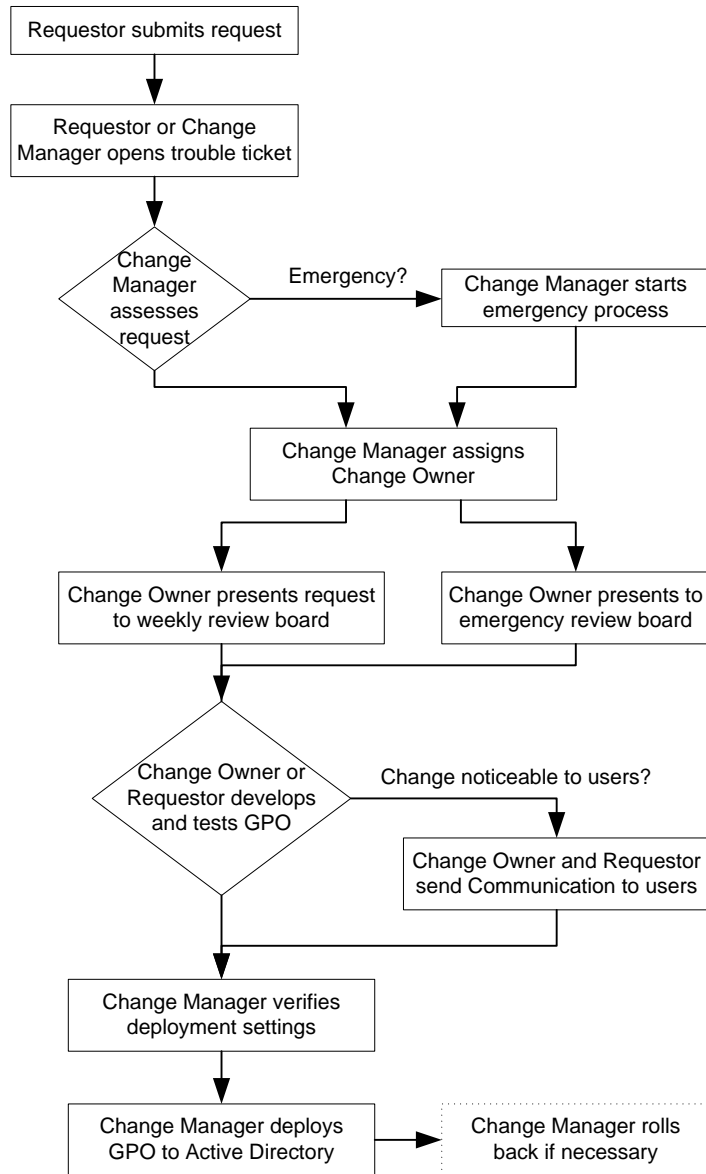


Figure 2. GPO Change Management Process

Requesting Group Submits Request for GPO Change

The requesting group could be any group within Microsoft that needs a GPO added or modified. Many groups have special testing needs that dictate developing a new GPO. Other internal IT groups may have a mandate to roll out some security enhancement across the enterprise. Anyone needing a GPO changed brings the request to the Identity Management Team.

The change request needs to identify the goal of the change, the timeframe for implementing it, the software involved, the priority, the sponsor of the change, a test plan, and specific settings desired, if known.

Open a Service Request

All GPO change requests are tracked in a support system so that all involved groups can see the status of all requests and any issues or discussion about a requested change.

Generally, the requesting group should have a written business policy published somewhere for the affected users to find. GPOs are created to support or enforce business policies—if there is no written business policy stating the reason for the GPO, the request usually will be denied.

Evaluate Request and Set Schedule

The Identity Management Team establishes minimum lead times and reviews GPO deployment on a regular weekly schedule. The group has established emergency request criteria and additional processes for emergencies. GPO changes are considered emergencies if leaving the GPOs unchanged results in:

- A work stoppage for 50 or more users
- Business (service) stoppage
- A high-impact security issue

If one or more of these criteria are met, the requesting client group must provide executive approval of the change, and the process is expedited. Other GPO change requests are delayed until the emergency request is handled.

For GPOs affecting a small group, non-emergency changes are put in a change request process that is executed weekly. For GPOs that are deployed enterprise-wide, the Identity Management Team works with other groups within Microsoft IT to deploy the GPO in stages when needed, starting with a small security group and rolling the GPO out to one of the smaller domains before deploying to the entire enterprise. By deploying in this way, the rollout can be reversed if an unexpected problem appears, without affecting the majority of the company.

Assess the GPO Settings

Most client requests indicate what the group is trying to accomplish, not necessarily the individual policy settings necessary to accomplish it. The Identity Management Team works with the client group to determine the appropriate Group Policy settings to accomplish the desired goal.

In most cases, the change requested involves using an administrative template to create a particular setting; sometimes, the group must create the administrative template to make the setting available. The requestor can create the administrative template, use Local Policy to apply the setting, and test to make sure it has the desired result.

If the requesting group does not have the required expertise to do this, a member of the Identity Management Team can develop the administrative template on behalf of the requestor.

GPO Change Review Board Approval

Once the appropriate settings have been determined, the GPO Change Review Board is notified of the request. The GPO Change Review Board fills the MOF role of a change advisory board. The Identity Management Team is the functional approver for all GPO changes in the IT-managed domains, and it participates in the GPO Change Review Board with representation from the Corporate Security group and various internal IT groups, account managers, and regional support managers.

With GPO changes, most of the reasons for rejecting a request are related to corporate security. The Corporate Security group evaluates the proposed changes to determine if they meet the security standards of the enterprise.

If the settings increase the security risk, the GPO may be rejected or revised to address the security concern.

Test the Settings

After evaluating the settings necessary to accomplish the goal of the change request, a member of the Identity Management Team creates a GPO containing the settings and applies it to a limited security group for testing. The requesting group may be involved to verify that the test GPO meets its needs.

The GPO creator can use a variety of tools to test the new GPO. Particularly important is the Resultant Set of Policies tool, which enables the tester to model the result for various computers and user logons. The tester determines whether the desired GPO will be deployed to the correct set of users and not deployed to users who should not get the GPO. The tester must also determine whether the policy settings put in the GPO have the desired effect and lead to the desired result.

Testing is done in an Active Directory lab environment, isolated from the production domains.

Communicate Changes to Users

The Identity Management Team uses an e-mail distribution list to communicate all GPO changes to interested parties within the company. For significant, enterprise-wide changes, the Identity Management Team may work with other groups to communicate changes to all affected Microsoft users. This may include posting notices in buildings, publishing stories in the employee newsletter and on the intranet, holding open question-and-answer sessions during the lunch hour, or other methods, as appropriate.

Many changes do not have a noticeable effect on users because they enforce policies that are already widely communicated. In these cases, no additional notification may be necessary.

Communication of changes to the affected users is critical to the success of the GPO change management process. If users are unaware of substantial changes to their systems, otherwise-smooth rollouts can cause significant disruption. If possible, it is important to notify people of changes before the changes occur.

Verify Deployment Settings

The Identity Management Team has an internal policy that requires a second source to evaluate a GPO before deployment. Someone in the group other than the policy administrator must approve the GPO settings before the GPO is deployed.

Deploy and Archive

Before applying a GPO to the target container, the previous GPO configuration is backed up. The new GPO also is archived after it is applied to the target container.

The Identity Management Team and the client groups carefully monitor the container for any unexpected side effects and make sure the GPO accomplishes the goal.

For large, enterprise-wide deployments, the Identity Management Team often deploys the GPO in a series of phases. In the first phase, a small representative group of workstations, servers, or users is put into a security group. The GPO is filtered to apply to that group only, and the Identity Management Team monitors for unexpected problems.

If the GPO does not have any adverse effects when applied to a small group, the Identity Management Team next deploys it to one of the smaller production domains and carefully observes the effects.

If the deployment is successful in one of the smaller domains and the GPO has the desired effect, the Identity Management Team deploys it to the other domains in the enterprise.

Deploying domains one at a time can reduce rollback time and disruptions if an unexpected problem appears.

Roll Back if Necessary

If there are any unexpected problems with the GPO deployment, the previous configuration is restored.

TROUBLESHOOTING GPO ISSUES

With hundreds of GPOs in Active Directory, troubleshooting Group Policy issues can be challenging. The Microsoft Identity Management Team has implemented a strong GPO management process to prevent problems from initially occurring and to be able to easily identify the source of a problem based on changes to the environment.

However, there are still a few issues that arise during GPO design and day-to-day operations. The following section identifies the main issues that the Identity Management Team encounters and the tools it uses to resolve them.

Conflicting Policies

In the process of creating a GPO, the implementers often get unexpected results. Sometimes a new GPO works well in the test environment but causes problems when it is deployed to a certain domain. Occasionally, the problems appear only for specific users. These issues are usually a result of the new policy settings conflicting with a setting in another GPO.

Several tools can help identify conflicting policy settings:

- **Group Policy Management Console.** This tool contains a settings report feature and inspection scripts that can gather information on GPOs.
- **Resulting Set of Policies.** RSoP is available in Windows XP, Windows XP with SP1, and Windows XP with SP2 as an MMC snap-in. With RSoP, the troubleshooter can view the effective set of policies for any computer or user in Active Directory, and it can identify which GPO contains which policy setting. RSoP can help to identify GPO overlaps, resolve security group filters, and highlight other factors that might lead to overlooked policy overlaps.
- **GPRresult.** GPRresult.exe is a command-line tool that can be used to find conflicts in a way that is similar to RSoP. This tool can be useful for troubleshooting specific GPO deployment issues on problem computers; it is also capable of much of the troubleshooting built into RSoP.
- **Windows Logs.** Logs can identify problem settings and the exact way in which Windows applied the settings from each GPO.
- **Partner Software.** The Identity Management Team uses partner analysis tools to identify potential conflicts with a GPO before deploying it to Active Directory.

Replication Issues

With the release of Windows Server 2003, many replication issues that might have caused extensive problems with Group Policy deployment have been resolved. However, there are still cases in which problems may occur, such as local changes that block replication or unreliable network links that result in incomplete transfers.

Group Policy is dependent on two different replication mechanisms:

- Active Directory replication
- File Replication Service

A problem with replication in either mechanism can cause Group Policy to fail during deployment or general operation. Depending on what fails, the result might be computers that cannot access domain resources, missing configuration settings, or extended logon times.

One benefit of Group Policy is that clients eventually will get the latest GPOs when the replication succeeds.

If a particular GPO is not applied, the client may either skip it, revert to slow link behavior and only apply security and administrative template-based GPOs, or stop processing GPOs.

Active Directory Replication

Group Policy is deployed through Active Directory. Each domain, site, and OU has a list of GPOs in Active Directory. Each GPO is labeled with a Globally Unique Identifier (GUID). GUIDs are easy for computers to recognize, but difficult for people because they consist of a long set of numbers and look very similar to each other.

The GPO itself, however, is not stored in Active Directory. Active Directory only stores a pointer that defines which GPOs must be applied by the client.

In the experience of the Microsoft Identity Management Team, Active Directory replication is highly reliable.

File Replication Service

The actual contents of a GPO are stored as files in the /Sysvol share on each domain controller within a domain. FRS is responsible for replicating this GPO content to all of the DCs within a domain.

File replication problems have become much less common than they were prior to Windows Server 2003. When these problems are encountered, the Ultrasound program, freely available from Microsoft at <https://www.microsoft.com/frs>, can help quickly diagnose the problem and report on the health of the files distributed across the domain.

Aside from replication issues, the other problem that the Microsoft Identity Management Team has encountered has been missing files in the policy itself. One example is the gpt.ini file, which identifies the version of a particular GPO and, if there is a problem with that file or the file is missing, the client will not be able to process that GPO.

Slow Link Issues

When a computer starts, before it reaches the logon screen, it will determine its link speed. If a slow link is detected, the Group Policy client goes into a slow link mode. In this mode, only security- and registry-based policy processing are applied by default. Administrators can configure which sections of Group Policy are processed over a slow link via Group Policy settings, if desired.

When troubleshooting GPO issues, slow link speeds can be responsible for many Group Policy issues that otherwise appear to be anomalous.

BEST PRACTICES

This white paper is filled with best practices and lessons learned by Microsoft IT about managing Group Policy in a large enterprise environment. This section summarizes some of the more important best practices.

- **Create and institutionalize a set of business processes for managing changes to Group Policy.** Without a clear process, it is easy to end up with a chaotic, conflicting network environment. Planning ahead, testing, and double-checking GPOs before deployment saves trouble in the future.
- **Set up GPOs for different behavior types to support IT and business unit testing.** On a large network, exception policies take additional management time. Wherever possible, combine exceptions to simplify management. Identify as few security groups and corresponding policies as necessary for meeting business and IT needs.
- **Limit the number of Group Policy administrators.** Because people who can change add or delete GPOs can drastically affect deployment across the entire enterprise, it is critical to limit Group Policy administration to a small number of administrators.
- **Use a naming convention that covers the policy function and target container for easier management and troubleshooting.** For example, create a "Domain Password Policy" GPO that contains the password policy settings that are applied to a domain. With different policies and target containers, it is easy to get confused about which policy was created for which container and what purpose that policy serves.
- **Beware of policy and administrator conflicts.** Domain administrators often can override settings that are controlled by Group Policy. Set clear guidelines and communicate policies to people who are in a position to create conflicts, and limit the number of domain administrators.
- **Use Group Policy Management Console.** This tool is a separate, free download from <http://www.microsoft.com/grouppolicy>. GPMC provides the basic functionality necessary for managing GPOs, including applying them, reviewing them, exporting and importing them to a file, and viewing the resulting set of policies of a group of GPOs.
- **Consider third-party products for enterprise-level management.** There are several third-party frameworks that provide more of a software configuration management environment for GPO management, including full revision history, conflict resolution, and the ability to test combinations offline.

Note: A list of third-party GPO vendors can be found at the Group Policy Task force Web site, at <http://www.gptf.org/>.

- **Monitor Group Policy operations through Microsoft Operations Manager 2005 and other tools.** MOM 2005 has a Group Policy Management Pack and an Active Directory Management Pack that can help monitor and manage Group Policy operations. Finally, the Ultrasound Resource Kit tool can help identify FRS failures for the replication of /Sysvol content for GPOs between domain controllers within a domain.
- **Implement a workflow with a pre-defined process for requesting, reviewing, and approving changes.** The Microsoft Identity Management Team used the Microsoft Operations Framework to develop an effective process for GPO requests, reviews, and approval. Having a process and a single team responsible for introducing GPOs to Active Directory is crucial for managing Group Policy effectively.

CONCLUSION

Group Policy provides a powerful framework for managing and enforcing settings on computers on a corporate network. Microsoft IT uses it to deploy some policies to all computers on the network, while managing specific settings for certain classes of servers.

An effective process surrounding the approval, development, and deployment of GPOs can reduce the expense and complexity of creating GPOs. Without an adequate process, it is easy to create settings that conflict with each other and, in drastic cases, these setting conflicts can make a computer inaccessible. It is critical to carefully manage changes to Group Policy Objects, making sure that the changes do not conflict with other GPOs and that they have the desired effect.

By setting up a clear Group Policy change management process and assigning ownership of the process to a particular group, Microsoft IT has reduced the number of GPO administrators from twenty staff members to the equivalent of four for the global Active Directory environment over the last 18 months. GPO management has become integrated into the business processes of the enterprise, providing the ability to continually refine enforcement of policies, provide evidence of regulatory compliance, segregate roles, and improve employee productivity.

FOR MORE INFORMATION

For more Group Policy information and resources, go to:

Group Policy Wiki: <http://GroupPolicyWiki.com>

Windows Server 2003 Group Policy:

<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/featured/gp/default.mspx>

Third-party Tools and Extensions for Group Policy:

<http://www.microsoft.com/windowsserver2003/technologies/management/grouppolicy/gptools.mspx>

For more information about Microsoft products or services, call the Microsoft Sales Information Center at (800) 426-9400. In Canada, call the Microsoft Canada Information Centre at (800) 563-9048. Outside the 50 United States and Canada, please contact your local Microsoft subsidiary. To access information through the World Wide Web, go to:

<http://www.microsoft.com>

<http://www.microsoft.com/itshowcase>

<http://www.microsoft.com/technet/itshowcase>

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Microsoft grants you the right to reproduce this White Paper, in whole or in part, specifically and solely for the purpose of personal education.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, email address, logo, person, place, or event is intended or should be inferred.

© 2005 Microsoft Corporation. All rights reserved.

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY. Microsoft, Outlook, SharePoint, Windows, Windows Server, and Windows Server System are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.