Staying Abreast of Group Policy Changes

White Paper

Contents

Introduction 3
Change Auditing for Compliance 4
How Change Auditing Relates to Change Management 5
Case in Point: Group Policy Changes 7
- Native Tools 7
- Building Versus Buying 7
- Third-Party Software 8
- Success Recipe 8

The Smart Choice: NetWrix Group Policy Change Reporter 9

Introduction

In the IT infrastructure of a company, change is normal. This aspect of an organization's life cannot remain static for a number of reasons:

- IT components are designed to be dynamic, flexible, and capable of supporting diverse configurations.
- The huge volume and diversity of information means today's enterprises rely on information technology, so a variety of completely unrelated tasks depend on the information cycle.
- The rate of changes, though varied across the range of tasks, is considerable.
- There is interdependency of information. A change in a single component can necessitate a series of changes in others. For example, a virus outbreak may lead to a revision of the antivirus policy, meaning that a new software distribution task needs to be created, Internet Explorer security zones need to be updated, and so on.

If information is allowed to become stale, operations can be disrupted. However, for the same reasons the information flow should not be allowed to stagnate, changes should not go unwatched. Those aspects of company life entrusted to IT are easier to change than other structures. However, the consequences of adverse changes can be as detrimental and expensive to correct as physical damage.

In addition, IT staff has to deal with compliance. SOX, HIPAA, GLBA, and FISMA compliance measures are not dictated by internal needs, but still must be considered for the enterprise to function smoothly.

How is it possible to make sure all necessary changes are implemented and the effects of unwanted changes are minimized? This white paper describes approaches to change auditing, explains how audit data can be used for change management, and focuses on one of the most important IT components for centralized and automated administration today: Group Policy.

Change Auditing for Compliance

Audit data must be kept for a very long time, up to 7 years by some regulations. The scope of the stored data should be sufficient to satisfy any requests from the auditors, and be as detailed as possible. Whether an auditor needs to know who modified the GPO used for the Accounting OU or view a complete history of changes to the default domain policy for the past 5 years, the data should be readily available for analysis.

Very importantly, the data should clearly indicate who initiated the recorded change. Otherwise, the responsibility for any harm caused by the changes rests with the CIO. The more complete the audit data, the more certainty there is that the actual responsible party will be held accountable for damaging actions.

→

How Change Auditing Relates to Change Management

Change management is a continuous process of deciding what kinds of changes to the IT infrastructure must and must not take place, what changes you want to watch for, and what you need to do about the changes you find. This process is impossible without a comprehensive body of audit data, which is provided by the auditing solution.

The volume of change-related audit data is necessarily large, and not all of it is useful for change management. In a corporate IT environment, the aspects that require special attention are primarily related to identity configuration and security configuration.

In these vital areas, not all changes deserve inspection, especially not when the volume of changes is routinely overwhelming. However, attention can be duly guided by clear-cut assessment criteria, such as those listed below.

Critical versus inconsequential

On the priority scale, changes vary by the consequences they cause. Clearly, the deletion of a Group Policy object is a more serious issue than the renaming of that object.

The response time for critical changes should be as short as possible, and the changes should be constantly monitored. Many of such change types are well-known and easy to track; this helps reduce the number of critical changes that need special attention.

Planned versus unplanned

Unanticipated changes are a problem. First, they are the primary cause of outages. Second, if these events are frequent and are not prevented, they may be the reason for a failed security audit. Such changes should not go unmonitored. However, even planned changes should be monitored to ensure they happen on time and without policy violations.

An example of a planned change is deployment of a new software package through Group Policy. This is a sensitive action that should never fall under the radar—care must be taken to ensure the software is installed as expected, no components are skipped, and no extraneous components are included. Likewise, applying an existing Group Policy object to a new organizational unit must be on record, unconditionally. If this is done without proper care, it may result in privilege escalation or, conversely, loss of productivity (for example, no access to Control Panel settings).

A meaningful change that is not typical is also most probably unplanned, and should be analyzed.

Noise versus signal

Audit trails contain a percentage of events that unambiguously indicate important changes. These events are easy to track. For example, changes to firewall settings controlled by Group Policy should be immediately investigated. When managed irresponsibly, these settings can open backdoors on servers and client computers.

However, the amount of useful information found in audit trails is never large. Many events are normally logged for even minor changes, and these events may need to be correlated to find out what actually happened. This means the same type of event may be part of the background noise, or it may accompany a critical change, depending on what other events were logged around the same time. An example of such an inconspicuous event is when a potentially non-secure service (such as RPC, www or WMI) is enabled (the state changes from **Disabled** to **Run at startup**) in the GPO settings for a DMZ service. This change is easy to overlook, but the result is increased attack surface on the DMZ servers.

Inadvertent versus malicious

Adverse changes are not always ill-intentioned. They may be the result of mistakes or irresponsible administration, especially when there are no evident attempts to cover the tracks after such changes. Inadvertent changes like this are often reversible.

It can be difficult to tell whether or not a change was intentional. For example, the priority order of Group Policy objects can be changed so that a less restrictive policy overrides a more restrictive policy. Without an investigation, it may not be clear whether this was done on purpose. Another possible change of this kind is the disabling of centralized automatic updates from Windows Server Update Services, which can cause all computers to download updates directly from the Microsoft website (generating huge traffic) or to never download them at all. To investigate such matters and restore the correct configuration, detailed records of what happened are essential.

Prioritizing the changes helps you build your change management strategy.

Case in Point: Group Policy Changes

Group Policy is an indispensable tool for policy enforcement and centralized end-point configuration. With Windows as the dominant business platform, Group Policy is vital for security, configuration and operations management.

Changes to some parts of this system can bring the entire business process to a standstill. The tools you use for change management must be able to cope with the enormous amount of audit data that needs to be sifted through. This section lists the main approaches used in production IT environments.

Native Tools

Freely available Windows MMC-based native tools, such as Active Directory Users and Computers, Group Policy Object Editor, Group Policy Management Console, and others, are entry-level solutions. They have the advantage of requiring no customization or third-party software but, even in a mid-size IT infrastructure, they are not powerful enough to perform any meaningful change management.

A viable non-free native alternative is the Advanced Group Policy Management tool, which is part of the Microsoft Desktop Optimization Pack. It provides improved Group Policy auditing and administration capabilities, and a framework for delegating them. However, the convenience comes at a cost—the product is licensed at $10 per user per year. In an organization with 1000 user accounts, the bill runs up to $10,000 per year.

Even with a well-designed change management strategy, native tools are either costly or unable to significantly reduce the effects of adverse changes; this is due to the high latency between the change and its discovery, and lack of reporting capabilities. A change is not examined until after it has caused some negative results, such as service failure or slowdown of operations.

The time between an unwarranted change and its undesirable effects can be very short, and change-detection automation is very important to ensure a timely response. However, if the administrator is armed with only native tools, a change-induced problem might take a week or longer to solve.

Building Versus Buying

The search for automation and analysis methods can lead a company to invest in in-house software. The range of technologies that can be employed is wide. PowerShell, the .NET framework, and many other programming and scripting languages, have bindings for Active Directory and Windows APIs, which are extensively documented.

Unfortunately, Group Policy auditing is a very complex programming task because, in this case, auditing is not simply a matter of processing the Security log. Group Policy changes are not recorded to event logs by the native auditing system, so more advanced technologies are needed for that purpose.

The effectiveness of in-house development is determined not so much by what is possible to do as by what can be done in a given time with the given resources. If the company does not specialize in change auditing

software—and most do not—then time and resources are bound to be too scarce for comfort. Even if the in-house solution is good, its development is certain to face problems:

- Support—the software produced in-house may have many authors, which increases support difficulty; in addition, such a solution may evolve organically and is not likely to be centralized
- Testing—new software does not normally go into production use until it has undergone extensive tests, which require a great deal of time and expertise

In-house scripts and programs may be the optimal solution for some companies, but this is a rare case in large distributed environments that have to accommodate internal and remote clients, heterogeneous systems, and so on. Often a more cost-effective and better-quality alternative is to purchase third-party software specifically designed for Group Policy change management.

Third-Party Software

When it comes to choosing a third-party solution for Group Policy change auditing, a great variety of available software seems to fit the bill. The final decision can be influenced by many factors, such as:

- Transparency of information about the product's capabilities
- Quality-price ratio
- Cost of ownership

When the choice is made, it is important to remember that the tools cannot, on their own, solve complex problems in Group Policy change auditing, tracking, and management.

Success Recipe

To be effective in tracking Group Policy changes, it is important to have both a sensible strategy and software tools that are flexible enough to meet all your needs but do not get in the way of your strategy.

Prioritize the changes by importance, relevance, and purpose. Be sure to differentiate between planned and unplanned changes. For planned changes, make certain they actually take place as expected; for unplanned changes, minimize discovery time and ensure timely response where needed.

The Smart Choice: NetWrix Group Policy Change Reporter

NetWrix Group Policy Change Reporter incorporates knowledge and understanding of the needs of Group Policy change auditing personnel. It is a cost-effective solution offering competitive functionality at a low price. Group Policy Change Reporter places Group Policy change information directly at the administrator's fingertips, without the need to extract it by roundabout methods.

The advanced reports provided with the product are based on SQL Server Reporting Services technology. Another feature essential for compliance is long-term archival of audit data.

Group Policy Change Reporter comes in two versions: freeware and commercial.

The freeware version can be used indefinitely, and is suitable for small businesses with lenient auditing requirements.

The commercial version is available as a free download. This version is as easy to use as the freeware version, but includes many advanced features. It is fully enabled for a 20-day evaluation period. To continue using the product after the expiration of the evaluation period, you must purchase it from NetWrix.

For details, see http://netwrix.com/group_policy_change_reporting.html.

©2009 NetWrix Corporation. All rights reserved. NetWrix and Group Policy Change Reporter are trademarks of NetWrix Corporation and/or one or more of its subsidiaries, and may be registered in the U.S. Patent and Trademark Office and in other countries. All other trademarks and registered trademarks are the property of their respective owners.