Gaining Control of Server Configurations
Table of Contents

1. Introduction 3
2. Auditing for Compliance 3
3. How Change Auditing Relates to Change Management 4
   3.1 Critical versus Inconsequential 4
   3.2 Planned versus Unplanned 4
   3.3 Noise versus Signal 4
   3.4 Inadvertent versus Malicious 5
4. Case in Point: Server Configuration Changes 5
   4.1 Native Tools 5
   4.2 Building versus Buying 6
   4.3 Third-Party Software 7
   4.4 Success Recipe 7
5. The Smart Choice: Netwrix Auditor 7
6. About Netwrix Corporation 8
Introduction

Change is normal in every IT infrastructure. The rate of change varies, but it is considerable. IT infrastructure cannot remain static because:

- Its components are interdependent; change to one necessitates a series of changes in others.
- Its components are dynamic and flexible, capable of supporting diverse configurations.
- It must reliably handle a huge volume and diversity of information that enterprises rely on for variety of unrelated tasks.
- The rate of changes, though varied across the range of tasks, is considerable.

IT is entrusted with aspects of company life that are easier to change than other structures. IT infrastructure that becomes stale can lead to disruption of operations. However, for the same reasons that information flow should not stagnate, changes to IT should not go unwatched. Change must be managed carefully because adverse consequences of change 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 have to be factored in to avoid failed audits and fines.

How to make sure that all necessary changes occur successfully and unwanted changes have the least possible negative effect? This white paper describes approaches to change auditing, explains how audit data can be used for change management, and focuses on the configuration of servers.

Auditing for Compliance

Data about IT systems operations must be continually recorded for possible use by systems managers and outside auditors in auditing changes. Systems administrators use recent audit data to monitor operations and diagnose problems as they arise. Outside auditors use data recorded over time to verify compliance with regulations.

Some recorded data must be kept for a long time – up to seven years – in order to comply with regulations. The scope of data stored should be sufficient to satisfy any requests from external auditors, and it should be as detailed as possible. For example, if an external auditor needs to know how firewall settings were changed at some time, or need to view a complete history of hardware changes on an application server for the past year, the requisite data should be readily available for analysis.

The diversity of regulations makes it necessary to ensure that available data is copious and highly detailed to avoid the risk of noncompliance.
How Change Auditing Relates to Change Management

Change management is a continuous process of deciding what kinds of changes to 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 to be inspected, especially not when the volume of changes is routinely overwhelming. However, attention can be guided by clear-cut criteria to assess changes.

Critical versus Inconsequential

Prioritizing changes helps build a strategy for managing change. Changes vary in priority according to the consequences they cause. For example, a device that stops working after a driver update is more important than installation of a video-game server that is not allowed. A detailed data trail makes it possible to detect and respond to both situations.

Critical changes should be watched for constantly and responded to quickly. Many such changes are familiar and trivial to track; this helps reduce the number of critical changes that need special attention.

Planned versus Unplanned

Unanticipated changes cause problems. They are the primary cause of outages, and if they are frequent and are not prevented they may cause a failed security audit. Such changes should be monitored. However, planned changes should also be monitored to ensure that they happen on time and without policy violations.

An example of a planned change is the adjustment of network settings. Sometimes this causes unforeseen issues, such as a failure of production software that relies on DNS resolution. Such high-priority changes should not fall under the radar; care should be taken to ensure that they have the expected results. Likewise, deployment of add-ins to important software must be recorded; for example, a useful but poorly implemented extension might cause Outlook to crash, making mail unavailable. A meaningful change that is not typical is usually unplanned.

Noise versus Signal

Some events in audit trails unambiguously indicate important changes. These events are easy to track. For example, the addition of a new startup program on an application server is a significant event that requires immediate attention; the program may cause long startup times and lower quality of service.
The proportion of useful information in audit trails is never large. Many events are normally logged even for minor changes. It is not possible to know in advance what kinds of data will be useful. Even minor events may need to be correlated to diagnose the cause of a problem. An event may be part of background noise, or the same type of event may accompany a critical change, depending on what other events were logged at around the same time. If a server unexpectedly stops working, the more complete the recent audit data, the better the chances of restoring the initial state of the server. An emergency may require examination of data ordinarily considered unimportant.

**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 tracks. Inadvertent changes are often reversible.

It can be difficult to tell whether a change was intentional. For example, a hardware device may disappear from the configuration of a server. Possible explanations are that the device failed or was removed (perhaps stolen). To investigate and solve the problem requires a detailed record of what happened.

The reverse situation — if someone installs a new device — is unlikely to be driven by malicious motives but is not necessarily harmless. The addition of a hardware device may cause the server to stop performing some or all of its functions. You should keep track of all newly added hardware and take appropriate action in case of any undesirable impact.

Prioritizing the changes helps you build your change management strategy.

**Case in Point: Server Configuration Changes**

Servers of various types are the driving force of business and the means of providing services to outside clients. Changes to the configuration of a server can bring business to a standstill. Tools used for managing changes in server configuration must be able to cope with an enormous amount of audit data. This section discusses the main approaches to managing changes in IT environments for production.

**Native Tools**

Windows MMC-based native tools, such as Event Viewer and others, constitute an entry-level solution. 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 meaningful change management.

Even with a well-designed change management strategy, native tools cannot significantly reduce the effects of adverse changes, because of the high latency between a change and its discovery and inadequate reporting capabilities. A change is not examined until after it has caused a negative result, such as a service failure or slowdown of operations.
Moreover, the process of manual examination is inefficient and painful. Several seemingly unrelated sources sometimes need to be analyzed to put an event into context.

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

**Building versus Buying**

The search for methods of automating and analyzing changes in the IT infrastructure can lead a company to invest in in-house software. A wide range of technologies can be employed in its development: PowerShell, the .NET framework, and many other programming and scripting languages have bindings for Windows APIs, which are extensively documented.

The following tasks are well-suited for automation:

- **Subscribing to events** — watching for anticipated events can be efficient because you know what kinds of events to look for.
- **Handling event logs** — backing up, archiving, and clearing logs for compliance and auditing continuity.
- **Querying for events** — centralizing the search for events and making it more efficient.

This list can continue depending on the specific needs of an organization. It can grow quite long because of the comprehensive scope of available functionality.

The effectiveness of in-house development is determined not so much by what is possible as by what can be done in the given time with the given resources. If a company does not specialize in change tracking software — and most do not — then the time and resources are bound to be too scarce for comfort.

Even if an in-house solution is good, its development is certain to entail problems:

- **Support**: Software produced in-house may have many authors, which increases the difficulty of support; 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 testing, a process that demands time and expertise.

In-house scripts and programs may be the optimal solution for some companies, but this is rarely the case in large distributed environments that have to accommodate heterogeneous systems and both internal and remote clients. In most cases, third-party software that has been specifically designed for managing changes in server configuration will provide a more cost-effective and better-quality alternative.
Third-Party Software

When it comes to choosing a third-party solution for server configuration 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 on their own cannot solve complex problems in server configuration change auditing, tracking, and management.

Success Recipe

To be effective at tracking server configuration changes, it is equally important to have 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.

Changes should be prioritized by importance, relevance, and purpose. Planned and unplanned changes should be differentiated. Planned changes should be verified to make sure they take place as expected; for unplanned changes, discovery time should be minimized and timely response ensured.

The Smart Choice: Netwrix Auditor for Windows Server

Netwrix Auditor for Windows Server incorporates knowledge and understanding of the needs of personnel who audit changes in server configuration. This is a cost-effective solution that offers competitive functionality for a low price. It places information at an administrator's fingertips, without the need to extract it by roundabout methods. It provides reports that are suitable for ensuring SOX, HIPAA, GLBA, and FISMA compliance, and offers long-term archiving of audit data.

The alternative freeware tool may be used indefinitely and is suitable for small businesses with flexible auditing requirements.

The fully functional Netwrix Auditor for Windows Server is available as a free 20-day trial. It is as easy to use as the freeware tool, but also includes many advanced features.
About Netwrix Corporation

Netwrix Corporation is the leading provider of change auditing software, offering the most simple, efficient and affordable IT infrastructure auditing solution with the broadest coverage of audited systems and applications available today. Founded in 2006, Netwrix has grown to have thousands of customers worldwide. The company is headquartered in Irvine, California, with regional offices in New Jersey, Ohio, Georgia and the UK.