Extending Change Auditing to Exchange Server
Table of Contents

1. Introduction ................................................................. 3
2. Change Auditing for Compliance ........................................ 3
3. Why Change Auditing Is Vital ............................................ 3
4. Auditing Toolset for Exchange Server Changes ....................... 5
   4.1. Bundled Tools .......................................................... 5
   4.2. Building versus Buying .............................................. 5
   4.3. Third-Party Software ................................................. 6
   4.4. Success Recipe ....................................................... 7
5. The Smart Choice: Netwrix Auditor for Exchange ..................... 7
6. About Netwrix Corporation ............................................... 7
Introduction

Email systems are among the most critical objects in the IT infrastructure of an enterprise. Problems with email systems can cause communication breaches, disrupt operations, or even jeopardize jobs at the company.

Companies take a lot of precautions against unauthorized access to email servers and hardware failure on those machines. However, preventive and protective measures don't help to find the cause of a contingency if it does occur. For that purpose, mail infrastructure and security configuration should be constantly audited, enabling you to investigate problems and minimize the effects of adverse changes.

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

This white paper describes approaches to change auditing for the most widespread email system technology: Microsoft Exchange Server.

Change Auditing for Compliance

Audit data must be kept for a very long time, up to 7 years according to some regulations. The scope of the stored data should be sufficient to satisfy any requests from the auditors, and be as detailed as possible. For example, if an auditor needs to view a complete history of permissions on an Exchange mailbox store for the past year, the requisite data should be readily available for analysis.

The diversity of the regulations makes it necessary to ensure that the audit data is copious and highly detailed. Otherwise, the organization runs the risk of noncompliance.

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 guilty party will be held responsible for damaging actions.

Why Change Auditing Is Vital

Consider an email system that does not audit administrative activity. This is a common situation, but that does not make it acceptable. If there is no auditing, any problems related to security and maintenance cannot be dealt with efficiently. In fact, most of them are not even discovered. Only major problems come to light indirectly and belatedly when the company starts to feel their consequences — for example, leaked trade secrets or sabotaged mailboxes.
Auditing on its own cannot prevent problems, but it can help do the following:

- Detect problems early
- Find the causes and solve the problems
- Plan for prevention of such problems in the future

These aspects of Exchange Server auditing are described in detail below.

**Detection**

If a problem occurs, it should be discovered as soon as possible, before it can cause an outage or impede operations. Email systems and mailboxes should be monitored closely.

The addition of a new Exchange Server is an extremely significant event that should be immediately examined, because a “rogue” server may completely invalidate the configuration of an Exchange organization. Even less conspicuous activity such as moving mailboxes from one server to another should not fall under the radar, because it affects the users who own the mailboxes. Unless the mailbox is moved during Exchange migration or due to the user changing offices, mailbox moving is an unplanned event. Such actions are easy to anticipate and track.

Early detection is just as important for some actions that concern sensitive Exchange organization parameters—accepted domains, email policies, journaling, and so on. This is vital both from the common-sense and compliance standpoint.

**Solution**

To solve problems that occur with multiple Exchange servers in an organization, especially if they are managed by multiple administrators, it is important to have a comprehensive body of specialized audit data. Although the share of useful information found in audit trails is never big, there is no way of knowing in advance which parts will prove meaningful. Solutions often begin with investigations into the causes of problems so that the people responsible can be confronted with the evidence and correct the situation.

For example, a mailbox store can be deleted unexpectedly, causing the loss of a number of mailboxes. To find out who did this and when it happened, you will need audit trails.

Sometimes, changes to address book settings can interfere with email users’ ability to find contacts. Without an investigation, it may not be clear whether this was done on purpose or what the original configuration was. To look into the matter and restore the configuration, you need a detailed record of what happened.
Applications

Experience with problems can be converted to preventive measures. As you resolve Exchange issues, your security and hardware configuration can evolve.

For example, to ensure that Exchange Server security conforms to the established enterprise policy, all changes to client access settings should be tracked and analyzed. This area includes technologies (such as Outlook Web Access, POP3 and IMAP, ActiveSync) that are associated with numerous security concerns.

Exchange administrators should also keep track of mailbox creation so that there are no mailboxes for nonexistent users.

Auditing Toolset for Exchange Server Changes

The tools you use for change tracking must be able to cope with the enormous amount of audit data that needs to be examined. This section lists the main approaches used in production IT environments that rely on the Microsoft Exchange Server technology.

Bundled Tools

The auditing facilities bundled with Exchange Server are an entry-level solution. Part of the Exchange Server audit data goes to the Application log, which can be browsed in Event Viewer. The other main audit trail, the Exchange Tracking log, is text-based and lends itself to parsing.

These tools have the advantage of requiring no customization or third-party software, but even in a mid-size IT infrastructure, they are not suitable for performing any meaningful change management, because the manual examination and correlation process is inefficient and tedious.

Even with a well-designed change management strategy, bundled tools cannot significantly reduce the effects of adverse changes because of 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, but 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 other programming and scripting languages have bindings for the Exchange and Windows APIs.
The following tasks are well-suited for automation:

- Subscribing to events — watching for the events you anticipate is very efficient as long as you know what kind of event you are looking for
- Handling text-based logs — parsing, 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 might be longer depending on the specific needs of an organization. It can grow quite long due to the comprehensive scope of available functionality.

The effectiveness of in-house development is determined not so much by what it is possible to do but by what can be done in the given time with the given resources. If the company does not specialize in Exchange Server change auditing software — and most companies do not — the time and resources necessary 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 lot 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. More often, a more cost-effective and better-quality alternative is to purchase third-party software specifically designed for Exchange Server change management.

**Third-Party Software**

When it comes to choosing a third-party solution for Exchange Server 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 Exchange Server change auditing, tracking and management problems.
Success Recipe

To be effective at tracking Exchange Server changes, it is 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. Good change auditing tools together with a sound audit policy have the additional benefit of helping you improve the management of your Exchange servers.

The Smart Choice: Netwrix Auditor for Exchange

Netwrix Auditor for Exchange incorporates knowledge and understanding of the needs of Exchange Server change auditing personnel. It is a cost-effective solution offering competitive functionality for a low price. The product places change information directly at the administrator’s fingertips, without the need to extract it using roundabout methods.

For each captured change, all possible detail is shown: who made the change, when it happened, the “before” and “after” settings, and so on.

The reports generated by the product are suitable for ensuring SOX, HIPAA, GLBA, and FISMA compliance. Another feature essential for compliance is long-term archival of audit data.

To learn more about Netwrix Auditor for Exchange, please read its overview or download a free 20-day trial.

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.