Practical Change Auditing for Virtual Environments
Table of Contents

Introduction 3
Change Auditing for Compliance 3
Why Change Auditing Is Vital 3
  Detection 4
  Solution 4
  Anticipation 4
Auditing Toolset for Virtual Environment Changes 5
  Bundled Tools 5
  Building versus Buying 5
  Third-Party Software 6
  Success Recipe 6
The Smart Choice: Netwrix Auditor for VMware 7
About Netwrix Corporation 7
Introduction

Platform virtualization has become a cost-effective alternative to maintaining multiple physical systems. Virtualization owes its popularity to such benefits as flexible performance leveraging, reduced downtime, and business agility. Many tasks previously performed by physical hosts, including business-critical operations, can now be done by virtual systems.

Virtual machines can be among the most critical objects in the IT infrastructure of an enterprise; therefore, auditing these systems is just as important as auditing actual servers. At the level of the operating system, there is little difference whether a machine is virtual or physical for auditing purposes; however, the underlying infrastructure of the virtual machine pool adds a whole new level of auditing needs: it is necessary to keep track of resource utilization, host pool management, and so on.

In addition, IT staff must deal with compliance regulations. SOX, HIPAA, GLBA, and FISMA compliance measures are not dictated by internal needs but must still be considered for smooth functioning of the enterprise.

Change Auditing for Compliance

Audit data must be kept for a very long time, up to seven years by some regulations. The scope of the stored data should be sufficient to satisfy any requests from auditors, and be as detailed as possible. Whether an auditor needs to know who changed memory allocation settings on an ESX server at some point or wants to view a complete history of hardware changes on a virtual machine for the past year, the requisite data should be readily available for analysis.

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

Why Change Auditing Is Vital

Consider a virtual machine environment where administrative activity is not audited. This is a common situation, but it is not acceptable. Lack of auditing means that any problems related to security, load balancing, or maintenance cannot be dealt with efficiently. In fact, most of these types of problems are not even discovered. Only major problems come to light indirectly, and then belatedly, when the company starts to feel their consequences — for example, denial of service or slowdowns.

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 virtual environment 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. The more important the services provided by the virtual machine host, the more closely it should be monitored. If resource pool parameters are changed, globally affecting production virtual machines, this should be reported the same day. The situation can be investigated promptly, before it can impact productivity.

Early detection is just as important for some actions that are not nearly as intrusive. The addition of a new ESX server to a Virtual Center is a significant event that should be immediately examined; even such sneaky activity as creation of a number of virtual machines for no apparent reason should not slip under the radar. Such actions are easy to anticipate and track.

Solution

To solve problems occurring in a virtual environment, 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 the people responsible can be confronted with the evidence and correct the situation.

For example, a good-state virtual machine snapshot can be replaced with an invalid snapshot. To determine who invalidated the snapshot and when it happened, you will need audit trails.

Sometimes, RAM size settings can be changed for multiple VMWare virtual machines, resulting in ESX server overload and slowdown of other machines. Without an investigation, it may not be clear whether the settings were changed on purpose or what the original memory quotas were. To look into the matter and restore the configuration, you need a detailed record of what happened.

It may also be necessary to find out where the files defining a particular virtual machine have gone. To track them down, you will need audit data ordinarily considered unimportant.

Anticipation

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

For example, if your virtual environment has been in production use for only a short time, permissions on virtual machine containers may not be configured optimally, but after you gather and study use statistics, you can confidently decide to whom to grant access to which resources. On a different note, if a host periodically experiences slowdowns, it might be a good time to increase the amount of RAM.
Auditing Toolset for Virtual Environment 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 virtualization technologies from the leading vendors: VMware and Microsoft.

Bundled Tools

The auditing facilities bundled with the most popular virtualization products are an entry-level solution. Microsoft records audit data to multiple event logs that can be browsed in Event Viewer; VMware provides similar functionality. These tools have the advantage of requiring no customization or third-party software, but even in a midsized IT infrastructure, they are unsuitable for meaningful change management because the manual examination and correlation process is inefficient and painful.

Even with a well-designed change management strategy, bundled tools cannot significantly reduce the effects of adverse changes because of the latent effects of those changes and lack of reporting capability. A change is not examined until after it has caused 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 has bindings for Microsoft virtualization solutions, and VMware’s text-based logs lend themselves to parsing.

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 the kind of event you are looking for.
- Handling event logs — backing up, archiving, and clearing logs for compliance and auditing continuity.
- Querying for events — centralizing 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 possibilities as by what can be done in the given time with the given resources. If the company does not specialize in change auditing software—and most companies do not — then the 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, increasing 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, requiring a lot of time and expertise.

In-house scripts and programs may be the optimal solution for some companies, but this would be a rare case in large distributed environments that must 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 virtual environment change management.

**Third-Party Software**

When it comes to choosing a third-party solution for virtual environment 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 virtual environment change auditing, tracking, and management problems.

**Success Recipe**

To be effective at tracking virtual environment changes, it is important to have a sensible strategy and software tools flexible enough to meet all your needs without getting 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 virtual environments.
The Smart Choice: Netwrix Auditor for VMware

Netwrix Auditor for VMware is a cost-effective solution offering competitive functionality for a low price. It places change information directly at the administrator’s fingertips, without the need to extract it by roundabout methods. For each captured change, all possible detail is shown, including the “before” and “after” settings.

Netwrix Auditor for VMware is a comprehensive solution that gives you complete visibility into all changes made within your VMware ESX, ESXi and vSphere environment. Based on the award-winning Netwrix Auditor platform, this solution covers critical areas of VMware reporting and auditing.

The advanced reports provided with the solution are suitable for ensuring SOX, HIPAA, GLBA, and FISMA compliance. Another feature essential for compliance is long-term archiving of audit data.

To learn more about Netwrix Auditor for VMware, 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 solutions 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.