



## **PEOPLE AUDITING**

**Why Are We Ignoring the #1 Cause  
of Downtime and Security Breaches?**

**A Troubleshooting Process Whitepaper**

**MARCH 2008**

---

## Table of Contents

<i>Executive Summary</i>	1
<i>The Challenge of Human Errors</i>	2
<i>The Limitations of Log-Based Troubleshooting</i>	4
<i>People Auditing</i>	6
<i>Conclusion</i>	9
<i>About ObserveIT</i>	9

---

## Executive Summary

Companies are investing in high-availability systems and performance monitoring solutions for data centers, but are failing to follow best practice procedures to avoid human errors.

As complexity grows in IT infrastructure, administrators are searching for solutions that will help them effectively monitor and maintain these environments. But oddly enough, the simple question “Who last accessed the server and what did he do?” remains one of the toughest questions to answer. This is despite the variety of system management tools in use today. It is not enough to just monitor servers and applications when the #1 cause for server downtime is human error. Ask an expert about high availability, and the conversation quickly turns to the subject of human error.

The problem of maintaining uptime is exacerbated by the increased dependency on outsourcing, offshore consultants, temporary employees and developers that administer servers and software from multiple vendors. This situation brings a decrease in direct accountability. Furthermore, the geographic dispersion of admin-level access makes verbal investigation more complicated by orders of magnitude.

To achieve efficient operations, administrators need a holistic view of the entire IT infrastructure, including monitoring of human factor.

By adding user activity auditing as a core property of system monitoring platforms, IT departments can easily achieve higher availability, through faster problem identification and time to resolution. In addition, thorough People Auditing demonstrates that employees and partners are meeting established guidelines for information access, transaction integrity and intellectual property protection.

---

# The Challenge of Human Errors

## *Incorporating Human Error Monitoring Into the System Management Infrastructure*

*In spite of the adoption of monitoring platforms, the processes available for troubleshooting service outages and securing IT servers has remained out-of-sync with the natural human analysis of IT administrators.*

### IT Concerns

#### *Service Outage - Smart Users Making "Smart" Mistakes*

Recent studies show that human errors account for approximately 34% of total outages when counting the *number* of outages. Factoring in the total effect of each incident (as measured by Mean Time to Repair and amount of lost data), 56% of total *server outage impact* comes as a result of human error.

Outage Type	Percentage of Incidents	Total Impact (Downtime / Data Loss)
System Error	66%	44%
Human Error	34%	56%

For system errors, the tedious process of log analysis has been alleviated partially by the adoption of system monitoring platforms and software profiling utilities.

But for human errors, administrators remain at a loss for assistance when searching for potential causes. There is no indicator that "This is probably a human error", or even the simple statement that "Someone touched this server around the same time as the start of the problem."

A correlary of this issue is that smart users make the "smartest" mistakes. They know the nooks and crannies of arcane configuration files that might tweak an extra 5% of performance out of the system. These nooks and crannies are subsequently the most difficult to find when they go wrong.

#### *Compliance Auditing and Security*

In today's world of compliance regulations, an additional trend of outsourcing, temporary contract employees and remote IT support staff creates a significant loophole to compliancy efforts: This rise of outsourcing brings with it a rise in mission-critical data being handled via Remote Desktop Protocol (RDP).

Of course, the bottom-line compliance responsibilities remain solely in the hands of the core IT team. *You can outsource Support, but you can't outsource Compliance.* IT

managers today may know how their platforms are secured from external access, but the question “How can we be sure that third-party vendors with RDP access are not accessing data that they should not be touching?” is more difficult to answer.

### ***How Human Error Differs from System Error***

There are a few fundamental differences between system errors and human errors, and the way that they each need to be managed.

The first basic difference is repeatability. For system errors, finding the problem is equivalent to fixing the problem. If your troubleshooting process leads to a conclusion that a NIC card is not working, then swapping in a new card closes the issue, and you can sleep well that evening.

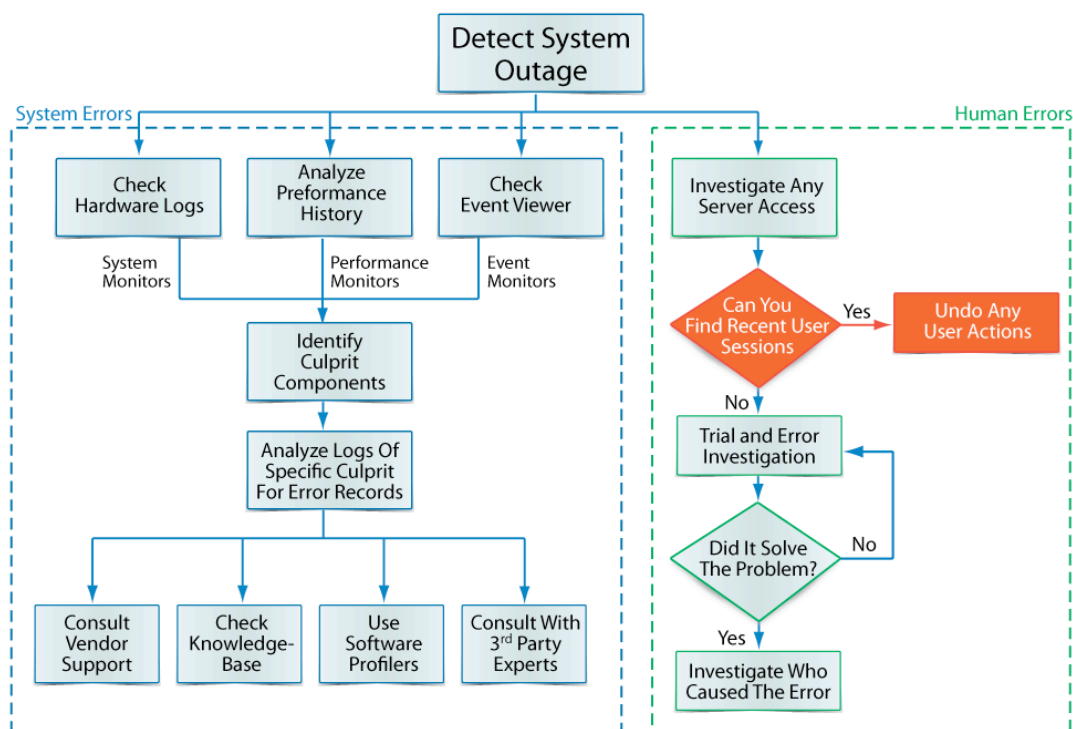
Human errors are not this direct. If you find an improper configuration file and swap it with the correct configuration file, the problem may be solved temporarily. But when you go to bed that night, you’re probably still scratching your head, wondering who or what caused this error, and whether it will happen again tomorrow.

# The Limitations of Log-Based Troubleshooting

## A Counter-Intuitive Approach For Human Error Analysis

The art of troubleshooting always starts with eliminating as many possible causes as possible, to answer the question "Why would a server that worked yesterday suddenly stop working?" Without a clear indication of what has changed on the server, IT administrators must employ a tedious trial-and-error process. If a verifiable indicator could show all human interaction with the server, a significant percentage of possible causes could be analyzed or eliminated immediately.

### Troubleshooting Process



### 'Who Touched This Server?'

The first thought that comes to mind of any IT administrator during a system outage is "Who touched this server?" If (and this is a very big If) the question can be answered, it has two benefits. In most cases, it immediately points to the cause of the outage. And even if it does not, it at a minimum will eliminate some subset of the other possible causes. Surprisingly, most IT administrators do not have an easy way to answer this question.

## Why Troubleshooting is Different for Human Error

Troubleshooting human error needs a different approach than troubleshooting software and hardware system errors. To solve human errors, you want to log what users did rather than digging through logs of system changes.

For system errors, the tedious process of log analysis has been alleviated partially by the adoption of system monitoring platforms and software profiling utilities.

But for human errors, administrators remain at a loss for assistance when searching for potential causes. There is no indicator that "This is probably a human error", or even the simple statement that "Someone touched this server around the same time as the start of the problem."

---

## People Auditing

### *Troubleshooting That Follows Our Own Human Logic*

*Deploying a system such as ObserveIT that audits all user activity will dramatically improve troubleshooting effectiveness as well as strengthen security and compliance assurances*

#### **ObserveIT In a Nutshell**

ObserveIT provides visibility into all user activity within any window server session, whether they are performed through remote access or console access. With support for Terminal Services, Citrix, Remote Desktop, PC-Anywhere, VNC and NetOP, ObserveIT is agnostic to protocol and to client application. In addition to capturing all screen activity for each user action, ObserveIT extracts meta-data on the state of the OS and the application in use, enabling precise identification of user actions and impact. No matter what method of user access, all activity can be searched and replayed in a single unified view.

#### **Starting With the Most Obvious Question - Who Did What?**

ObserveIT turns the troubleshooting process upside down, by allowing administrators to follow your own natural instincts. If your first question is "Who did what on which server?", ObserveIT follows through with an immediate and thorough answer to this question.

#### **Solving the Most Important Problem Quickly**

With human error being responsible for 56% of server outages, ObserveIT lets you solve your most painful problems in the most direct path possible:

1. See what was done.
2. Undo it.

#### **The Monitoring Safety Net**

Log analysis is like a safety net: It has to be there, but truth be told, you really don't want to use it. If you are using it, something must be drastically wrong. Any safety net is best augmented with safety ropes tied to the actual work location.

Having detailed log collection provides you with coverage in almost any instance of failure. But coverage is not the whole story, and any root-cause monitoring can augment the log collection security. With ObserveIT, you achieve significantly faster corrections to server outages, without losing any of the safety net assurances that log analysis can provide, for cases where human activity is not involved in the outage.

#### **Video Recording and Session Meta-Data**

For each session, ObserveIT records all window activity, enabling you to replay the entire session and see exactly what transpired. When you can see the window actions

performed by a user, it removes all doubt about what *might have* caused a certain change in system configuration.

In addition to capturing video recordings of screen activity, ObserveIT also extracts meta-data of all application and window elements, allowing detailed indexing and searching. This makes culprit analysis even faster, allowing you to drill-down to the exact recordings that matter, even without replaying a single frame.

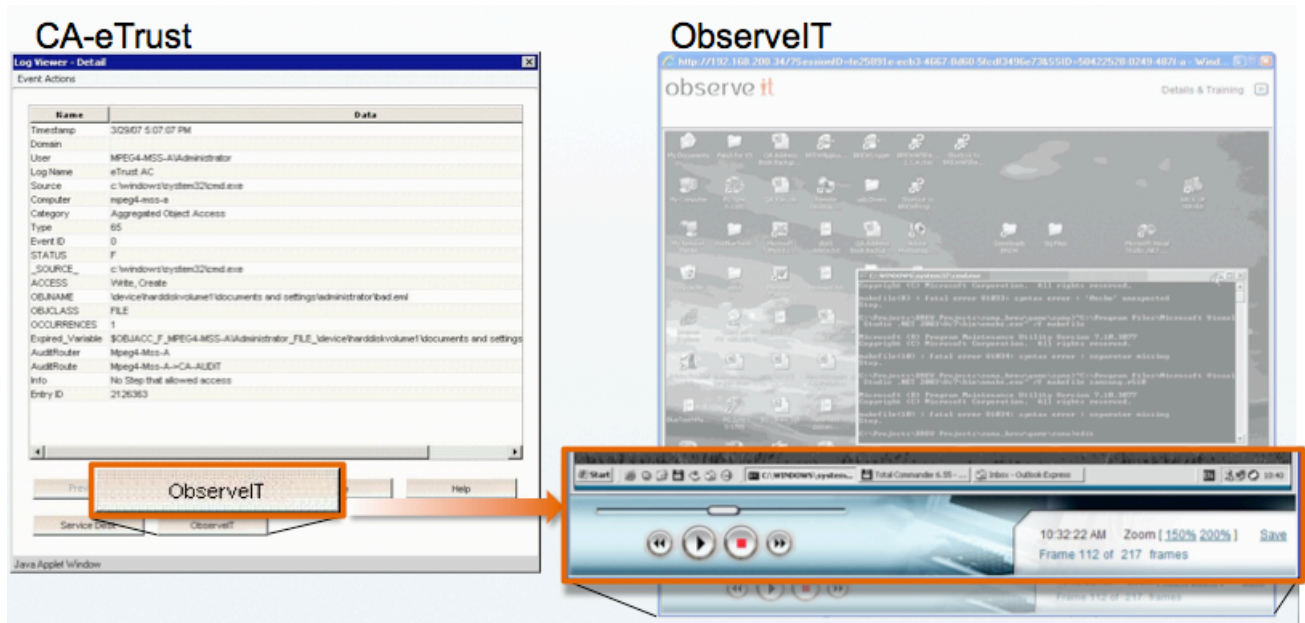
The screenshot displays the ObserveIT Agent Diary interface. The top navigation bar includes 'Agent Diary', 'User Diary', 'Configuration', 'Search', 'Reports', 'Admin Tasks', 'Training', and 'Logoff'. A notification states 'This Demo version will expire in 59 days'. The 'Agent Diary' sidebar on the left lists 'Tasks', 'Bookmarks', 'Inventory', and 'Software'. The main 'Activity View' section shows filters for 'Agent' (OITMOM) and 'Up to' (September 2007). Below the filters, a table lists activity results:

Hour	Login	User	Client Name	Slides	Video
10:36 AM	Administrator	Andrew	AndrewWS	37	[Video Icon]
3:54 PM	Administrator	gaby	GabyPC	44	[Video Icon]

Overlaid on the interface is a 'Registry Editor' window. The left pane shows the tree structure expanded to 'HKEY\_LOCAL\_MACHINE\SOFTWARE\JavaSoft\Java Plug-in\1.5.0'. The right pane shows a single registry value: Name: (Default), Type: REG\_SZ, Data: (value not set). The taskbar at the bottom shows the Start button, taskbar with '13 Windows Explorer', 'SQL Query Analyzer', '5 Microsoft Manage...', and 'Registry Editor'. A video control bar at the bottom right shows '7:04:03 AM', 'Zoom [150% 200%]', and 'Frame 45 of 59 frames'.

## Integrating with Monitoring Tools

By incorporating user activity auditing in your system management infrastructure, ObserveIT makes it easy for you to achieve high availability. Any system alert provided by monitoring tools are automatically enriched with information showing any user actions that took place on the server in question, or at the time in question, or even those that used a particular resource in question.



## Enhancing Compliance

ObserveIT provides ongoing risk management and regulatory compliance with full documentation of all user sessions. By eliminating any doubt of what is happening in your server environments, and by tying each activity to a specific user, your compliance records gain a new level of reliability. This compliance strength is provided automatically, according to any policy rules desired.

## Automated e-Discovery

By recording every user session, ObserveIT provides direct evidence for any security related research. The e-Discovery capabilities of ObserveIT serve as hard evidence for existing legal or disciplinary actions, and also act as a deterrent. When admin-credentialed users know that user sessions are recorded, they are less likely to break security policy.

---

## Conclusion

Most IT organizations today utilize system monitoring platforms that are efficient for system error troubleshooting, but are ineffective when diagnosing human-generated errors. These human errors – which represent over half of all downtime and data loss – are best handled by focusing on the root cause: *What was done on this server, by whom?*

Answering this root-cause question will bring drastic improvements in troubleshooting effectiveness, and will also enhance security and compliance robustness. The answer to this root-cause question is achieved quite easily via thorough recording and indexing of remote desktop and terminal sessions. A robust, enterprise-ready platform such as ObserveIT will provide coverage of all user sessions, with immediate drill-down to the precise information you need.

---

## About ObserveIT

Established in 2005, ObserveIT Inc. focuses on developing ingeniously easy-to-operate tools that simplify the business of troubleshooting and monitoring server and workstation activity across the enterprise. Founded by System Administrators with years of IT Management experience and the frustration of user-initiated server downtime, we believe in simplicity of solutions and visibility of user activity.

Our focus on simplicity and visibility represents itself not only in our product development. We also commit to these goals in our entire business operations: Affordable pricing with simple licensing terms, fast, friendly customer support, and dedication to continually fulfilling the core requirements of our user community.

ObserveIT is a privately held company with offices in Albany, NY USA and Tel Aviv, Israel.

ObserveIT R&D Headquarters:  
5 Haarad Street  
Tel Aviv, Israel  
69710

Tel. +972 (0)3-648-0614  
info@observeit-sys.com

US Corporate Office:  
ObserveIT  
25 St. Agnes Lane  
Albany, NY  
12211-2038

Tel. 800-647-6685  
sales@observeit-sys.com