ManageEngine

EventLog Analyzer

Privileged User Monitoring and Audit Using EventLog Analyzer

Solution Brief

Privileged User Monitoring and Audit Using EventLog Analyzer

Privileged Users, like Network Administrators, System Administrators, and Database Administrators all have unrestricted access to all the critical servers, applications, and databases in an enterprise. They have the powers to create or remove user profiles and manage user privileges. Their job function is critical for the business continuity of the organization and necessitates such unfettered access and supreme privileges.

External Threat

Through backdoor entry programs, once a network resource is compromised, hackers often go after Privileged User credentials leading to incidents of identity theft. This enables them to access business critical systems, read sensitive data, and ultimately cause the maximum damage to a business.

There is a saying in Latin '*Quis custodiet ipsos custodes?* ' Which if literally translated means '*Who will guard the guards themselves?*' and it is this false sense of security, associated with Privileged Users, that Hackers leverage to gain access to networks without leaving a trace!

Insider Threat

The infamous Wikileaks fiasco underscores the key challenges that governments and organizations face due to threats from within. According to the 2011 CyberSecurity Watch Survey

" Insider attacks are becoming more sophisticated, with a growing number of insiders (22%) using rootkits or hacker tools compared to 9% in 2010, as these tools are increasingly automated and readily available…..Harm to an organization's reputation, critical system disruption and loss of confidential or proprietary information are the most adverse consequences from insider cyber security events "

The phrase '*With great powers comes great responsibility*' is very relevant for Privileged Users. In real-world when faced with daunting work challenges Privileged Users sometimes undermine their responsibilities and tend to take few shortcuts like sharing their credentials with co-workers, inadvertently granting administrator privileges to unauthorized insiders like consultants, contractors, or partners in violation of the documented IT policy.

The Challenge

Left unchecked, violations in Privileged User activities can lead to misuse and cause irreparable damage to the enterprise's credibility and its very existence. The challenge faced by organizations world over are, the activities of Privileged Users going unnoticed. They could not visualize the security implications of policy violations by the very custodians who are supposed to enforce the policy.

Given the seriousness of the problem, compliance auditors are now demanding monitoring of privileged users to prevent incidents of identity theft and obtain a 360 degree view of user activities, as well as to comply with a wide range of regulatory mandates. The challenge is providing a robust privileged user monitoring and audit capability without affecting business productivity.

The Solution

In this information age, where people and devices communicate in an endless stream of bits and bytes, we need the ability to collect, archive, analyze and visualize all the activities that are recorded by the information systems. WHO, WHAT, WHEN, WHERE, and WHY an incident or event occurred is recorded by

information systems in their logs (event log or syslog). Actions performed by Privileged Users in any information system are also recorded in the machine logs and using solutions like ManageEngine **EventLog Analyzer** (www.eventloganalyzer.com) organizations can now monitor and report on the privileged user activities.

ManageEngine EventLog Analyzer

EventLog Analyzer is a web-based, real time, agent less (optional agents available), event log and application log monitoring and reporting software. It is used by organizations worldwide to generate automated reports for security and regulatory compliance audits like: PCI-DSS , HIPAA , FISMA , SOX , GLBA , and for other custom compliance needs. EventLog Analyzer helps in monitoring enterprise IT resources for internal threats and tightens security policies in the enterprise.

Listen to how a Federal Government Agency benefited from EventLog Analyzer PUMA Reports

Privileged User Monitoring and Audit Reporting with EventLog Analyzer

Within an hour of deploying EventLog Analyzer, it starts collecting and archiving logs from all the network servers and devices. The logs are then analyzed and a detailed Privileged User Monitoring and Audit Report is generated. There are two parts to PUMA reports in EventLog Analyzer: **User Based Reports** and **User Activity Overview Report**

Part 1 : User Based Reports

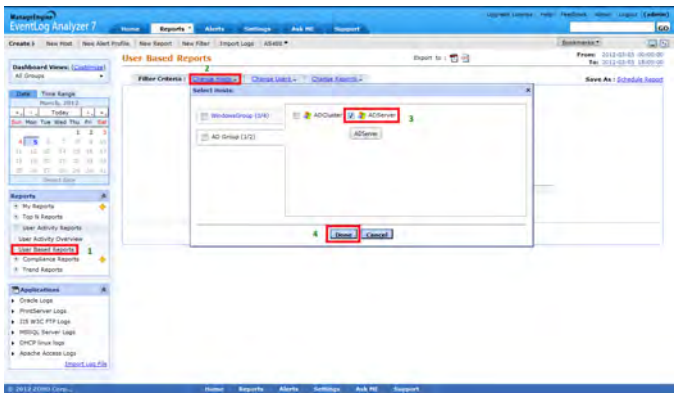
This report displays the user activity events for a specific user or group of users. You can filter for selected hosts, users and events. The following events are displayed in the report graphically:

User Logons , User Logoffs , Failed Logons , Successful User Account Validation , Failed User Account Validation , Audit Logs Cleared , Audit Policy Changes , Objects Accessed , User Account Changes and User Group Change

How to create an User Based Report using EventLog Analyzer:

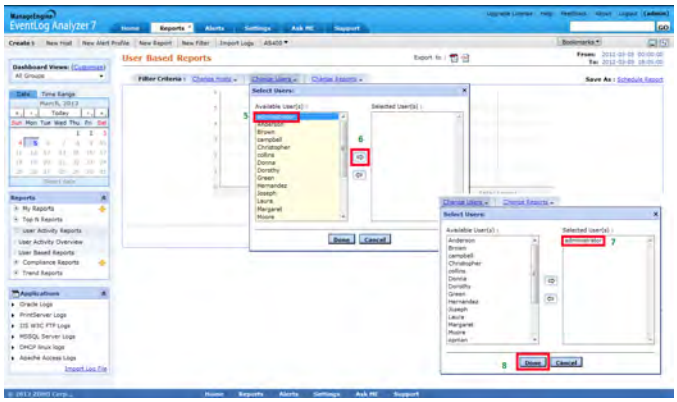
STEP 1

'User Based Reports' are available under 'User Activity Reports'. Select 'Change Hosts' and select the business critical servers (or groups) that should be monitored.



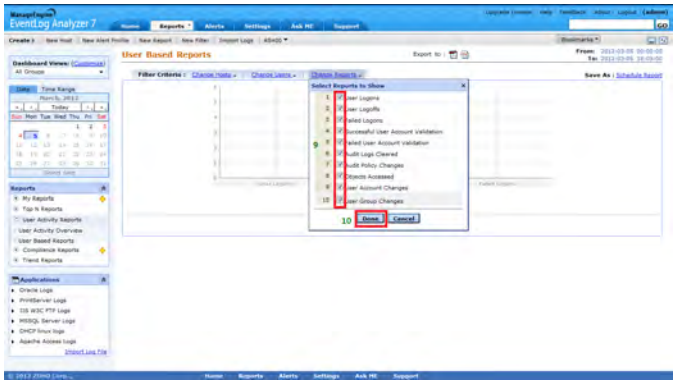
STEP 2

Now click on 'Change Users' and select the privileged users who should be

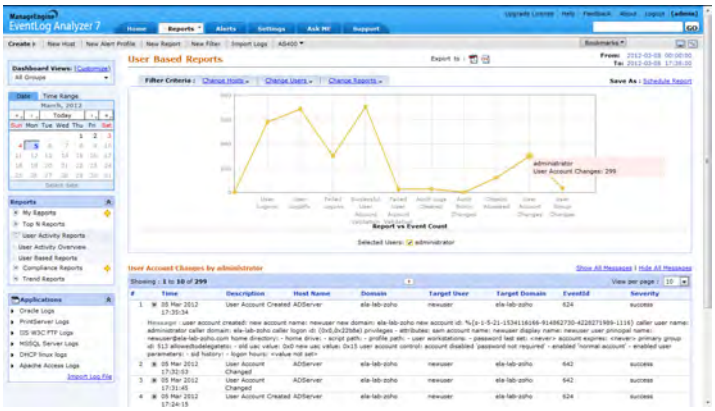


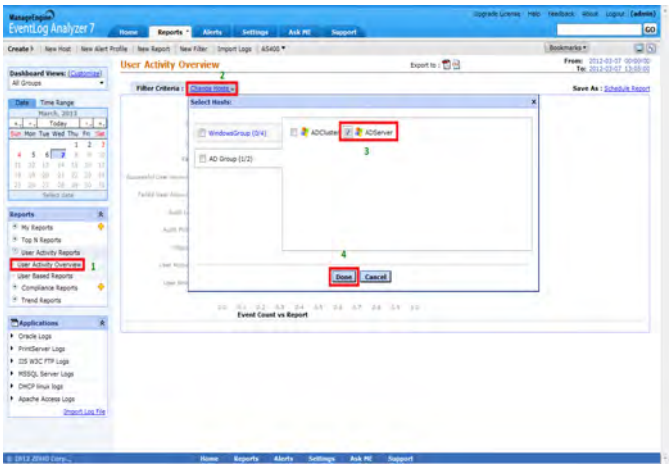
STEP 3

Once the privileged user has been selected, click on 'Change Reports' and select the events which needs to be reported



And the User Based Reports are ready!





Part 2 : User Activity Overview Report

This report, on the other hand gives an overview of the user activity events for a specific host or group of hosts. You can select a specific host of host group. The following events are displayed in the report graphically:

User Logons , User Logoffs , Failed Logons , Successful User Account Validation , Failed User Account Validation , Audit Logs Cleared , Audit Policy Changes , Objects Accessed , User Account Changes and User Group Change

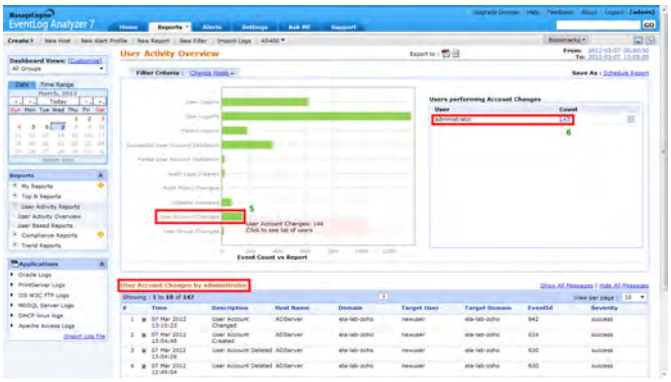
How to create an User Activity Overview Report using EventLog Analyzer:

STEP 1

'User Activity Overview' reports are available under 'User Activity Reports'. Click on 'Change Hosts' and select the business critical servers (or groups) that should be monitored.

STEP 2

Now clicking on any of the events will display the users performing the events, the number of such events and furher details on the target user, target domain, event id, severity, etc.



EventLog Analyzer can be scheduled to generate these PUMA Reports at specified time intervals and automatically emailed, as PDF, to the authorized individuals. The reports can also be exported on-the-fly in PDF or CSV formats which proves very useful during compliance audits.

About EventLog Analyzer

EventLog Analyzer is a web based, real time, agent less (optional agent available), event log and application log monitoring and management software. EventLog Analyzer helps monitoring internal threats to the enterprise IT resources and tighten security policies in the enterprise.

http://blogs.eventloganalyzer.com/ www.facebook.com/LogAnalyzer https://twitter.com/LogGuru

About ManageEngine

ManageEngine delivers the real-time IT management tools that empower an IT team to meet an organization's need for real-time services and support. Worldwide, more than 60,000 established and emerging enterprises — including more than 60 percent of the Fortune 500 — rely on ManageEngine products to ensure the optimal performance of their critical IT infrastructure, including networks, servers, applications, desktops and more. ManageEngine is a division of Zoho Corp. with offices worldwide, including the United States, United Kingdom, India, Japan and China.