E-BOOK

ManageEngine
ADAudit Plus

ManageEngine **ADAudit Plus**

Vs

Windows **auditing tools**

WWW.ADAUDITPLUS.COM

TABLE OF CONTENTS

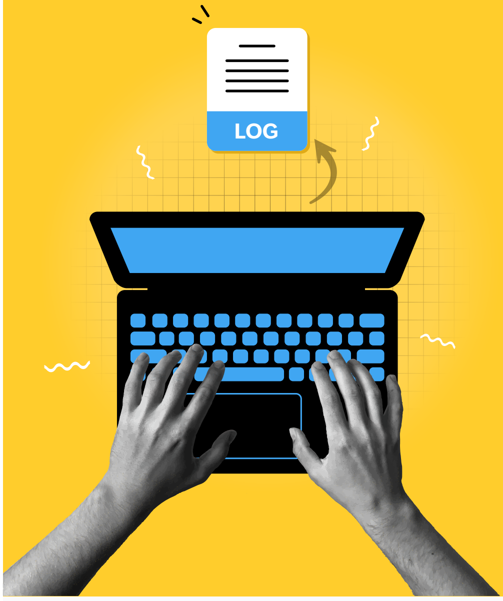
Preface

Auditing is essential for addressing security, operational, and compliance needs in a Windows Server environment. However, inherent limitations in Microsoft Windows security auditing tools—such as the need for expertise, time-intensive processes, and missing capabilities—necessitate the use of third-party auditing tools like ManageEngine ADAudit Plus.

This e-book will take you through five essential capabilities required for AD auditing, the limitations of Windows auditing tools, and how ADAudit Plus helps you overcome them, followed by 15 important use cases where ADAudit Plus beats Windows auditing tools.

Windows auditing tools vs. ManageEngine ADAudit Plus

1. Log aggregation



Broadly speaking, in a domain, authentication and change activities get logged on domain controllers (DCs), while logon activities get logged on the computer where the logon occurs.

Event logs do not get replicated. So, to get a consolidated audit trail of all activities happening across a domain, administrators need to sift through logs on each computer manually, which is not feasible.

To overcome this issue, logs need to be aggregated in a centralized location.

Limitation of Windows auditing tools

Windows Event Forwarding (WEF) can be leveraged to forward specific events from any computer to a Windows Event Collector (WEC) server.

However, successful WEF deployment requires expertise and time as admins need to factor in several considerations, such as collector and forwarder health, cross-domain forwarding, load balancing, and event subscriptions.

Also, WEF is primarily designed for Windows event logs. While it may be possible to forward events from some non-Windows systems, it might not be as seamless or reliable.

Vs

How ADAudit Plus helps you overcome the limitation

ADAudit Plus compiles data from all configured computers across the domain and provides a central repository of audit information with just a few clicks.

Data sources covered by ADAudit Plus, in addition to DCs, Windows servers, workstations, and file servers, include Azure AD and NAS file systems, such as NetApp, EMC, Synology, Hitachi, Huawei, Amazon FSx for Windows, and QNAP.

2. Critical activity detection for improved security

Each Windows activity creates multiple events. For example, the simple act of a user logging on and off of their workstation creates numerous events on their workstation and on the DC that handles their authentication.

Considering the number of users and the activities performed by each one of them, a huge volume of events gets logged on a daily basis. So, spotting a critical activity manually is akin to searching for a needle in a haystack..

Limitation of Windows auditing tools

Task Scheduler and PowerShell scripts can be leveraged to trigger an email whenever a particular event ID is generated. However, Windows cannot raise red flags.

For example, Windows can send you an email every time event ID 4624 is generated, but it will not be able to notify you about logons from a disabled account.

Note: *The **Send an e-mail** capability—which can be found under **Attach Task To This Event** in Event Viewer—has been deprecated by Windows.*

Vs

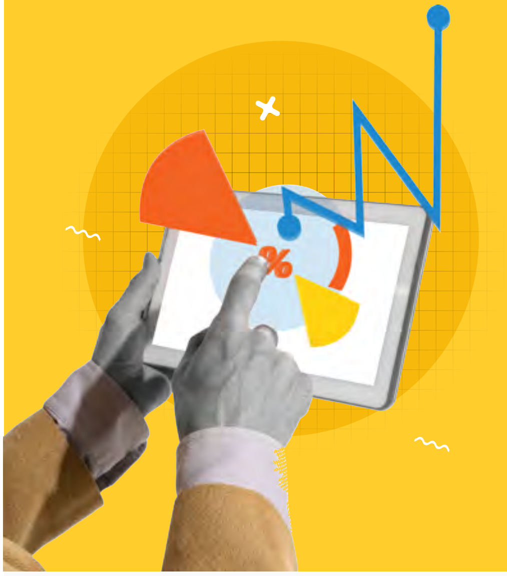
How ADAudit Plus helps you overcome the limitation

ADAudit Plus' alerts let you define thresholds based on the volume, time, and other criteria to detect critical activities such as logons from a disabled account. You can get instantly notified via email and SMS of such activities.

UBA can be leveraged to establish activity patterns and spot subtle anomalies, such as an unusual volume of privileged user activity, that go under the radar of conventional detection systems.

You can also execute scripts to automate response actions, like shutting down a device to mitigate the impact of a security incident.

3. Audit report generation to meet compliance needs



In some cases, individual Windows events provide limited information. For example, before and after values of modified AD attributes are captured in two separate events. This requires correlating multiple events to understand the full change.

Similarly, Windows events capture only the GUID of a GPO and not its display name. To resolve the name of a GPO from its GUID, you need to manually go through the GUIDs of all domain GPOs. Regulations require organizations to capture such vital information in real time.

Limitation of Windows auditing tools

PowerShell can be leveraged to correlate multiple events and resolve the display name of a GPO from its GUID.

However, creating effective PowerShell scripts to audit AD requires expertise and time as admins need to posses a solid understanding of PowerShell and AD as well as perform thorough testing to fine-tune each script.

Also, PowerShell is not suitable for real-time auditing, especially in large Windows Server environments.

Vs

How ADAudit Plus helps you overcome the limitation

ADAudit Plus' built-in reports provide real-time information on the before and after values of AD changes and the names of GPOs that have been changed.

You can also automate the generation and delivery of built-in reports to pass compliance audits with ease.

Apart from the before and after values of changes, another important use case where ADAudit Plus employs correlation is its User Work Hours report. This report provides information on the active and idle time spent by users at their workstations by correlating multiple events related to user logon and logoff times, workstation lock and unlock times, and screen saver start and stop times.

4. Security settings configuration

In a Windows environment, events do not get logged by default.

To ensure that events are logged, advanced audit policy settings must be configured for a domain, and System Access Control Lists (SACLs) must be configured for secured objects, such as users, groups, OUs, GPOs, and files.

Limitation of Windows auditing tools

Advanced audit policy and SACL settings need to be configured, keeping in mind what activities and objects you want to track and the event volume generated by a particular setting.

If important settings are missed, you might miss out on logging critical events. On the other hand, if too many settings are configured, you might end up logging noisy events, which will prevent you from spotting critical ones.

So, successful configuration of security settings again requires expertise and time.

Vs

How ADAudit Plus helps you overcome the limitation

With just a few clicks, ADAudit Plus can automatically configure the required advanced audit policy and SACL settings in your environment—with your consent, of course.

You can also leverage ADAudit Plus' alerts to get notified of changes made to configured advanced audit policies and SACLs.

5. Long-term log retention

Regulations mandate the long-term storage of event logs.

By default, the file size of Windows event logs is limited, and when it is exceeded, new events begin to overwrite old ones.

Limitation of Windows auditing tools

Event log size and retention settings can be configured to ensure long-term retention of event logs.

However, event logs can be lost when a WEC server goes down or when event logs are cleared inadvertently or intentionally.

Vs

How ADAudit Plus helps you overcome the limitation

ADAudit Plus' alerts let you get notified when a configured computer stops sending logs or when an event log gets cleared (and event ID 1102 gets logged). These countermeasures will help you mitigate the loss of audit data.

15 important use cases where ADAudit Plus beats Windows auditing tools

Here is a compilation of 15 of the most searched for AD auditing use cases on the internet. For each of these use cases, we'll discuss how these can be carried out using both Windows auditing tools and ADAudit Plus to show how ADAudit Plus can significantly simplify the process of auditing.

01 Find locked-out accounts.

02 Detect who enabled a user account in AD.

03 Detect who deleted a user account.

04 Monitor FSMO role changes.

05 Audit account logon events.

06 Audit Kerberos authentication events in AD.

07 Detect who deleted a computer account.

08 Detect who added a user to the Domain Admins group.

09 Detect who unlocked a user account.

10 Monitor administrator user activities in AD.

11 Detect who created a user account.

12 Monitor computer activities in AD.

13 Audit process tracking.

14 Detect user password changes in AD.

15 Audit Group Policy changes in AD.

About ManageEngine ADAudit Plus

ADAudit Plus is a UBA-driven auditor that helps keep your AD, Azure AD, file systems (including Windows, NetApp, EMC, Synology, Hitachi, Huawei, Amazon FSx for Windows and QNAP), Windows servers, and workstations secure and compliant. ADAudit Plus transforms raw and noisy event log data into real-time reports and alerts, enabling you to get full visibility into activities happening across your Windows Server ecosystem in just a few clicks.

Here are the **top 10 things** you can do with ADAudit Plus:

Get instantly notified about changes in your Windows Server environment.

Continuously track Windows user logon activities.

Monitor the active and idle time spent by employees at their workstations.

Detect and troubleshoot AD account lockouts.

Get a consolidated audit trail of privileged user activities.

Track changes and sign-ins in Azure AD.

Audit file access attempts across Windows and NAS file systems.

Monitor file integrity across local files residing in Windows systems.

Mitigate insider threats by leveraging UBA and response automation.

Get audit-ready compliance reports for SOX, the GDPR, and other IT mandates.

Here are the

TOP 3 REASONS

why you should choose ADAudit Plus

You can save around $4,226 by automating IT audit report generation using ADAudit Plus. You can check this for yourself using this ROI calculator.

ManageEngine has been named a Gartner® Peer Insights™ Customers' Choice for SIEM for four years in a row now.

ADAudit Plus is licensed on a per-server basis with pricing starting at $595, while other IT auditing solutions are licensed on a per-user basis. With per-server licensing, even with a year-over-year increase in the number of users, you can continue to ingest log data from all sources without having to pay more.

Here are the next steps:

- ✓ To explore ADAudit Plus yourself, download a 30-day trial.
- ✓ To have an expert take you through a demonstration of ADAudit Plus, schedule a call.
- ✓ To see ADAudit Plus in action directly from your browser, launch the instant demo.
- ✓ For more information about ADAudit Plus, visit manageengine.com/active-directory-audit.

Author:

Mahidhar Adarsh,
Product marketer, ManageEngine

Disclaimer: While much care has been taken to prepare this document, we give no warranties whatsoever with respect to its contents, including but not limited to the accuracy of any information contained therein.