ManageEngine
ADAudit Plus

Eagle's eye View

Get a Thorough Monitoring & Sharper View into
Your Windows Server Environment Changes

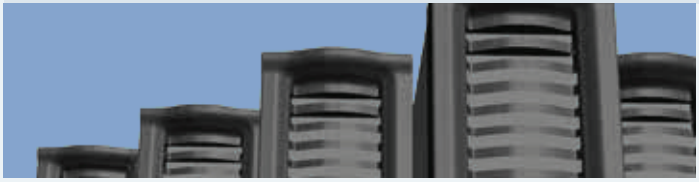
ACTIVE DIRECTORY | WORKSTATIONS | FILE SERVERS | MEMBER SERVERS

Active Directory Auditing

For security reasons, monitoring changes to critical resources are crucial, ADAudit Plus lists the entire information to track information of users Logon / Logoff, GPO, Advanced GPO, Groups, Computer, OU, Configuration, DNS, Permission, Schema changes with 150+ detailed event specific reports and instant emails alerts and also, export the results to xls, html, pdf and csv formats to assist in interpretation and computer forensics!

- Track every change in Windows AD, system, permission, configuration and file modifications by Admin, Users, Helpdesk, HR etc.
- Single Dashboard view of all critical audit data for configured domains.
- View 150+ pre-configured reports and set email alerting for changes to monitored folders / files.
- Meet PCI, SOX, GLBA, FISMA, HIPAA.... Compliance with audit reports in XLS, CSV, PDF and HTML formats.
- Archive AD event data for Security and Forensics.

Workstations Auditing



Administrators can view the exact time of User Workstation Logon & Logoff time along with the Logon Duration. This critical data is at the utmost ease to view in the event of unauthorized entry or regular monitoring. The user workstation actions monitored, audited and graphically reported are 'Logon Duration', 'Logon Failures', 'Logon History', 'Terminal Services Activity', and 'Users Logon Duration on Computers'.

- Track Users' Workstation Logon / Logoff.
- View pre-configured reports; automate periodic reporting with scheduled reports.
- Set email alerts for critical accounts, unauthorized access.
- Logins for IT Auditors with reports view only.

Reports

View from the 150+ pre-configured audit reports with automatic periodic report generation- right to your inbox. 50+ Search Attributes I Schedule email reports | Filter reports on business / non-business / all hours I Browser-based.

Active Directory

Administrators can track all domain events like Logon / Logoff, audit User, Group, Computer, GPO, OU changes with 150+ ready-to-view reports and email alerts. Exportable Reports | Archive Audit Data | Assign Operator roles (reports view only) for Compliance | Much, much more.

File Server

Securely track File Server / FailOver Cluster for document changes to files (file creation / modification / deletion) and folders audit-access, shares and permissions.

File Integrity

Monitor attempted / unauthorized changes to configurations, files (Log, audit, text, exe, web, configuration, DB) and file attributes (dll, exe and other system files). Ensure Windows Servers security and PCI, SOX, HIPAA & FISMA compliance requirements.

Removable Storage

Monitor changes on every removable storage device with reports on all file or folder changes, file read / modified / copy and paste. This feature is supported only in Windows Server 2012 & Windows 8.

Databases

Audit your Windows Server Environment from a choice of database formats: SQL Server, PostgreSQL and MySQL.

Admin

Administrator can audit and monitor with the 150+ pre-configured reports and instant email alerts for a clear view on the Windows Server environment changes.

Compliance

Get specific 'set of detailed graphical reports' for SOX, HIPAA, GLBA, PCI and FISMA to easily meet each compliance requirements.

ManageEn
ADAudit

Alerts

Instant on-screen alerts and emailing of alerts to your inbox! User, time and volume based threshold alerts help identify the problem precisely. Email Notification I Web Based I In-Depth Event Analysis.

Workstations

Monitor every user logon / logoff and know the day-to-day user actions with detailed reports of every successful / failure logon event across workstations in the network.

Member Server

Monitor every Windows Member Server change with various detailed reports: Summary Report, Process Tracking, Policy Changes, System Events, Object Management and Scheduled Tasks.

NetApp

Centrally audit, monitor and report with instant alerts on the NetApp Filer CIFS Shares changes. View reports on files created / modified / deleted, permission changes, failed attempt to file read / write.

Printers

Track all files printed over the Windows network, with thorough reports on the printer usage, recent print jobs, user / printer based reports for added security & SOX, HIPAA Compliance.

Other AD objects

Keep a track on other significant AD Objects: Containers, Contacts, Schema, Configuration, Site, DNS & Permission changes.

Ease of use

Centrally operated, web based, detailed yet simple reports even for non-technical personnel with alerts help answer the four vital Ws: 'Who' did 'what' action, 'when' and from 'where'! Also, export the results to xls, html, pdf and csv formats for analysis.

Data archiving

To control the database growth, processed event log data older than what is required for immediate audit reporting can be cleared from the ADAudit Plus database and archived, saving on space. Unzip at ease for history reporting, compliance and forensic analysis.

Windows File Server Auditing

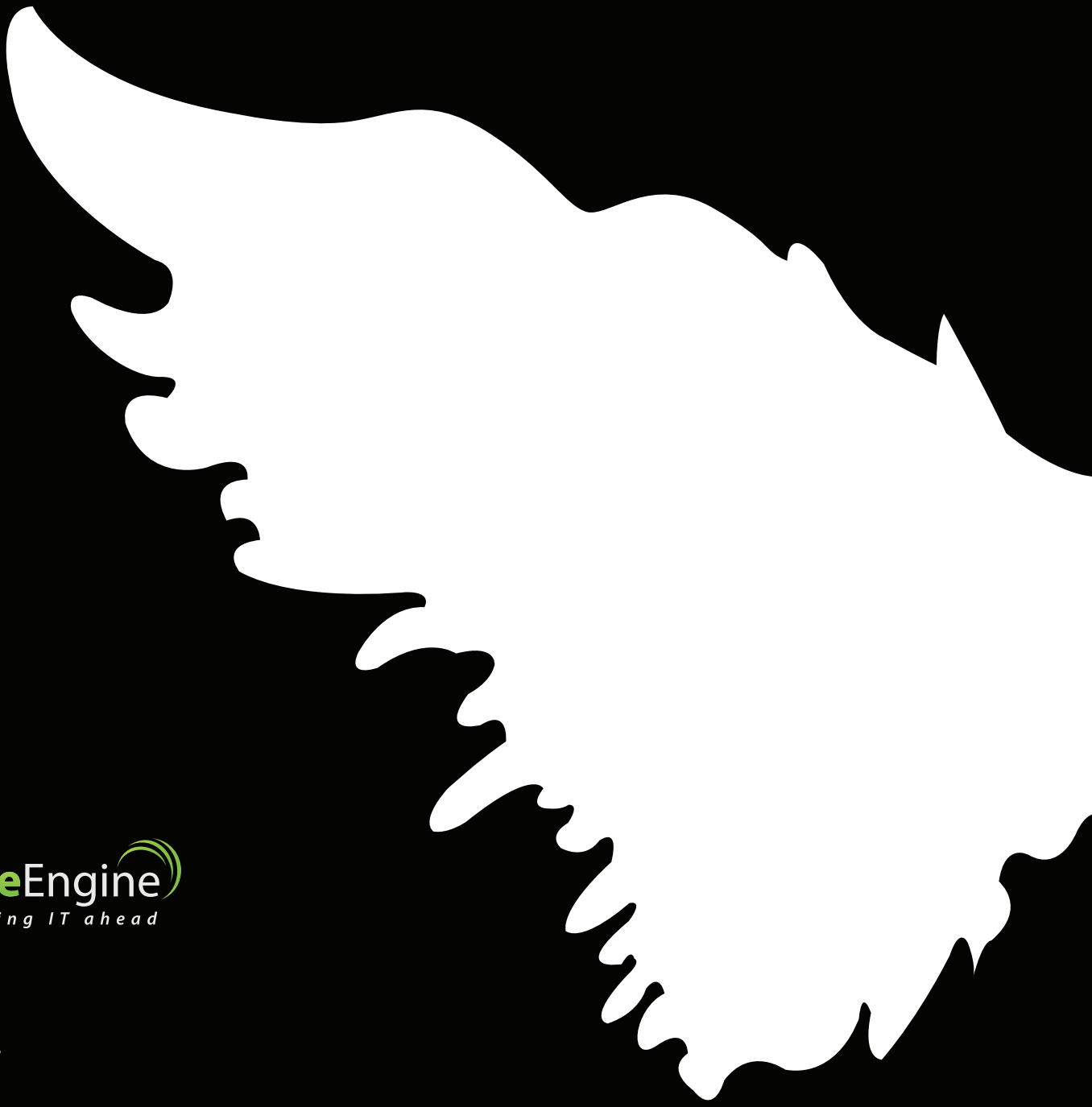
Securely track the File Servers, NetApp Filers and FailOver Clusters for access, changes to the documents in their files and folder structure, shares and permissions. View from the exclusive file audit reports with 50+ search attributes and filter based on user / file server / custom / share based reporting for crisp detailed information.

- Detailed forensics of all changes / failed attempts to file create, delete, modification and folder structure.
- Track file and folder access permissions & owners.
- Audit Windows FailOver Clusters for a secure, downtime-free and a compliant network environment.
- Monitor NetApp Filers CIFS files / folders create, modify and delete, change permissions etc.,

Windows Server Auditing

Member servers are the (file, print, web, application, and communication) workhorses of any Microsoft Server environment. Monitor every Windows Member Server change with various detailed reports: Summary Report, Process Tracking, Policy Changes, System Events, Object Management and Scheduled Tasks.

- Member Server monitoring with a events summary report, track scheduled tasks and system events, track all processes and policy changes.
- File Integrity Monitoring (FIM) of system, configuration, files and file attributes modifications.
- In real-time, identify all the files printed over the Windows network.
- List file details with time and date, user name, pages, copies, file size, printer name and Server details.



ManageEngine
Powering IT ahead

ZMA
IT SOLUTIONS

Lavalle 381 piso 3º | Tel: (54 11) 5219-5555 | C1047AAG
Ciudad Autónoma de Buenos Aires | ARGENTINA
www.zma.la - info@zma.la

+54 9 11 3657 0780
WhatsApp: mensajes/llamadas

Contacto inmediato con nuestro
chat en línea www.zma.la