ManageEngine
ADAudit Plus

14 AD auditing mistakes admins should avoid

Table of Contents

1. Introduction ---- 1
2. Mistakes made in auditing Active Directory ---- 2
    2.1 Overlooking failed login attempts ---- 2
    2.2 Treating all logins the same ---- 4
    2.3 Relying on the default password and account lockout settings ---- 5
    2.4 Failure to implement the principle of least privilege ---- 7
    2.5 Ignoring stale, inactive, and orphaned user accounts ---- 9
    2.6 Lack of automated response to potential IT security threats ---- 10
    2.7 Absence of proactive threat hunting using ML ---- 12
    2.8 Disregarding legacy authentications active on the network ---- 13
    2.9 Too many domain admins ---- 15
    2.10 Excessive levels of AD delegation ---- 16
    2.11 Trusting native auditing to get it done ---- 17
    2.12 Neglecting system log auditing ---- 19
    2.13 Insufficient and incomplete audit trail ---- 20
    2.14 Absence of a real-time auditing solution ---- 21
3. About ADAudit Plus ---- 22
4. Conclusion ---- 23

1. Introduction

The need to audit Active Directory (AD) is not new, but a successful implementation that establishes accountability across network resources is still rare. There are just far too many instances where the limitation in auditing tools and gaps in the audit trail have cost organizations massive losses in data security breaches, non-compliance penalties, diminished reputation, and much more.

To avoid such instances, let us take a look at the fourteen most common mistakes made in auditing your AD environment, so you can ensure it never happens in your organization.

2. Mistakes made in auditing Active Directory

Listed below are the most common mistakes made in auditing an Active Directory environment.

2.1 Overlooking failed login attempts

More often than not, organizations fail to keep track of users who fail to log in to their resources. The common misconception is that since the users have failed to log in to the network, they wouldn't have access to the network resources, and therefore pose no threat to the organization.

It's vital to note that login irregularities and failures are both excellent indicators of compromise. A quick analysis into the failed login patterns can help you:

1. Gauge the effectiveness of password management policies

   A very high count in login failures might be an indication that the password hygiene policies are just too stringent and ambitious. Monitoring failed login attempts helps organizations gauge and refine AD password management policies to prevent needless account lockouts without compromising their network security.

2. Find careless employees who frequently forget their passwords

   Track login attempts to find employees who are negligent in managing their passwords and put your whole organization at risk. Conduct regular security awareness training sessions to educate and caution your users about the consequences of violating the organization's password policies and reset procedures.

3. Detect brute-force attacks instantaneously

Any password guessing attacks such as a brute-force attacks use a trial-and-error method to discover the right combination or key. A sudden spike in failed login attempts from the same IP address is a surefire indicator of a perpetrator trying to access your network's resources maliciously.

How ADAudit Plus helps

- Audits and reports on failed login attempts along with details on who tried to log in, when, and from where.
- Scrutinizes multiple failed login attempts based on factors such as the IP address, login time, and user name.
- Triggers an instant threat response mechanism when multiple failed login attempts are observed within a short period.

2.2 Treating all logins the same

There are multiple ways through which a user logs in to a network. Some of the most common ones are:

Login type	Description
Type 2: Interactive	User logs in from the device console by typing in their credentials in the Windows logon prompt.
Type 3: Network	User logs in to a computer on the network to access a shared resource such as folders.
Type 10: Remote interactive	User logs in to a computer using a remote machine via terminal services.
Type 11: Cached interactive	User logs in to a computer using the network credentials that were stored locally on the computer.

These login types should be used as contextual information while analyzing the logon events to get insights into employee behavior. It could provide critical insights on which of your employees are working from home, who used a service to log in, and more.

Lack of visibility into user login type can lead to an oversight resulting in damaging security breaches and loss in productivity.

How ADAudit Plus helps

- Monitors and reports on all types of user login behavior, including interactive, remote, local, and network logins.
- Find employees working off-site by monitoring all your workforce login data for cached interactive logins.

2.3 Relying on the default password and account lockout settings

Most organizations don't change the default password and account lockout settings provided by Microsoft. However, as there is no such thing as "one size fits all" in IT, these default settings may not suit every organization. The most common security issues that arise out of ill-suited policies are:

- Brute-force attacks
- Insider threats
- Loss of employee productivity

Both the password and account lockout policies should be periodically reworked and evaluated for their effectiveness. Any policy has to consider the following elements:

1. Employee or user count

   Resolving account lockouts takes time and money. Excessively stringent policy settings become highly impractical when there are hundreds or thousands of employees in your organization.

2. Sensitivity of the data stored

   The level of security required is proportional to the nature of business-critical information being stored and processed. Stronger policies and rigorous security practices are put in place when the network resources being accessed have a high net value.

3. Use of account lockout examiners

The use of account lockout analyzers helps to quickly identify and resolve password and account lockout issues raised, especially when dealing with a large workforce.

How ADAudit Plus helps

- Audits every account lockout event, along with critical details on lockout time, machine, and the user's login history.
- Troubleshoots repeated account lockouts by analyzing multiple Windows components, including services, applications, scheduled tasks, RADIUS logons, OWA/ActiveSync, and faulty drive mappings.

2.4 Failure to implement the principle of least privilege

The principle of least privilege (POLP) is a security concept that ensures employees are granted only the bare minimum privileges required to complete their daily tasks. Providing excessive or unneeded levels of access rights and permissions will expand the attack landscape and may serve as an intrusion point for perpetrators.

The top benefits of implementing POLP in your organizations are:

1. Reduces the breach potential of insider threats

   POLP adds an extra layer of security by ensuring that even when a malicious actor gains access to another employee's user account, they will be unable to exploit anything beyond that user's privileges, making it imperative to periodically locate and roll back any excessive permissions given to users.

2. Restricts propagation of malware like ransomware

   Issuing accesses based on users' roles helps limit access points to sensitive data, permissions to system settings, changes to registry configurations, and more, thus reducing the aggressiveness of the malware propagation and giving admins valuable time to contain it.

3. Strengthens data security measures

   Restricting unwanted and over-the-top access levels like "write" and "execute" to critical devices, applications, and servers means that the possible pathways and points of ingress for a security breach are greatly reduced.

4. Helps comply with regulatory mandates

Numerous compliance regulations, including HIPAA, the GDPR, CCPA, and PCI DSS, mandate that organizations practice privacy by design, i.e., access is to be provided to the employees on a need-to-know basis.

How ADAudit Plus helps

- Keeps track of every time a new user is added or removed from a security group.
- Finds and analyzes high-risk changes to AD schema, FSMO roles, and more.
- Maintains a detailed audit trail of whenever a user's permission changes along with both its old and new Access Control List (ACL) values.

2.5 Ignoring stale, inactive, and orphaned user accounts

The presence of unused user accounts in Active Directory is a significant security risk. It leaves the organization's critical resources vulnerable to former employees and perpetrators. It's vital to have a strategy in place to handle employee terminations, including disabling their AD user accounts, removing them from email groups, revoking their access to business applications, and more. To prevent unwarranted accesses and data theft, keep track of stale and unused user accounts in your organization, analyze their need, and then delete them.

How ADAudit Plus helps

- Keeps track of all user account management tasks, including creation, deletion, un-deletion, disable, enable, and much more.

2.6 Lack of automated responses to potential IT security threats

It is impossible to become completely immune to IT security breaches and data thefts. This is why it's prudent for organizations not only to be able to look for indicators of compromise, but have a strategy in place that will instantly attempt to mitigate the security threat. Some of the most common security threats and the automated responses that can help contain them are:

1. Ransomware attacks

   Most ransomware attacks are accompanied by telltale indicators like sudden surges in file rename, move, delete, and permission change activities. Using an instant threat response mechanism to identify and shut down infected devices quickly quarantines the ransomware infection and prevents lateral movement.

2. Insider threats

   To manage insider threats, organizations have to consistently monitor user activities to identify improper, accidental, or even malicious changes made by employees. Using strong remediation techniques, such as USB blocking, disabling rogue users' sessions, and email filtering, help build your organization's defense against both intentional and inadvertent insider threats.

3. Privilege abuse

When the company fails to employ strict access control measures or lacks visibility into employees' login behavior and other activities, it is vulnerable to users' privileges being inappropriately or fraudulently used. Once an indicator of privilege abuse is detected, it is vital to either disable or disconnect that particular user's AD account to mitigate the damage being inflicted.

How ADAudit Plus helps

- Uses scripts to automate responses that include shutting down infected devices, disconnecting rogue users' sessions, and more.
- Triggers scripted threat responses that execute scripts to perform actions tailored to fit the organization's unique requirements.

2.7 Absence of proactive threat hunting using UBA

Protecting your organization's resources from insider threats and data theft attempts requires collecting and analyzing data across thousands of endpoints and servers. It then needs to be cross-referenced with employees' behavior patterns to spot anomalies and vulnerabilities, which is a time-consuming and complex task for even the most robust tool.

On the other hand, if the same tool is incorporated with user behavior analytics (UBA), it can quickly scour through large amounts of data, recognize patterns, and uncover security issues by making machine learning an integral part of threat hunting.

Gartner predicts that by the end of 2024, 75 percent of organizations will shift from piloting to operationalizing AI. The use of machine learning helps establish a baseline of behavior for every employee from which we can predict what's normal and what's not. It maps patterns relevant to file accesses, processes run, user management activities, login behavior, and more.

How ADAudit Plus helps

- Spots anomalous user behavior, including sudden spikes in login failures, unusual login times, a user using remote access for the first time, and more using UBA.
- Finds hidden threats by monitoring sudden deviation in typical user behavior, such as a new process running on a server or an unusual time or volume of account lockouts.
- Updates normal behavior patterns or the baseline every day to increase the accuracy of ADAudit Plus' threat hunting capabilities.

2.8 Disregarding legacy authentications active on the network

The use of legacy authentication in both Azure and on-premises AD leaves the organization vulnerable to ransomware attacks, data theft attempts, and more.

In on-premises AD, legacy authentication refers to the use of insecure protocols such as NTLMv1, SMBv1, and TLS 1.0 and 1.1. Ransomware attacks, including WannaCry and Petya, uses SMBv1 vulnerabilities to proliferate laterally across network devices. Also, NTLM is extremely vulnerable to man-in-the-middle attacks due to lack of mutual authentication and weak cryptography.

On the other hand, in Azure, legacy authentication refers to authentication requests from older software clients like Office 2010 using protocols like SMTP, POP, and IMAP. It's an outdated and obsolete authentication service most commonly used to access email servers.

There are multiple risks inherent with the use of legacy authentication, because it lacks the extra layer of security that protects credentials, i.e., multi-factor authentication (MFA). MFA cannot be enforced by legacy authentication protocols, making them the prime target for perpetrators and hackers.

More than 99 percent of password spray attacks and 97 percent of credential stuffing attacks use legacy authentication protocols.

The first step to blocking both Azure and on-premises legacy protocols is to identify where they are used, by whom, and what they're being used for. Once identified, analyze their necessity and block unwarranted use of these authentication protocols.

How ADAudit Plus helps

- Audits every time NTLM authentication is used to access your resources along with details on who logged in, when, and from where.

2.9 Too many domain admins

Administrative groups and users have significant privileges to perform critical functions in a domain-joined system such as workstations and servers. Such power is perilous when it is shared indiscriminately. Rogue insiders can cause serious damage via compromised credentials when the user account involved is a domain admin.

These elevated privileges should be granted sparingly and after thorough analysis. It is essential to review and manage the domain admin group periodically. Additionally, it's vital to monitor all activities by high privileged users for anomalies.

How ADAudit Plus helps

- Helps you selectively monitor high privileged users and their actions along with details on who did what, when, and where.
- Finds rogue insiders and compromised user accounts by looking for sudden deviations in typical user behavior using machine learning.

2.10 Excessive levels of AD delegation

Delegation is provisioned in Active Directory to make domain admins' work easier by providing necessary privileges to non-admin users to carry out predefined tasks without adding them to high-privileged groups.

Immoderate levels of AD delegations cause significant issues like losing track of the tasks delegated, lack of visibility into the changes made, and more. It's important to analyze and ensure that the tasks delegated get processed in a transparent and secure manner.

How ADAudit Plus helps

- Audits every time users and groups are granted permissions at various levels, including domain, OU, GPO, container, and more.

2.11 Trusting native auditing to get it done

Auditing an AD environment is mandatory both from a security and a compliance standpoint. Most times, organizations prefer to use native auditing, i.e., the inherent provision offered by Microsoft to track down specific events using the event viewer. However, any skilled admin knows that relying solely on native auditing to meet security and visibility requirements is going to be a laborious and tedious task. The most common risks that arise are:

1. Provides only partial information

   More often than not, native auditing does not provide the whole picture. It's important to analyze every event with the quintessential four details, i.e., who did what, when, and from where to get a complete picture. In native auditing, the details of who initiated the change or the old and new values after a modification are usually cryptic and take an enormous amount of time and effort to understand.

2. Powerless to meet regulatory mandates

   Numerous compliance regulations, including the GDPR, HIPAA, SOX, CCPA, and PCI DSS, mandate the implementation of access control and IT security measures to protect the integrity, confidentiality, and availability of your business-critical data.

   But native auditing does not provide out-of-the-box audit reports, and the task of exporting necessary data from the event log is almost insurmountable.

3. Generates excessive noise and useless data

When admins try to use native auditing to monitor all AD changes using the event log, they end up with monstrous levels of noise in their security event log. It becomes almost impossible to find an anomaly or even to get a collation of what is being changed.

How ADAudit Plus helps

- Provides over 250 compliance-ready reports to help meet multiple compliance regulations, including the GDPR, SOX, HIPAA, GLBA, FISMA, ISO 27001, and PCI DSS.
- Overcomes the limitations of AD native auditing with real-time auditing capabilities. ADAudit Plus is an easy-to-use, central platform that provides overall visibility into all the changes taking place across various Windows components with in-depth detail.

2.12 Neglecting system log auditing

All audit data by default is stored as event logs in Windows environments. Rogue employees often try to cover their steps by deleting the audit data that indicates their inappropriate and immoral activities, making it necessary to audit the event log every time an employee tries to archive, overwrite, or tamper with the existing audit data.

How ADAudit Plus helps

- Audits and triggers instant notifications every time the security log containing audit data is cleared or is full and unable to log new data.

2.13 Insufficient and incomplete audit log storage

The security event log can store audit data only up to a predefined limit. When the audit data surpasses this limit, old logs get automatically deleted or overwritten by the new ones. This is a massive drawback, especially when organizations are mandated by regulatory bodies to keep the record of foolproof audit trails for years.

How ADAudit Plus helps

- Maintains a consolidated user-based audit trail as legal evidence and for analysis.
- Auto-archives and stores the older security logs to comply with regulations that mandate storing audit data for years together.

2.14 Absence of a real-time auditing solution

Any knowledgeable administrator knows that it's pointless to use a third-party auditing tool if it's not going to work in real time. Auditing your AD in real time helps monitor changes periodically with minimal effort and time spent.

The top benefits of establishing a real-time auditing tool are that it helps:

1. Scrutinize deviations and anomalies with brevity

   It's important to detect unusual activities and vulnerabilities immediately to help remediate the issue before it snowballs into a huge security breach. A sudden spike in high-risk user activities, strange login behavior, and critical changes made during non-business hours are just a few examples where real-time auditing and notification functions would come in handy.

2. Notify stakeholders on critical changes

   Triggering instant notifications on high-risk user activities like changes to AD schema, GPO settings, permissions, FSMO roles, and more is possible only when the tool is able to identify the changes as soon as they occur.

3. Maintain employee productivity

   Critical high privileged user's getting locked out can result in crippling downtime to the organization. The time taken to trace, diagnose, and resolve issues like account lockout is much less when the issue is detected immediately.

How ADAudit Plus helps

- Provides real-time visibility into changes made across Active Directory; Azure AD; Windows file servers; EMC, NetApp, and Synology storage devices; Windows servers; and workstations.

3. About ADAudit Plus

ManageEngine's AD auditing solution, ADAudit Plus is a UBA-driven change auditing tool that helps keep your AD and IT infrastructure secure and compliant.

ManageEngine ADAudit Plus can:

- Audit and report all changes made across your AD and Azure AD environment.
- Monitor and analyze employees' login activities for anomalies.
- Track and resolve repeated account lockouts.
- Provide visibility into all file accesses and modifications in real time.
- Audit GPO setting changes along with their old and new values.
- Proactively identifies potential threats early on using UBA.
- Monitor employee productivity and attendance.
- Maintain a detailed record of all privileged user activities.
- Provide over 250 out-of-the-box reports to help comply with the GDPR, SOX, PCI DSS, and more.

What's next?

Sign up for a guided demo

Get a one-on-one product walk-through with one of our technical experts to learn more about how ADAudit Plus can benefit your enterprise.

Request a personal quote

Obtain an annual pricing quote tailored to best suit your organization's needs.

Download slide deck

Get our free slide deck to learn more about ADAudit Plus, including its full list of features.

Start your free trial

4. Conclusion

Auditing AD is complex, but with the use of the right tools, it can be much easier. Proper implementation of auditing across your Windows environment will help maintain compliance with industry standards, detect and respond to security threats, and in short, strengthen your IT security infrastructure.

Perfect your AD auditing by identifying and correcting the most common mistakes made.