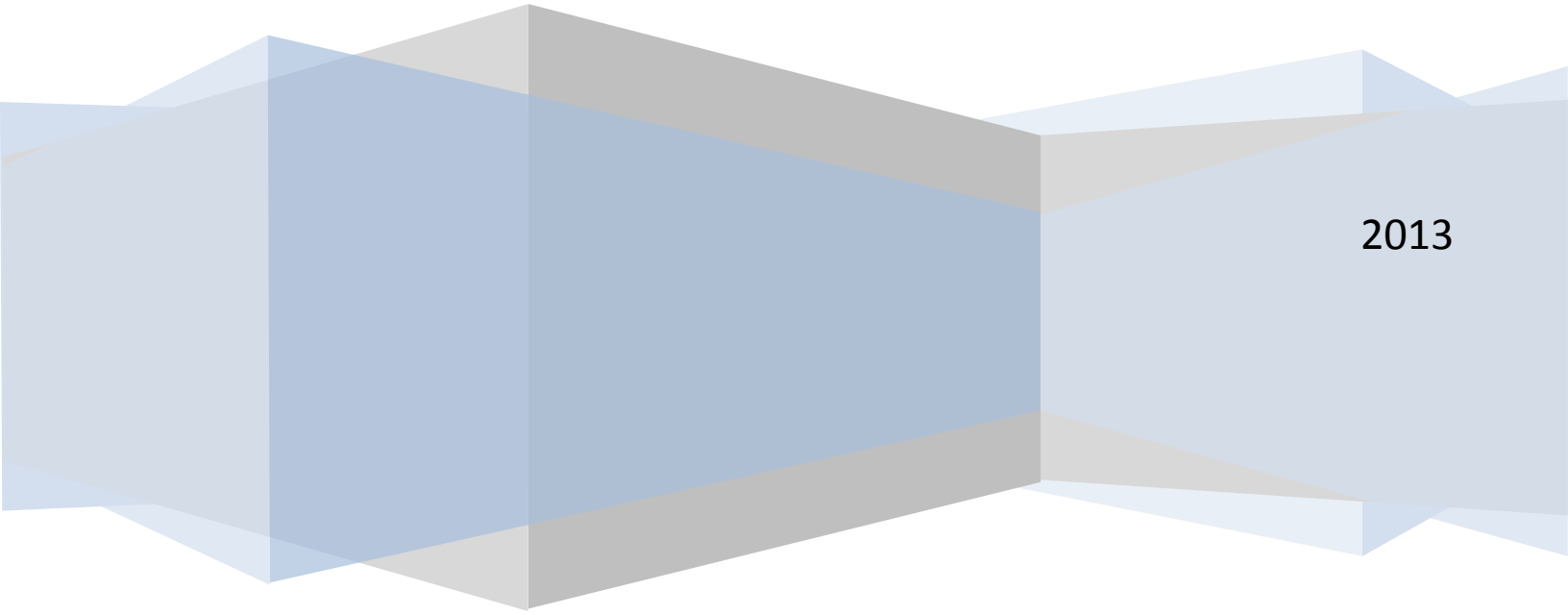
www.lepide.com

Active Directory Auditing – The Need and Result

Whitepaper



2013

What are IT Audits?

Increasing number of cases of malpractices and lackadaisical approach towards handling sensitive data by a handful of organizations are leading government agencies to tighten the noose on entire corporate community. While Corporate feel a bit uncomfortable with stringent regulatory policies, as they have to adjust existing processes and put in additional resources to satisfy regulatory standards, they also understand the importance of such regulations in the backdrop of customer data theft and corporate scandals, and are ready to go out of their way to keep the interest of their most important stakeholders – customers.

IT audits are a way to ensure that organizations are following the industry specific and other regulations put forward by concerned authorities. Organizations first need to implement the regulations, if they not already are, and then periodically verify it by answering questions and providing proof to auditors – designated persons to conduct the audit. Inability to provide correct answers and proof of compliance to auditors may draw heavy financial penalty as an immediate effect and loss of reputation which could be more damaging in the long run.

How does IT Audits help organizations?

IT Audits go a long way in securing significant gains for organizations. Corporate would benefit by not considering IT auditing just as a means to satisfy external regulations that are binding to all entities operating in the concerned environment. Instead, it should be taken as an opportunity to adhere to practices that satisfy interest of all stakeholders in the environment and also help in establishing secure and robust foundations in terms of improved and refined processes that ensures business continuity and long-term benefits. Satisfying IT audits help organizations to:

- Create a risk-free and secure IT environment that ensures business continuity by eliminating potential harmful changes that could lead to downtimes and outages.
- Avoid loss of reputation in the face of failed Compliances.
- Save heavy financial penalties that need to be paid in case of failed compliances.
- Provisions to satisfy audits also help you to perform forensic analysis in case of such requirements.

What is Active Directory change audit and what is the need to audit AD changes?

Active Directory change auditing is the process of tracking and logging all changes made to the Active Directory with following information for each change: Who made the change, What change was made to which Object, When was the change made and from Where the change was made.

As an administrator you must be aware of all changes being done to Active Directory to be able to scrutinize them and ensure that only beneficial changes exist in the system. In real-world scenario even a single undesirable change made to Active Directory can bring the IT operations to a standstill. The following are some of the specific scenarios that underline the need of Active Directory auditing:

- Recent User attempts to change password, for instance, is the information that you would definitely like to have, particularly for administrator-assigned passwords.
- An important task is being run on a computer and it should better remain untouched by unauthorized persons. You need complete history of all logon attempts made to that computer.
- Unauthorized access and modifications to a particular task might hamper the task or even worse, your IT infrastructure. There is a requirement of instant alert, so that whenever anyone accesses that particular task, the admin will be immediately notified and he can stop that particular user from doing any damage.
- Five Users were disabled yesterday; now it is important to investigate why were they created and what led to them being disabled. Do you need to change your User creation policies or is there something that could be done to improve the process.
- An administrative user got deleted, Organizational Unit created at the time of system setup was moved to another location; these are the kind of changes that can create serious trouble for administrators if they are unauthorized.
- Any changes made to the three policy areas i.e. User Rights assignment, Audit policies and Trust relationships need to be tracked and logged as best practices for Active Directory auditing.
- Tracing all historical changes to an object may become important as part of the forensic analysis; Single Object change history may bring to you all the changes that have been done to the particular object.

How will Active Directory Audit help an organization?

Active Directory auditing helps organizations keep a close eye on all changes done to AD. A security lapse could lead to undesirable changes being made to important Active Directory objects and policies. Identifying these changes at the earliest is necessary to take required actions to revert the changes. Comprehensive Active Directory auditing can help organization in a number of ways:

- Reports giving detailed information on each change of Active Directory both in real time and for a particular duration of time allows you to take corrective measures before such changes further deteriorate the Active Directory environment.

- As soon as a User right is assigned to a critical resource in the network like domain controller, instant alert to the administrator ensures that such access rights are genuine and in tune with organizational policy.
- Information about changes in Audit Policy of an Object and Domain policy changes ensures that no Object is left unaudited thus preventing loopholes in audit policies.
- Alerts on attempts to un-register security events source also helps in ensuring tight security of Active Directory objects.
- Successful Active Directory audit also means avoiding heavy financial penalties and loss of reputation due to failed compliance.

What are the most important features/requirements for Active Directory Audit?

Audit and Compliance requirements for organizations dealing with sensitive customer data are becoming stringent day by day. Today, it is no more just about keeping the records of changes happening in your enterprise; regulatory standards are expecting you to take more proactive approach to safeguard the interest of all stakeholders. To support present age regulatory requirements -

- There is a need to collect and store Who, What, When and Where information for each change dating back to the period suggested by Compliance standards. These 4 Ws have become the backbone of audit policy requirements that provide even minutest details about each Active Directory change to answer all audit questions.
- It takes a system that can dwell deeper into the core of Active Directory and collect all sorts of change logs and present it in a user friendly format with extensive search and filter options to present the desired data at the earliest.
- Another requirement is that of an alert system to identify changes as they occur with minimal detection time. The longer an undesirable change exists in the system the greater is the damage potential of that change. Alert system can send instant intimations to intended recipients as soon as the change occurs.
- Administrators also need provision to rollback unwanted changes at the earliest, as just getting an alert about an unwanted change without any means to undo it does not help much in ensuring secure and risk free Active Directory environment from audit perspective.

Active Directory and Compliance.

Active Directory plays a very critical role in meeting various Compliance standards. It allows you to manage network identities and access permissions, carry out all user login authentications, allocate resources and perform centralized logging of all access attempts in the network. These provisions give a significant grip on entire network objects and make it possible to implement

strict regulatory policies and standards through this hub. Active Directory auditing and Compliance are closely related in following ways:

- Getting a complete report on security settings of network objects, like who can access, modify, add and delete it and whether the client can be granted the desired access to it or not lets you control access to sensitive financial data as per SOX and PCI guidelines.
- Comprehensive reporting of Active Directory can help you identify potential risks and mitigate those risks using proper measures – another important compliance requirement.
- Reports on disabled Users and Computers can help you to eliminate the possibility of such entities being used to gain unauthorized access by cleaning such objects from Active Directory.
- Failed User logon attempts and Failed Network logon attempts can provide vital clues while investigating unauthorized access by hackers.
- Tracking day-to-day changes done in Active Directory is important from both organizations' internal and external policy compliance perspective.
- Generating a list of recently created, modified and deleted objects like Users, Computers, Groups and OUs gives you complete insight into all the changes happening in the organization.
- Taking regular snapshots of Active Directory environment that stores all structural details can be extremely useful in meeting disaster recovery guidelines of various Compliance standards.

Compliance Standards and their requirements

- The Sarbanes-Oxley Act or **SOX** deals with the issues of financial accounting indecencies in the corporate world. It intends to bring proper control, transparencies and accuracy in the financial disclosure of the firms. IT system plays a very important role in access control management determining who accesses what and when, and thus can ensure fulfillment of these requirements. SOX regulations require keeping of audit reports for a period not less than 7 years.
- Health Insurance Portability and Accountability Act (**HIPAA**) ensures that healthcare providers keep the patients information safe and secure. Any unwanted change to Active Directory may affect data access negatively resulting in the severe financial penalties to the organization. Reports on all user activities pertaining to access control and related areas for a period of at least 6 years are mandatory to support HIPAA compliance. HIPAA regulations require holding records of all activities for a minimum of 6 years.
- Organizations dealing with financial data may need to adhere to Gramm-Leach-Bliley Act **(GLBA)** compliance. Satisfying GLBA regulations require you to monitor and review on continuous basis who accessed what and when particularly for sensitive resources such

as files, programs and processes pertaining to customer financial data. Monitoring network activity of all domains to identify security breach and log events to analyze and generate reports is another important requirement.

- **PCI** compliance requires you to monitor all security related changes to Active Directory and folders and their permissions. Not only tracking but you also need to have full control on creation, modification and deletion of user accounts. All user logon activities need to be recorded to identify who is accessing what and when. Complete auditing of Admin activities to track changes to access-rights for network resources, and a host of other reports on changes with ability to roll them back are needed to satisfy PCI compliance. PCI regulations require retaining of the audit trail history for at least one year.

What if an organization fails in an IT Audit?

Penalties of non-compliance vary from act to act and also depend on the section(s) that have been violated.

- Penalties for PCI compliance violations could range from $5,000 to $100,000 per month.
- Non-compliance to SOX means you can be fined anything between $1 million to $5 million along with up to 20 years of imprisonment and exchange delisting for publicly traded companies.
- Penalties under HIPAA for compliance failure are not any less severe; wrongful disclosure of individually identifiable health information could lead to fine of $50,000 to $250,000 and imprisonment between 1 year to 10 years, or both.
- Loss of reputation that could shake investors' confidence and also drive customers to competitors; and this could uproot even big and cash-rich companies in the long run.

Given the advantages of IT audits and severe penalties of non-compliance, it doesn't take much to understand that following regulations to satisfy audits and compliance is the way to go for all small and big organizations.

What would the organization gain with Active Directory Audit?

Active Directory auditing is no longer an option but a necessity for most of the organizations. Even for companies which do not fall under the ambit of government regulations, Active Directory auditing will be beneficial for a number of reasons such as reduced security threat, meeting internal regulatory policies and ensuring high availability of IT resources. Some of the prominent benefits of Active Directory Auditing are:

Tracking Active Directory changes: Track all Active Directory changes to get Who, What, When and Where information about all changes. Monitor administrative and privilege user actions

responsible for critical changes. Perform real time tracking by setting alerts on important changes; get email alerts as soon as such changes occur to minimize detection time and thus potential damaged caused by such changes.

Get full control over Active Directory: Tracking Active Directory changes means you get full control over Active Directory environment. Knowing old and new value for each change means you can restore Active Directory changes whenever necessary.

Stay Complaint with law: For organizations dealing with sensitive financial and healthcare data, Active Directory auditing is a must and they should be ready to provide answers to all auditing questions to avoid penalties and loss of reputation. You should have provisions in place to satisfy regulatory requirements as per law.

Eliminate risks and threats and ensure high uptime: Organizations performing thorough Active Directory auditing can minimize downtimes by preventing undesirable changes from occurring and rollback such changes even if they occur with just a few clicks.

LepideAuditor for Active Directory – an apt tool for Active Directory auditing

LepideAuditor for Active Directory (LAAD) is specialized software to perform Active Directory auditing and offers some coveted features that you won't get with native Active Directory auditing. Active Directory change logs may remain scattered across domains making it difficult and time consuming to collect such logs and get useful information out of it. Maintaining Compliance means you need to archive change logs for all the domains in the network for a number of years which could be quite resource consuming. Furthermore, native Active Directory auditing lacks Reporting and Alerting feature as well.

LAAD consolidates change logs from all the domains in the network at one centralized location from where it is easy to archive and manage. It offers a number of out-of-the-box reports that cover all aspects of Active Directory and can answer all your Compliance questions as well. Functions of LAAD can be categorized under two heads:

Active Directory Change Tracking: Track all changes made to Objects, Users, OUs, Computers, Groups, and Network Policy. Schedule reports to get information on all changes periodically right in your Inbox. Get real time alerts to identify critical changes as they occur to minimize detection time.

Active Directory Change Control: Rollback unwanted changes to restore Active Directory to a previous stable state. Take regular snapshots of Active Directory and compare with current state to identify changes with old and new value.

LAAD offers an easy way to audit Active Directory changes comprehensively. It provides valuable benefits such as eliminating risk factors, upholding compliance, protecting Active Directory against unwanted changes and saving time and resources that are consumed in native auditing. Let's consider some of the scenarios and understand how LAAD could be immensely useful:

Scenario 1: Who changed what, when and from where?

Problem: Active Directory logs may remain scattered across domains; moreover, logs are cryptic in nature and there could be multiple entries for the same event making it difficult and time consuming to get this information.

Solution: LAAD consolidates logs from various domains in one centralized repository. Information related to a particular event is presented at one place as a single record and Who, What, When and Where information is presented in separate columns for easy comprehensibility.

Scenario 2: Maintaining Compliance.

Problem: Major requirement for staying complaint with various acts and regulations is the ability to archive data for a long period of time and then access and present that data in required format at the time of auditing to demonstrate compliance. SOX and HIPAA compliance, for instance, require you to archive audit data for a period of seven and six years respectively for compliance purpose. Storing such a bulk of data without using specialized software is not only inefficient from storage perspective but it is also difficult to access required piece of information from such a bulk of data to answer audit questions. Data security is another concern as such a pile of data is vulnerable to manipulation and deletion.

Solution: LAAD creates a central repository of audit data in SQL server database that is out of reach for unauthorized users. Moreover, efficient storage and ability to filter and store only required data means you can archive audit data for as long as you want and access and present it in required format as and when required to support compliance.

Scenario 3: Handle cases of accidental deletion.

Problem: Accidental deletion of Active Directory objects is not easy to handle using native services. You first need to assemble pieces of information scattered in the log files to establish what was deleted and what were the values of various attributes associated with it. Even after complete information has been gathered, restoring deleted objects manually in itself might take a lot of time and effort.

Solution: Lepide Auditor for Active Directory shows deleted objects in red with who, what, when and where information for each deleted object. Administrators can restore deleted objects with a single click. Result of undoing a change is also displayed in simple English for the users' knowledge. Setting up alert for cases of deletion will instantly inform Admins about such changes; reactive measures could then be taken to restore deleted objects.

Scenario 4: Active Directory backup and restore

Problem: It is advisable to take regular backup of Active Directory to restore entire AD in case of disasters or restore selected items to rollback undesirable changes. To increase the effectiveness of the backup process, it is important to take backup as frequently as possible. That, in effect, requires huge storage space to store backup data. Then, restoring changes from backup is another problem area that needs to be tackled effectively.

Solution: LAAD allows you to create regular backup and store it with efficient use of storage. You can select any of the snapshots/backup and use it to restore Active Directory to a previous stable state or rollback selective changes as per requirement.

……

About Lepide

Lepide Software offers cutting-edge products that help customer to excel in their businesses. It has a wide portfolio of products serving clients across verticals that have benefited largely from them. The company puts in years of experience and innovation that is has developed from designing wide range of products developed by skilled workforce. It aims to be recognized as the best provider of business enhancement software tool.

For more information visit:
http://www.lepide.com/active-directory-audit/
To try LepideAuditor for Active Directory, visit:
http://www.lepide.com/active-directory-audit/download.html