

White Paper

Why It Is Important to Audit Your Active Directory ?



Published: February 2006

Authors: Dominic Bland & Marc Barnard



The Active Directory Maturity Model

The Active Directory Maturity Model is an audit process that examines the "current state" of the Active Directory. It delivers an accurate and quantitative report on the security and functional capability of any Microsoft Active Directory Implementation.

For more information on this subject and a White Paper entitled 'Why Is It Important to Audit the Active Directory' please visit our website at:

www.GenesisRKeyTec.com

please feel free to **Contact Us** if you require more information.

At the core of all Windows networks lies the Active Directory. Correctly used, it provides vital security and ROI for Windows systems. A clear insight into the design maturity and current state of the Active Directory is essential to an organisations awareness of its infrastructure security

Background on the Active Directory

The core of the Windows server infrastructure is a component called the Active Directory (AD). The Active Directory is designed by Microsoft to be configured by IT professionals and so provide a secure environment for managing users, services and resources. The Windows Active Directory provides organisations with tremendous scope to improve Windows security and IT management and it also provides many features to enhance the user experience. A well designed and implemented Active Directory is the foundation of any optimised Windows infrastructure which enhances the operational capabilities of the environment and reduces total cost of ownership (TCO).

Active Directory: Critical to Internal Security

Over the years, as more and more threats have presented themselves, system security has risen up the agenda to the point where it is now a primary consideration when building a network.

Boundary security in the form of Firewalls are subjected to a vast amount of scrutiny – audits of their configuration, penetration attacks - which is good, but perimeter firewalls do nothing to mitigate internal threats.

If some malevolent code does manage to enter the network it is essential that it is never executed with high level privileges, thus minimizing any damage that may be caused. A correctly designed, configured and implemented Active Directory will significantly reduce this risk. More and more companies are realising that a properly secure Active Directory is a critical component of a fully secured Windows network.

Any organisation that follows the Best Practice of penetration testing their firewalls every 6 months to maintain their boarder security, should also be auditing the internal structures of the Active Directory because they are the foundation of the organisations internal security.

A note on the different types of audit

Active Directory is a 'stateful' system, it maintains a minimum of historical information regarding any changes or updates to its structure or to its objects. The primary concern of an Active Directory is the current state in which it finds itself – hence, 'stateful'. The only historical information that is kept for any object or attribute, concerns the last update applied to it. A log is kept of the GUID of the Domain Controller that initiated the change, and also a transaction number for the update. This is not a conscious attempt at recording historical information, but an aspect of the replication process.

There are two types of Active Directory audits available to a system administrator.

- Historical audit – i.e. the changes that have taken place to an Active Directory.
- Stateful audit – i.e. validating the current state of the implemented design; an investigation of the current structure and efficiency of an Active Directory.

There are various tools in the marketplace that perform historical audits. These tools provide a complete history of the system. This is usually achieved by Event Triggers logging information into a separate system, often an SQL database, every time an Active Directory is updated. This form of audit is very useful for tracking deviant behaviour within a structure and offers then bonus of rolling back a structure if corruption, or a security compromise, has occurred.

Stateful audits are used to gain an understanding of the current state of the Active Directory, and their output is not 'who did what, and when?', but rather 'who can do what, now?', or 'what floors exist right now?' This type of audit will only look at the current functional state of the Active Directory – any history is irrelevant. Some of the major considerations are:

- The current state of system security
- The current state of infrastructure control
- The current state of Disaster Recovery readiness

This white paper is primarily concerned with stateful audits

... continued

The next step: Request a web-based demonstration or personal appointment by using the contact information, opposite. Reference sites available upon request.

Contact Details:

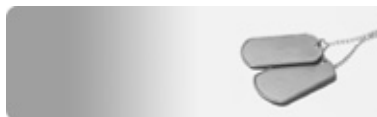
Telephone:
+44 20 7870 1618

Email:
Info@GenesisRKeyTec.com

Fax:
+44 8700 528 179

Web:
www.GenesisRKeyTec.com

White Paper Reasons To Audit Active Directory Continued . . .



Reasons to Conduct a 'Stateful' Active Directory Audit

There are many reasons why an organisation may wish to commission an independent audit of their Active Directory. The most common are as follows:

- The Active Directory implementation is NOT meeting expectations
- An Internal security breach has occurred
- Design ratification is called for before implementation
- Standard security audit
- Due diligence or compliance assessment
- Support staff validating their internal implementation
- New administrator wants independent assessment of the Active Directory
- Security ratification
- Ensuring that the architecture has integrity after an Active Directory upgrade
- Part of regular maintenance / checks and balances

The Active Directory implementation is NOT meeting expectations

This situation may manifest itself in many ways:

- Too many support calls
- Too many instances of accidental damage to the system
- Policies not being constantly applied

The Active Directory may not be meeting basic operational requirements, e.g. Server, workstation. and User validation – this tends to happen automatically – but there might be questions as to how effectively this is happening. Domain Controller placement might be wrong causing logons to be slow.

User profiles & home directories might be inconsistent causing data to be stored in the wrong locations and so be missed by the backup processes.

Correctly implemented, the Active Directory controls the environment, providing security and to lower the cost of ownership of systems, so one of the most fundamental questions to ask about an Active Directory implementation is 'did the cost of ownership of our desktops drop by 20–30%?' If it didn't then an investigation is required to find out why!

An Internal security breach has occurred

Internal security can be breached in any number of ways, but the main avenue of attack is usually privilege elevation or someone abusing the privileges that they have – quite often privileges they shouldn't have in the first place. One of the main purposes of hierarchical authority is to prevent people from having privileges above those required to carry out their duties. The implementation of true hierarchical, role based authority will minimise the scope of malicious attacks. It is important to note that even if damage is caused by accident rather than malice, it is still a breach in the security of the system.

Design ratification is called for before implementation

This would not be an audit on an existing Active Directory, but on a proposed implementation of an Active Directory design – this would have to be more of a theoretical audit because it would not be possible to resolve all questions pertaining to an audit. It would be possible to see the Organisational Architecture and the application of Access Controls and Group Policies to that architecture. It wouldn't, for example, be possible to see any empty OUs or see how many Domain Admins were present. But it is possible to get a very clear idea of how effective the design would be in a production environment.

Standard security audit

An audit such as this can be regarded as a theoretical penetration test – mainly looking for opportunities for privilege elevation. It would often concentrate on the hierarchical authority structure, which is produced (mostly) the access controls & the Organisation Units. Adherence to corporate baselines would be assessed. A physical penetration test could also be mounted to assess how well the support staff are adhering to the best practices and design rules for using the structure.

Due diligence or compliance assessment

Due diligence directives usually come from Director or Chief Executive level of corporate responsibility. If a company does not take the correct security or Disaster Recovery measures then the directors can be deemed to have failed in their obligations and duties towards their shareholders, employees and customers. This can expose them to personal liability. Compliance assessment with Sox or Basel regulations can be a major driver within financial institutions, calling on them to manage their business risks, both technical and operational. Inappropriate internal security controls can lead to audit failures and have serious financial consequences.

Support staff validating their internal implementation

This is link a design audit, but post implementation, rather than pre-implementation. These are often commissioned on the grounds of pure "assurance" for the implementation or to gain new ideas to improve upon the work already carried out.

. . . . continued

The next step: Request a web-based demonstration or personal appointment by using the contact information, opposite. Reference sites available upon request.

Contact Details:

Telephone:
+44 20 7870 1618

Email:
Info@GenesisRKeyTec.com

Fax:
+44 8700 528 179

Web:
www.GenesisRKeyTec.com

Customer Feedback

"Security is a key consideration of the way we use our computer technology. With the help of RKeyTec Genesis we have implemented a flexible and easily manageable security solution to the foundation of our whole computing infrastructure; our Active Directory."

Sam Green
Technical Architect
The Met Office

White Paper Reasons To Audit Active Directory

Continued ...



New administrator wants independent assessment of the Active Directory

An administrator who is new to a role may have documentation, but may also want independent confirmation that the system is stable & secure. For example, the new administrator may notice that there are too many support staff with "Domain Admins" privilege (an extremely powerful authority), which always raises security concerns.

Security ratification – an important distinction

The normal security ratification processes for industries, such as the defence industry, do not cover an Active Directory. Normally when an auditor is commissioned to perform a security audit, at an organisation, they generally tend to look at only a few areas of the Active Directory – their primary interest is usually areas such as User Password controls – e.g. do passwords have to be reset every 30 days? Quite often auditors knowledge is detailed enough to go and check to see if similar policies have been applied to the Workstation Account databases and not just Domain Account databases. They may not be experienced enough to check hierarchical authorities – passwords can have maximum security, but this is meaningless if everyone has been made a member of the Domain Admin group. An Active Directory should be subject to a penetration test and also be included in any kind of security audit of the system.

This is an area of great concern: The Active Directory is a critical security component of all Windows infrastructures, but there is a significant lack of understanding of how it works and how to secure it appropriately.

Ensuring that the architecture has integrity after an Active Directory upgrade

Active Directory is a product that is undergoing constant evolution: New features are being added with each release. Active Directory is always backwardly compatible – i.e. an Active Directory architecture built in a Windows 2000 environment will be valid when upgraded to a Windows 2003 environment. However, it may be that an Active Directory that has been upgraded will not be taking advantage of any new controls, components or capabilities that have been added by the upgrade.

A prime example of this new functionality (when upgrading from Active Directory 2000 to 2003) can be seen in the management of Domain Controllers. Active Directory 2000 contains a management group called Server Operators. It was intended that people who performed the physical maintenance on the servers should be placed in this group. Unfortunately Server Operators did not possess sufficient privileges to fully perform this task (e.g. inability to stop & start Services, reset network connections) so, under Active Directory 2000, members of Server Operators also had to be placed in the Administrators group to allow them a truly useful authority. Unfortunately the Administrators group is placed on various access controls in the Active Directory database, allowing its members to elevate their privileges to those of Domain Admins, then onto Enterprise Admins.

"Active Directory 2003" has addressed this issue by adding extra groups into the database like "Network Configuration Operators". Now an administrator can be made a member of "Server Operators" AND the new "Network Configuration Operators" and be granted sufficient privileges usefully carry out their duties without compromising overall system security.

Part of Regular Maintenance / checks and balances

The internal structures of an Active Directory are changing continually, therefore it is a very worthwhile exercise to perform regular audits to constantly analyse and verify the integrity of the Active Directory. Firewalls (see above) are subjected to regular penetration attacks and tests to verify their integrity, so it is important to subject the Active Directory to equivalent tests. Because the Active Directory is such a critical security structure, the maintenance of the AD security and architecture should be treated in the same way as the maintenance of a Firewall because it serves the same purpose – it is critical to the security of the system.

In Conclusion

Whatever the reason that calls for an Audit of the Active Directory, the process is the same. The reason for the audit makes different aspect of the final report more relevant to current thinking and decision making, but all components of the internal Active Directory architecture interact with each other to create a consistent and secure system and so all must be examined. The Active Directory Maturity Model (ADMM) provides the framework and process for this.

If you found this article helpful or if you feel that you may benefit from an ADMM audit, please feel free to contact us using the details provided, below.

The next step: Request a web-based demonstration or personal appointment by using the contact information, opposite. Reference sites available upon request.

Contact Details:

Telephone:
+44 20 7870 1618

Email:
Info@GenesisRKeyTec.com

Fax:
+44 8700 528 179

Web:
www.GenesisRKeyTec.com

Customer Feedback

"We were in a bit of bother with fast approaching deadlines. The Active Directory for our target migration system was not progressing quickly enough. Genesis RKeyTec Consultants came in and hit the ground running by using Genesis to build our Active Directory very quickly. As a result our deadlines were not impacted."

Michael Hutton-Squire
Head of IT Infrastructure
Financial Dynamics

What Is Genesis ?

GENESIS is an expert system that allows any organisation to rapidly, and cost effectively implement a highly secure and functional "Pre-fabricated" Active Directory architecture into a new or existing Active Directory.

