



Active Directory Maturity Model

For “The Client” Ltd

Produced by “The consultant”

Date “The Date”

LEGAL NOTICES

Copyright

Copyright © Genesis RKeyTec Ltd., 2004–2007. All rights reserved.

Distribution of substantively modified versions of this document is prohibited without the explicit permission of the copyright holder.

Distribution of this work or derivative work in any standard (paper) book form for commercial purposes is prohibited unless prior permission is obtained from the copyright holder.

Disclaimer

THIS REPORT IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS REPORT, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Trademarks

Microsoft, Active Directory and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Feedback

If you have any comments or feedback concerning the contents of this document please use the 'Contact Us' facility on the Genesis RKeyTec Ltd web site:

www.genesisrkeytec.com/contactus

1. Contents

1.	Contents	2
2.	Introduction	3
2.1.1.	Understanding this report	3
2.2.	Overall Scores	4
2.2.1.	Overall Physical Stability	4
2.2.2.	Overall Logical Implementation	4
2.3.	Logical Breakdowns	5
2.3.1.	Security	5
2.3.2.	Manageability	5
2.3.3.	Stability	5
2.3.4.	Compliance	5
3.	Suggested Actions	6
4.	Further Reading	6
Appendix A:	Understanding Security and ROI for the Active Directory	7
Appendix B:	A Note on the Different Types of Audit	7

2. Introduction

This summary report outlines the current state of the Active Directory implementation at “The Client” Ltd as assessed by “The Consultant” of Genesis RKeyTec Ltd on “The Date”.

The information was gathered by direct review of the productions systems. Questions arising from our observations were handled by Stuart Stace.

2.1.1. Understanding this report

The Active Directory Maturity Model (ADMM) is an assessment of how the current state of the Active Directory implementation is meeting the requirements of the business. Active Directory is the foundation of internal security and authority in any Windows infrastructure and, as such, must be handled with the same level of care and attention as the internet facing firewall.

The ADMM begins with an assessment of the physical stability of the directory and is designed to highlight any major issues with the physical implementation. This is followed by a detailed assessment of the logical architecture that gives rise to most of the Active Directory’s security and Cost of Ownership benefits.

In each stage the use of the relevant Active Directory objects and structures is assessed on a scale of 1-5 against clearly defined criteria. These values are statistically analysed to produce the 6 metrics which are the quantitative result of the audit:

Overall Physical Stability	This determines if the placements of directory servers, their replication and availability to clients and suitability of meeting the needs of the organisation’s Windows infrastructure.
Overall Logical Implementation	This is the main focus of the audit, highlighting the overall “fitness for business purpose” of the Active Directory implementation. This score is a statistical amalgamation of the component scores described below.
Security (logical Breakdown)	How well the directory has been structured to provide the best security for the organisation
Manageability (logical Breakdown)	How well has environmental control been implemented to increase the security and reduce the cost of ownership of the system
Stability (logical Breakdown)	How resilient is the directory and how resistant to uncontrolled change
Compliance (logical Breakdown)	How well the directory meets the demands of appropriate industry best practice guidelines and diligence requirements (for example ITIL or SOX)

Associated with each score are the assessor’s comments.

The report finishes with a set of suggested actions that would mitigate any serious issues uncovered.

2.2. Overall Scores

2.2.1. Overall Physical Stability

The Physical Implementation concerns those objects and structures that determine the availability and proximity of Active Directory services, while ensuring efficient replication of the directory data between the Domain Controllers.

The Active Directory is physically strong. Minor alterations to the configuration would further improve the replication and availability.

4.4

- Domain naming is appropriate
- No Trusts are evident
- Replication shows evidence that it could be more tightly channelled between sites
- UK Subnet identifiers needs re-modelling to bring them in line with the WAN sites
- UK DCs are both in same server room even though a second room on site is available
- Appropriately, all DCs are Global Catalogue servers
- Some flaws in DNS implementation (see below)
- Appropriately, all DCs are DNS and All Zones are AD integrated

2.2.2. Overall Logical Implementation

The Logical Implementation provides the security and virtually all the Return On Investment for the Active Directory.

The Active Directory is logically weak, particularly in the areas of security and change control.

Work is already underway to improve the architecture, advancing it from maturity level 2 up to level 3. This work is being well done, moving the organisation in the correct direction.

This trend must be continued to allow the development of effective role-based authority (a capability that appears at maturity level 4) and the creation of full documentation.

2.1

- The internal architecture is currently in transition from a level 2 to a level 3 implementation. This is a very positive move.
 - Moving to good object based structure, but naming convention is too complex and structure is still modelled on the organisation rather than the technology being managed
 - Moving to unified object based Group Policy objects from settings based objects
 - Access controls for Administrative delegation are appearing but using are individuals identities accounts instead of group identities
 - The first user and client authorities have been created, but will be unusable without appropriate extensions
- Groups scattered - built-in groups have been moved - group structures seem overly complex
- Generally consistent naming conventions are followed
- No documentation exists to describe either the original (lvl2) or proposed (lvl3) structures

2.3. Logical Breakdowns

2.3.1. Security

2.3

- Native Security is not in use to protect the directory architecture
- Password requirements are not long enough or complex
- Local authority passwords on all member systems are not changed regularly
- Most users have Administrative authority over their own workstations
- Administrators use the same login account for normal use (e.g. email, browsing) and administrative functions
- Authority is not hierarchically organised

2.3.2. Manageability

2.3

- Access Controls are not being used to support change control
 - One member of the "Domain Admins" group was an unknown user, created by an unknown source two months before the review
- Stronger change control procedures need to be enforced

2.3.3. Stability

2.2

- Group Policy is not being used effectively for environmental control
- Group Policy is not being used to enforce authority control

2.3.4. Compliance

1

- No Documentation
- No Role Based Authority

3. Suggested Actions

Most Significant Issues	Actions to Correct
DNS issues	The following Configuration should be updated <ul style="list-style-type: none"> • Fully implement scavenging • Allow only Secure dynamic update on any zones
Implement Role-based Authority	Optimise the logical architecture to at least level 4 maturity. Curtail the membership of all senior authority groups to a minimum and reinforce with Group Policy.
Separate Administrative Accounts	Create 2 nd accounts for all admin staff and move all Administrative authorities to them. Their normal user accounts (that have email and personal folders) should have no elevated privileges.
Implement Change Control procedures	Simple change control (the SharePoint Helpdesk template for example) would allow invaluable change control information to be centrally stored and indexed.
Fully Document the directory architecture	Full Documentation is critical to the organisations DR procedures, well as supporting the day-to-day administration, and the induction of new administrative staff.
Use GPO more effectively for environmental control.	This will lead to reduced complexity and reduced administrative overhead.

4. Further Reading

Please visit our web site for further reading about Active Directory matters. We have a selection of White Papers and Customer Case Studies for reading or download.

www.GenesisRKeyTec.com

Appendix A: Understanding Security and ROI for the Active Directory

The implementation of the Active Directory is done in two distinct phases. Each phase deals with the implementation of particular objects and structures which have specific purposes. The table below describes the nature of these phases and how they affect the overall maturity of the Active Directory.

Implementation Phase	Phase 1 (Physical)	Phase 2 (Logical)
Overall Goals Phase	Availability and proximity of Domain controllers Efficient replication	Security Authority Return on Investment Regulatory Compliance
Effect of phase on major deliverables:		
Manageability	20%	80%
Security	5%	95%
Compliance	None	100%
Stability	70%	30%
General Maturity of Implementations	Most Organisations clearly understand the goals and technology of this phase	Few organisations realise the full potential of the Active Directory and many that do lack the knowledge exploit it.
Knowledge/Skill Availability	Readily available. Training <i>always</i> stresses phase one.	Rare to find good understanding. Training usually conveys no more than 20% of the required technical knowledge (that defines how to build a solution) and none of the operational knowledge (that defines what should be build).
State of the AD	Installed and working	Secured and Manageable

Appendix B: 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 document is concerned with stateful audits.