Understanding the risks of legacy Active Directory architecture

White Paper

wanstor

Contents

+ The risk legacy Active Directory architecture presents to the business
+ Establishing the appropriate Active Directory architecture
+ Remediating existing forests
+ Where should you begin?
+ Enhanced Security Administrative Environments (ESAE)
+ Build a strong foundation

Introduction

Active Directory (AD) is Microsoft's technology for storing information about users, devices and systems that controls access to the Windows network, programmes and data in a universal manner across the IT infrastructure.

Microsoft provides several utilities bundled with AD such as Active Directory Users and Computers (ADUC) and Group Policy Management Console (GPMC) that can be used to manage data and policies within the directory.

Widespread integration of business applications, servers and workstations often leverage Active Directory as the source for access and privilege information.

When a business or not for profit organisation is faced with consolidation, migrations, new implementations, or remediating Active Directory environments, understanding the architectural approach is critical to maintaining security, user experience and cost targets for the business.

The Risk Legacy AD Architecture Presents to the Business

Stalled Growth

According to Gartner in their 2017 study of IT in mid-sized businesses, more than 50% of mid sized businesses are unable to extend incumbent AD architectures. This means they are unable to support their expanding digital workplace requirements - including access for an increasingly mobile workforce.

Degraded User Experience and Security Risk

The consumerisation of end user computing tools is forcing IT security leaders to restructure their efforts to offer protection against heightened risks without degrading the user experience (UX) objectives of a digital workplace. Traditional authentication methods, such as legacy password and X.509 smart cards, are no longer viable authentication choices for an employee-friendly IT workplace that uses “anywhere, anytime” computing models.

Most local access use cases cannot be tailored with the same authentication methods due to varied trust, accountability and integration requirements. It is advisable to choose from authentication methods that can offer consistent UX and minimally required trust throughout the business or not for profit organisation.

This intention is complicated by the mix of varied IT systems that appears in most mid-sized business or not for profit organisations. At Wanstor we generally see IT teams implementing more than one authentication approach to serve the varied requirements of different local access use cases. This introduces additional cost, increased complexity, inconsistent UX, and the inability to correlate authentication events and threats across the organisation.

Increased Cost Exposure

A poorly managed Active Directory architecture can incur significant extra costs. Especially if the business or not for profit organisation is facing a licensing audit by Microsoft. Over-reporting of SQL installations, picking up fragments of decommissioned machines and duplicated user account details are common in legacy AD environments.

This can result in inflated total device and user counts if not verified before submission, and, if you are in an Enterprise Licence Agreement (ELA), it can increase the risk of non-compliance for products that require an enterprise-wide commitment.

Establishing the Appropriate Active Directory Architecture

At Wanstor we understand that IT systems change rapidly due to new technologies, demands, and business drivers. At the heart of these systems are basic building blocks which include Active Directory.

Mid sized business and not for profit organisations are often faced with architectural decisions that contemplate consolidation, migration, new implementation, or maintaining the existing directory.

The right answers are derived by security requirements, desired management efficiencies, organisational restructuring, or compliance with regulations or other controls.

Understanding the subtle differences of each requirement and its potential solution is the first step in modernizing the Active Directory environment.

Understanding the risks of legacy Active Directory architecture

Typical architectural choices include:

Consolidation: Typical in the case of a merger or acquisition, one of the company directories and associated resources are migrated into the other directory, along with adoption of the associated policies, security, and management.

Greenfield: When there is no destination forest for a consolidation, or a company is looking for a fresh start to leave behind instability, security issues, or a simple name change then a new domain can be built to overcome these chronic or unresolvable issues.

Remediating Existing Forests: Companies may find that their desire to migrate is outweighed by the cost or complexity of migrating the associated resources from one domain to another. Others may find that the domain or forest security boundary is required to meet compliance or security requirements.

In those cases, remediation to correct issues can be done on existing forests. The inclusion of advanced tool sets such as Quest Active Roles Server can assist with allowing a logical coupling to streamline management and improve security.

Enhanced Security Administrative Environments (ESAE): Organisations may wish to redesign their directory structure to enhance privileged access to critical systems. This security model can be implemented in conjunction with any design choice in order to leverage advanced safe guards.

Example of a legacy Active Directory environment

Over a period of time, most AD environments accumulate a mix of both useful and discarded identity data. A common example is when a company acquires another organisation, sets up an Active Directory forest and discovers the acquired company has a legacy directory infrastructure from a previous acquisition.

Over time, the build up of unmanaged AD information can produce:

+ *Users with missing information due to poorly followed manual processes*
+ *Many forests and domains created by different IT groups with inconsistent standards for username, display name and email address, etc.*
+ *Disconnected Active Directory environments that do not communicate with each other, but collectively hold redundant user and group information.*

At Wanstor we have found these problems prevent an easy move to Office 365. A migration presents a chance to standardize on email address formats and an opportunity to clean up user data, such as job titles and department names.

Where Should IT Administrators Begin?

At Wanstor we believe every successful AD Architecture starts with proper implementation of Active Directory Core Services and establishment of Standard Use Cases.

Physical Design

Proper domain controller placement in the network, sizing, and making sure the right replication post-installation are the key elements of a successful Active Directory roll out. Other tasks such as high availability, redundancy, proper backups and recovery procedures are also critical to the physical health of the Active Directory implementation.

Other supporting services for name resolution and DHCP are often collocated with domain controllers, so any new rollout must consider the disposition of these services as well.

Logical Design

Alongside the physical roll out, the logical design and configuration of the new Active Directory is also required to make sure that the following areas meet the needs of the business:

+ **Organisational Unit (OU) Design:** Simplicity and perceptiveness are the keys to the design. Most policy and security configurations can be applied through a more useful set of filters than the organisational unit. Since a typical goal of the consolidation is to reduce IT management complexity, the segmentation of users by offices or business units is no longer required.

+ **Security (Role Based Access Control):** RBAC, Password Policies, Privileged Accounts. Making sure the proper roles are designed, implemented, and validated is essential to proper adoption of restricted privileged accounts. If IT administrators can be confident that they will have the rights they need when they need them, falling back to the Domain Admins group becomes less relevant.

Fine grained password policies can also strengthen the security around privileged accounts, as well as other sensitive user communities.

Group Policy (GPOs)

Extending security to the desktops and servers is the last mile in any governance policy and properly configured group policy will provide the majority of the requirements. Analysing and reconciling the current group policies in the existing domains is the first step in creating baseline GPOs for the new environment that can offer a simple and intuitive design that follows best practices.

Even with a design and implementation that adheres to best practices, there are still gaps in management and governance that can be addressed with many of the additional tools that ManageEngine ADManager offers including Change Auditor, GPOAdmin, Recovery Manager, and others. The right inclusion of these tools during the design and implementation will maximize the return on investment and prevent redundancies.

Ensure Active Directory is Optimized for the Cloud

Many business and not for profit organisations are moving toward Office 365 workloads in conjunction with their consolidation efforts. Proper planning is required to make sure that resources move in the correct order and that prerequisites are met and maintained as each workload is migrated. Almost any combination of the workload migration order can be supported.

Enhanced Security Administrative Environments

IT teams may want to redesign their Active Directory structure to enhance privileged access to critical systems. This security model can be implemented in conjunction with any design choice in order to leverage advanced safe guards. The right design would also include identity lifecycle management of privileged accounts. Mitigating the threat of “Pass-the-Hash” in any Active Directory environment hinges on stopping privilege escalation through credential theft. A solid foundation to for privileged account access includes:

Privileged Account Hygiene: Workstations that are isolated from Internet and email access are the first step to reducing the attack surface to gain control of the workstation. Adding two factor authentication for privileged accounts with smart cards to these machines completes the solution.

Hardened Workstations: The workstations are designed to be highly secure via specific hardware requirements, drive encryptions, and native or third party management tools. These systems can be traditional desktops, portable laptops, or remote desktop servers depending on the organisation’s needs.

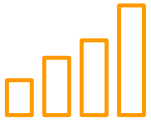
Monitoring: The addition of rigorous audit rules through both native tools and, optionally, ManageEngine’s AD Manager tool, can help IT teams to understand breaches in the environment and provide the audit trail required to prove compliance.

Building A Strong Active Directory Foundation

At Wanstor we recommend the following approach is taken by IT teams when attempting to tackle legacy Active Directory issues. Our advice is based on 15+ years experience of dealing with Active Directory issues.

Best Practice Active Directory Workshop

This is typically the first in-depth discussion where we will explore your Active Directory issues with stakeholders, executives, and business application owners to fully understand the business drivers and choose the high-level architecture.



Analysis

This is the review of the current environments to understand the network topology, current objects, policies, security requirements, and connected resources that would be in scope of the design.

Final Design and Executive Presentation

A final design would be produced and reviewed by the working team. This collaborative effort would then be presented to executive leadership for approval.

Detailed Planning

With the design signed off and a full understanding of the business goals, a detailed plan to execute the design can be created to understand both the timeline and the resourcing requirements.

Execution

A variety of services can be offered for the execution of the Active Directory clean up plan. Everything from consultation and guidance to a full turnkey execution of the design dovetailed into the desired migration, including full project management.

Previously, many mid sized business and not for profit organisations might have viewed a domain migration or Active Directory clean up as a simple exercise that could be completed by their internal IT team quickly with little disruption to end users. In fact up until a few years ago it wasn't uncommon to complete migrations over a long weekend and fix a few problems on Monday morning.

Active Directory has matured as a platform and many organisations are relying on it more than ever before. Having access to the right data, user profiles, and associated resources that depend on AD infrastructure to operate, must be understood and planned in advance to provide the new stable platform and a bridge to travel from the existing environment to the desired one.

Having access to the right experience in these types projects is critical to making that the user experience and business impact are both understood and meet the expectations of everyone involved.

Active Directory

Practical Management Solutions

What is ADManager Plus?

What is ADManager Plus?

ADManager Plus is a simple, easy-to-use Windows Active Directory Management and Reporting Solution that helps IT administrators and Help Desk Technicians with their day-to-day activities. With a centralized and intuitive web-based user interface, the software handles a variety of complex tasks like Bulk Management of User accounts and other AD objects, delegates Role-based access to Help Desk Technicians, and generates various AD Reports as an essential requirement in satisfying Compliance Audits. This tool also offers mobile AD apps empowering performance of important user management tasks right from mobile devices at any location with an internet connection.

What problems does ADManager Plus address?

- **Eliminates repetitive, mundane and complex tasks associated with AD Management**
- **Automates routine AD Management and Reporting activities for AD Administrators**
- **Facilitates Creation, Management and Deletion of AD objects in Bulk**
- **Provides 'on the move' AD user management capability through its mobile apps**
- **Acts as an essential resource during Compliance Audits like PCI, GDPR and ISO**

What features does it offer?

+ Single and bulk user management	+ Group Computer Management	+ Help Desk Delegation
+ O365 Management & Reporting	+ Active Directory Automation	+ Active Directory Cleanup
+ Active Directory Reports	+ Real Last Logon Reports	+ Exchange Management

Key Features of AD Manager Plus

Every IT administrator faces the challenge of managing Active Directory objects including users, groups, computers, OUs and more daily. Manually performing complex tasks such as configuring user properties is extremely time consuming, tiresome and prone to error. AD Manager Plus enables automation and simplification of many of these tasks, with key features including:

MANAGEMENT

+ Create users in AD, Exchange, Office 365, Google Apps, and Skype for Business (Lync) in a single step
+ Create or modify AD objects (users, groups, contacts, OUs, computers) in bulk via CSV import
+ Perform tasks like password reset, account unlock, clean up and more
+ Streamline management of AD objects such as users and OUs with customizable templates
+ Assign, replace, or revoke Office 365 licenses in bulk
+ Manage shared, remote, room, equipment mailboxes

OU & ROLE-BASED HELP DESK DELEGATION

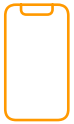
+ Delegate AD tasks to help desk technicians granularly within specific OUs
+ Delegate tasks like password reset and user creation
+ Delegate without elevating technicians' AD privileges

AD AUTOMATION & WORKFLOW

+ Automate routine tasks such as AD clean up
+ Manipulate automated tasks via workflow with automation
+ Configure review-approval workflows to execute AD tasks with a structured flow

REPORTING

+ Generate and schedule more than 150 preconfigured, granular reports on AD, Exchange, Office 365, and Google Apps
+ View inactive users, locked out users, disabled computers, and more in just few clicks
+ Perform management tasks for specific users within reports
+ Export to various formats: HTML, PDF, XLS, XLSX, CSV, CSVDE
+ Mention specific users or computers in a CSV file for generating their important details
+ Generate compliance reports to meet regulatory standards such as PCI, GDPR, ISO and more



iOS & ANDROID APPS

+ Manage users from anywhere - reset passwords; unlock, enable, disable and delete accounts
+ Report on locked out, disabled, password, expired, inactive users
+ View, manage, and execute AD workflow requests

Other Active Directory Tools by Wanstor & ManageEngine

		Features & Benefits
ManageEngine ADSelfService Plus	ADSelfService Plus is an IT self-service solution designed for Windows environments. It is a feature rich IT self service solution which can be implemented independently or integrated seamlessly with company websites.	+ Self-service password management for on-premises Active Directory and cloud applications + Notify users (email & SMS) on impending password & account expiration + Enforces granular password policies across AD and connected on-premises and cloud applications + Automatically syncs Active Directory password in real-time across multiple applications + Offers Active Directory-based single sign-on (SSO) for cloud applications
ManageEngine ADAudit Plus	In real-time, IT administrators can ensure critical resources in the network like Domain Controllers are audited, monitored and reported on with information on Users, Groups, GPO, Computer and OU changes, with 200+ detailed event specific reports and instant email alerts.	+ Web-based, Active Directory tool to track all domain events, including user, group computer, GPO, and OU changes + Audits Windows files servers, failover clusters, NetApp for doc changes to files and folders, audit access + Monitors every user logon and logoff, including every successful and failed logon event across network workstations + Tracks Windows member servers, FIM, printers, and USB changes with events summary; tracks application, policy, and system events + Brings 150+ ready-to use audit reports with instant email alerts to ensure security and meet IT Compliance requirements
ManageEngine Exchange Reporter Plus	ManageEngine Exchange Reporter Plus is a comprehensive web-based analysis & reporting solution for Microsoft Exchange, providing over 100 different reports on every aspect of the Microsoft Exchange Server environment.	+ Web-based change auditing / reporting solution for MS Exchange environments + Track / monitor enterprise ActiveSync infrastructure & inventory of related smart devices + Report on Outlook Web Access usage, mailbox traffic, mailbox growth + Supports customized reports that use data filters, automatic scheduling, and multi-format report generation + Provides audit feature to enable investigation of unauthorized mailbox logons and other critical changes
ManageEngine RecoveryManager Plus	Empowers IT teams to back up changes made to AD objects as separate versions, providing an Exchange Online backup solution for numerous Exchange functions & data	+ Automated incremental backup of Active Directory objects + Simple and granular restoration down to the attribute level + Change tracking to undo changes + Detailed version management of each attribute change + Provision to roll back Active Directory to an earlier state

		Features & Benefits
ManageEngine **SharePoint Manager Plus**	ManageEngine SharePoint Manager Plus is a tool that helps IT administrators to manage, audit and report on both on-premises and Office 365 SharePoint environments. It also allows monitoring, tracking and analysis of all activities in a SharePoint infrastructure, which facilitates informed, timely and accurate decision-making and management.	+ Web-based tool to manage and audit SharePoint on-premise servers and Office 365 configurations + Provides complete infrastructure visibility into both on-premise and online SharePoint server components + Includes out-of-the-box reports for monitoring SharePoint components such as farms, content databases, web applications, site collections, sites, lists and document libraries + Performs component level and security level auditing. Tracks permission changes, group changes and new role changes instantly with alerts + Meet compliance requirements by archiving audit log data for flexible time period
ManageEngine **DataSecurity Plus**	ManageEngine DataSecurity Plus is agent-based, real-time file auditing & reporting software that delivers complete visibility into Windows file server environments, showing IT administrators the 'who, what, where and when' behind every access event while also perform storage analysis. This helps to improve organisational Windows file server data security and information management, in a simple yet efficient and cost-effective way.	+ Web-based, real-time Windows file server access auditing & storage analysis tool helping meet data security, information management & compliance needs + Track & analyze access to files & folders by inspecting anomalies, recording access patterns & examining share & NTFS permissions + Optimize storage space by isolating old, stale & non-business files, gain insight into disk space usage & viewing file and folder properties + Actively respond to security breaches with instant email alerts. Detect & counter ransomware with mass access alerts & response automation + Stay compliant with SOX, HIPAA, FISMA, PCI, GLBA, GDPR, and other regulatory mandates
ManageEngine **O365 Manager Plus**	Providing exhaustive preconfigured reports on Office 365 & helping IT administrators perform complex tasks including bulk user & mailbox management, secure delegation and more. Monitor Office 365 services 24/7 and receive instant email notifications about service outages. 0365 Manager Plus eases compliance management with built-in reports, offering advanced auditing & alert features to keep Office 365 setups secure.	+ An Office 365 reporting, monitoring, management and auditing tool + Utilize out-of-the-box reports Exchange Online, Azure Active Directory, OneDrive for Business and Skype for Business, as well as reports on security, compliance management and licences for Office 365 + Monitor Office 365 service health around the clock, and receive instant email notifications on service outages + Effortlessly oversee your Office 365 setup with a wide range of Exchange Online and Azure Active Directory management features + Track even the most granular user activities in Exchange Online, Azure Active Directory, OneDrive for Business, Sway, and other services + Audit critical activities and changes in your Office 365 environment with custom alerts for each Offices 365 service + Delegate Office 365 administration tasks granularly to help desk staff and other non-IT users through role-based delegation

Wanstor's ManageEngine Customers

Final Thoughts

Every IT Administrator faces a number of Active Directory management challenges, which include managing user accounts in Active Directory almost every day.

Configuring user properties manually is extremely time consuming, tiresome, and error-prone, especially in a large, complex Windows network.

A solution that can automate cumbersome, boring, repetitive tasks, simplify AD management and provide exhaustive reports on tasks completed is now a must-have for all proactive IT departments, no matter what the size of their organisation.

Wanstor is ManageEngine's largest European partner. We work with ManageEngine to plan, deploy and manage Active Directory tools such as ADManager Plus in helping IT administrators overcome their Active Directory management challenges.

Our Active Directory management tools are designed to offer IT professionals absolute control over their Active Directory environment, with the main toolset that we recommend being ADManager Plus.

ADManager Plus is comprehensive web-based Microsoft Windows Active Directory management software that simplifies user provisioning and Active Directory administration with complete security and authentication, allowing only authorized users to perform management actions.

It also provides a complete set of management tools to IT administrators for efficient management of Active Directory.

For more information about Wanstor and ManageEngine's Active Directory management solutions, call us on **0333 123 0360**, email us at **info@wanstor.com** or visit our website at **www.wanstor.com** and one of our Active Directory experts will be in touch.

Wanstor | 124-126 Borough High Street | London | SE1 1LB | info@wanstor.com

wanstor