XMS SOLUTIONS

Quest

Privileged Perspective: Understanding the Risk of Legacy AD Architecture

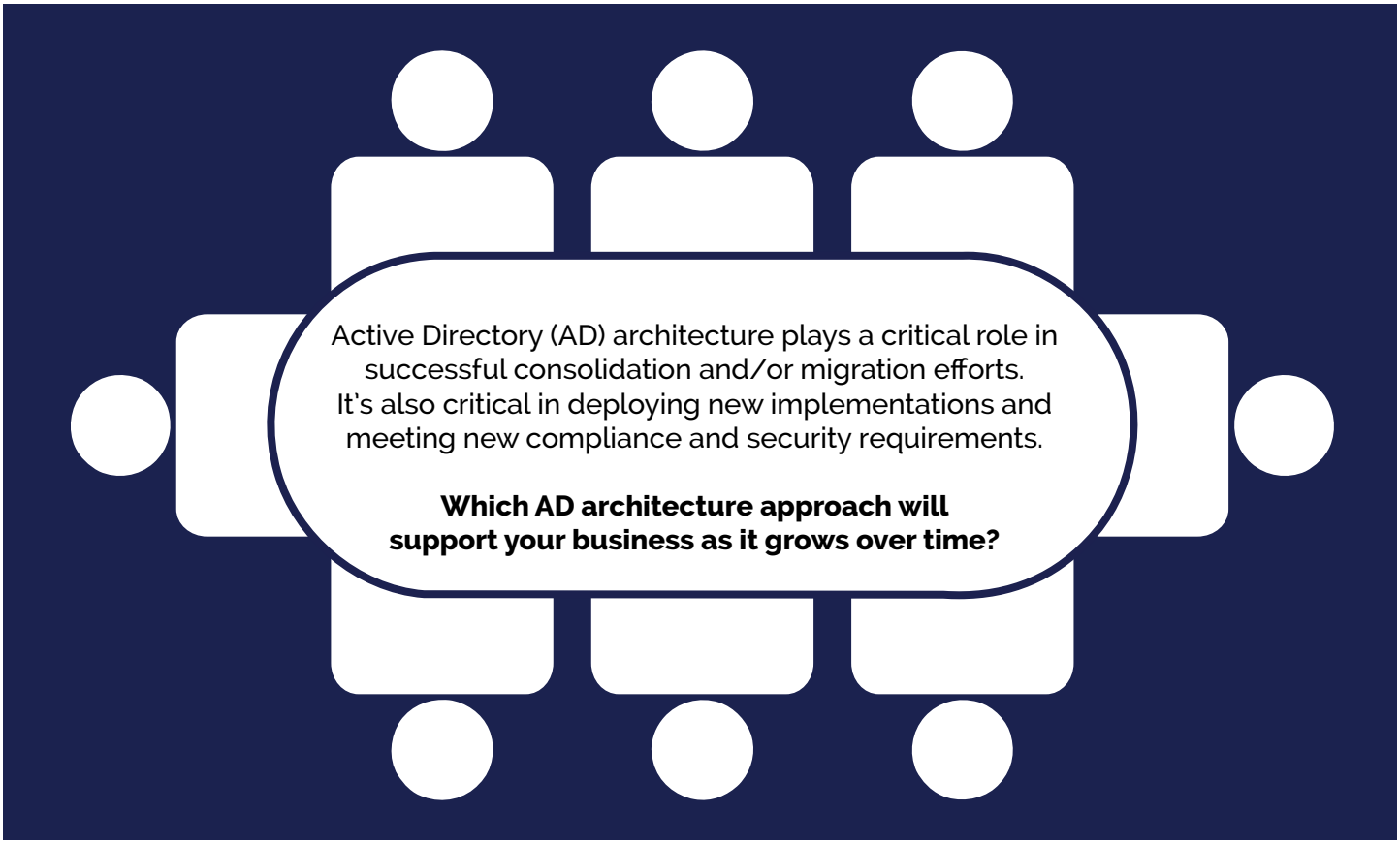


TABLE OF CONTENTS

INTRODUCTION

Active Directory (AD) is Microsoft's technology for storing information about users, devices and systems that controls access to the Windows network, programs and data in a pervasive 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.

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

When companies are faced with consolidation, migrations, new implementations, or remediating Active Directory environments, understanding the proper 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 a recent Gartner study, more than 50% of organizations are unable to extend incumbent AD architectures to support their expanding digital workplace requirements — including access for an increasingly mobile workforce.

Degraded User Experience, Security Risk

The consumerization of workplace computing tools is forcing security leaders to restructure their efforts to offer protection against the 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 workspace that uses "anywhere, anytime" computing models.

Most local access use cases can't be fitted with same authentication methods due to varied trust, accountability and integration requirements. While it is advisable to choose from authentication methods that could offer consistent UX and minimally required trust throughout the enterprise, this intention is complicated by the mix of heterogeneous IT systems that appears in most enterprises. IT teams often end up 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 organization.

Cost Exposure

A loosely managed AD architecture can incur significant cost, especially if the business faces a licensing audit by Microsoft.

Over-reporting of SQL installations, picking up remnants 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 EA, it can increase the risk of noncompliance for products that require an enterprise-wide commitment.

Active Directory Modernization Engagements with the IT staff, stakeholders, and application owners should develop a plan forward and then execute on these plans, ensuring these foundational services are properly supporting the organization and meet the unique needs of each business.

Establishing the Appropriate Active Directory Architecture

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.

Companies are often faced with architectural decisions that contemplate consolidation, migration, new implementation, or maintaining the existing directory. The right answers are driven by security requirements, desired management efficiencies, organizational restructuring, or compliance with regulations or other controls. Understanding the nuances of each requirement and its potential solution is the first step in modernizing the Active Directory environment.

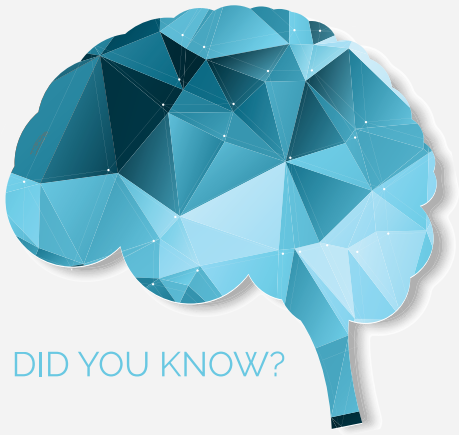
Typical architectural choices include:

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)
Organizations 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.



Over time, most AD environments accumulate a mix of both useful and discarded identity data.

A common example is when a company acquires another organization, sets up an Active Directory forest and discovers the acquired company has a legacy directory infrastructure from a previous acquisition.

Over time, the buildup 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.

These problems always 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 You Begin?

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 ensuring proper 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

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

Organizational Unit (OU) Design
Simplicity and intuitiveness are the keys to the design. Most policy and security configurations can be applied through a more useful set of filters than the organizational 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 long required.

Security (Role Based Access Control - RBAC, Password Policies, Privileged Accounts)
Ensuring that the proper roles are designed, implemented, and validated is essential to proper adoption of restricted privileged accounts. If 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. Analyzing 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 Quest offers including Change Auditor, GPOAdmin, Recovery Manager, and others. Proper 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 companies are moving toward Office 365 workloads in conjunction with their consolidation efforts. Proper planning is required to ensure 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.

Secure Privileged Access With A Red Forest

Enhanced Security Administrative Environments (ESAE)

Organizations 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. Proper design would also include identity lifecycle management of privileged accounts in the Red Forest.

Mitigating the threat of Pass-the-Hash in any Active Directory environment hinges on preventing privilege escalation through credential theft. A Red Forest is a solid foundation to provide high trust workstations for privileged account access. **This trusted model provides the following advantages:**

Privileged Account Hygiene
Workstations that are isolated from Internet and email access are the first step to reducing the attack surface for 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 organization's needs.

Monitoring
The addition of rigorous audit rules through both native tools and, optionally, Quest Change Auditor, can help customers understand breaches in the environment and provide the audit trail required to prove compliance.

Hank the Hacker appears in all shapes and sizes, from malicious cyber-attackers using sophisticated threat tactics like spear phishing emails, Ransomware or pass-the-hash techniques … to disgruntled ex-employees, temporary contractors, and even accidental changes made by careless employees.

Hank's big prize? Your Active Directory. It's his crown jewel, and, if he cracks it, he controls your network, its data, the devices on it — the whole shebang.

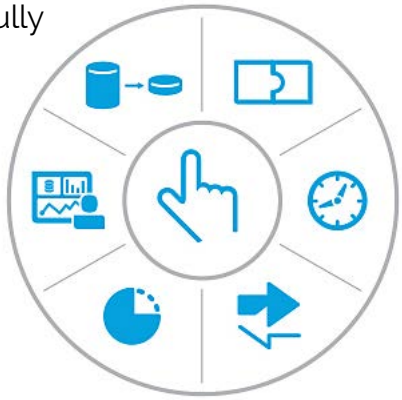
Are you ready to do what's necessary to stop Hank the Hacker and a million others like him?

Click here to learn more.

Build A Strong Foundation

XMS Best Practice Planning Engagement

Workshop
This is typically the first in depth discussion with the client representatives including stakeholders, executives, and business application owners to fully understand the business drivers and choose the high-level architecture.



Detailed Analysis
This effort 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 in hand along with 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 detailed plan. Everything from consultation and guidance to a full turnkey execution of the design dovetailed into the desired migration, including full project management.

Conclusion

In the past, companies might have viewed a domain migration as a simple exercise that could be completed by their internal team quickly with little disruption to end users. It wasn't uncommon to complete migrations over a long weekend and fix a few problems on Monday morning.

With the maturation of Active Directory and the associated resources that depend on this infrastructure to operate, upgrades and changes must be understood and planned to provide the new stable platform and a bridge to travel from the existing environment to the desired one. The proper experience in these types projects is critical to ensuring that the user experience and business impact are both understood and meet the expectations of everyone involved.

ABOUT XMS SOLUTIONS

The rush of new people and things accessing systems and devices has created previously unimagined risks around scale and security.

Since 2008, XMS Solutions has been helping enterprise and mid-market customers solve the challenges of growing access needs, providing IT leaders answers to the question of who has access to what. Our heritage provides us a unique perspective on how systems are accessed, used and managed. Our partnerships give us the leading edge in designing, deploying and managing the best Enterprise IAM and Collaboration solutions in the market today.

Collaboration Without Limitation means we are laser-focused on making security, identity management, messaging, and directory services components work together to achieve our customers' goals in ways they never imagined possible. Our architects, consultants, and business analysts are amongst the most sought-after in our industry, bringing decades of experience and practical application know-how to each and every project we undertake.

One of Gartner's Top IAM Service partners for 2017, XMS helps IAM leaders understand, implement and communicate value-driven security solutions that enable security and empower productivity.

Contact us today to learn more:

XMS Solutions, Inc.
www.xmssolutions.com
sales@xmssolutions.com
702-940-6545