Improving AD security through consolidation and modernization

Quest

Active Directory (AD) architecture plays an important role in keeping your organization safe from threats. It is important to ensure you keep up with AD compliance and security requirements as they change over time.

If you have multiple AD environments or aging environments, it becomes more difficult to control your risk. Consider performing an AD migration and consolidation to modernize and improve security.

Introduction

AD is the standard architecture used for identity and access management (IAM) in a networked environment. Using a combination of built-in Microsoft utilities and third-party solutions, you can manage devices, policies and resource access in a pervasive manner across your IT infrastructure.

Companies integrating applications, servers and workstations often use AD as their source for access and privilege information. That increases the importance of having proper security controls in place. As companies migrate user content to Microsoft 365 workloads, tools like Azure AD Connect (AADC) and Azure AD Cloud Sync enable integration between Active Directory and Azure AD, providing additional access points that must be properly managed and secured.

Many companies end up managing multiple AD environments over time, which can cause management and security problems. In some cases, they have configured multiple AD environments during initial deployment to split geographical or business units or to create a Red Forest for privileged accounts. In other cases, they have performed a tenant-to-tenant consolidation during a merger, acquisition or divestiture, without consolidating the AD environments.

When managing multiple AD environments or legacy AD environments, consider whether AD migration, consolidation and modernization can help reduce risk, lower operational costs and improve your overall security posture with centralized control.

Challanges with multiple environments

Inconsistent policies and management tools

Companies have custom AD policies and use different tools to assist with domain management. During a merger or acquisition, the combined organization must identify and address conflicting policies to allow the domains to coexist successfully. Unnecessary operational overhead can result if the domains use different tools for management and software deployment.

Multiple and dispersed administrators

Privileged accounts are used to perform AD management tasks that can have forest-wide and domain-wide impacts if used incorrectly or compromised. Managing multiple AD environments increases risk by introducing additional privileged accounts.

Directory synchronization and coexistence

Coexistence solutions such as directory synchronization are frequently deployed to reduce the impact on end-users. Common solutions provide password synchronization, group membership sync, unified global address lists (GALs) and direct resource access through trusts and Security Identifier (SID) history. These coexistence solutions take time to configure and maintain, and integrating them generates additional risk if accounts are compromised.

Challenges with legacy AD architecture

Red Forest retirement

Previous guidance from Microsoft recommended a Red Forest security architecture that used a separate, trusted AD forest for administrative accounts in an Enhanced Security Admin Environment (ESAE). The goal was to provide better protection against cyberattacks. But Red Forest environments require additional overhead and have not been immune to the increased number of cyberattacks; therefore, Microsoft no longer recommends this configuration and is retiring ESAE.

The updated guidance is to use modern, privileged-access strategies based on Zero-Trust principles to secure and manage privileged accounts within your primary AD. Microsoft's rapid modernization plan (RAMP) provides a roadmap with steps to help you meet modern security recommendations.

Determining the future state of your AD

Companies that embark on a consolidation or modernization effort must first decide on the desired end-state of their AD environment and related architecture. Consider your business requirements and technical requirements when making this decision.

Consolidate to an existing AD

In a typical merger or acquisition, one of the company directories and its related resources are migrated into the other directory, and associated policies, security and management are adopted. Consolidating into an existing environment usually has less business impact and lower project costs than other options.

Consolidate to a greenfield AD

When a company is looking for a fresh start to leave behind instability or security issues that cannot be remediated, then a new AD environment can be built to overcome any chronic or unresolvable issues. Consolidating to a greenfield environment requires additional time and effort to set up the directory from scratch. It also involves managing duplicate infrastructure for some length of time.

Start the Azure AD migration

Companies that have migrated most of their workloads to Microsoft 365 can also consider a complete migration to Azure AD. Once all the users, groups and devices are cloud-only, the legacy AD can be decommissioned. This option is best for companies that do not have many legacy resources or applications remaining on premises, because those systems will require additional time and effort to convert to cloud-only.

Remediate existing forests

Some companies find that their desire to migrate is outweighed by the cost or complexity of migrating the associated resources from one domain to another. Others find that the existing domain or forest security boundary must remain as is to meet compliance or security requirements. In those cases, remediation of security holes must be completed on existing forests.

Advanced tools such as Quest® Active Roles® Server can assist in streamlining management and improving security.

Where should you begin?

Every successful AD consolidation starts with discovery workshops and a detailed environment analysis. The result is a consolidation plan that meets all business requirements and technical requirements with as little impact to business operations as possible.

Environment discovery

Identify all forests, domains and child domains that your company manages. Document architectural details of each, highlighting similarities and differences.

Organizational unit (OU) design

Determine which structure will work best for IT management. Many policy and security configurations can be applied through filters other than the organizational unit, so segmentation by offices or business units is no longer required.

Policy review

Compare policies in each environment and determine which ones to retire and which to retain in the consolidated environment. Reduce privileged accounts to the fewest users necessary and implement strong password policies to strengthen the security around all account types.

Group Policy (GPOs)

Extending security to the desktops and servers is the last mile in any governance policy. Analyzing and reconciling the current group policies in existing domains is the first step to creating baseline GPOs for the consolidated environment.

To assist in designing and implementing best practices, preventing redundancies and addressing governance needs, Quest offers tools such as Change Auditor, GPOADmin® and Recovery Manager.

Microsoft 365 integration

Many companies are moving toward Microsoft 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.

Quest On Demand Migration provides solutions for all your AD migration and consolidation needs, including account provisioning, directory synchronization, GAL sync and device migration from AD and hybrid environments to any other environment, including Azure AD.

Did you know?

Over time, most AD environments accumulate a mix of both useful and discarded identity data. Over time, the buildup of unmanaged AD information can produce:

- Users with missing information due to poorly followed manual processes
- Forests and domains managed by different IT groups with inconsistent standards for fields like username, display name and email address
- Disconnected environments that do not communicate with one another but collectively hold redundant user and group information

AD consolidation is an opportunity to standardize on naming formats, clean up user data and eliminate duplication.

About Quest

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Microsoft 365 migration and management, and cybersecurity resilience, Quest helps customers solve their next IT challenge now. Around the globe, more than 130,000 companies and 95% of the Fortune 500 count on Quest to deliver proactive management and monitoring for the next enterprise initiative, find the next solution for complex Microsoft challenges and stay ahead of the next threat. Quest Software. Where next meets now. For more information, visit www.quest.com.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our website (www.quest.com) for regional and international office information.