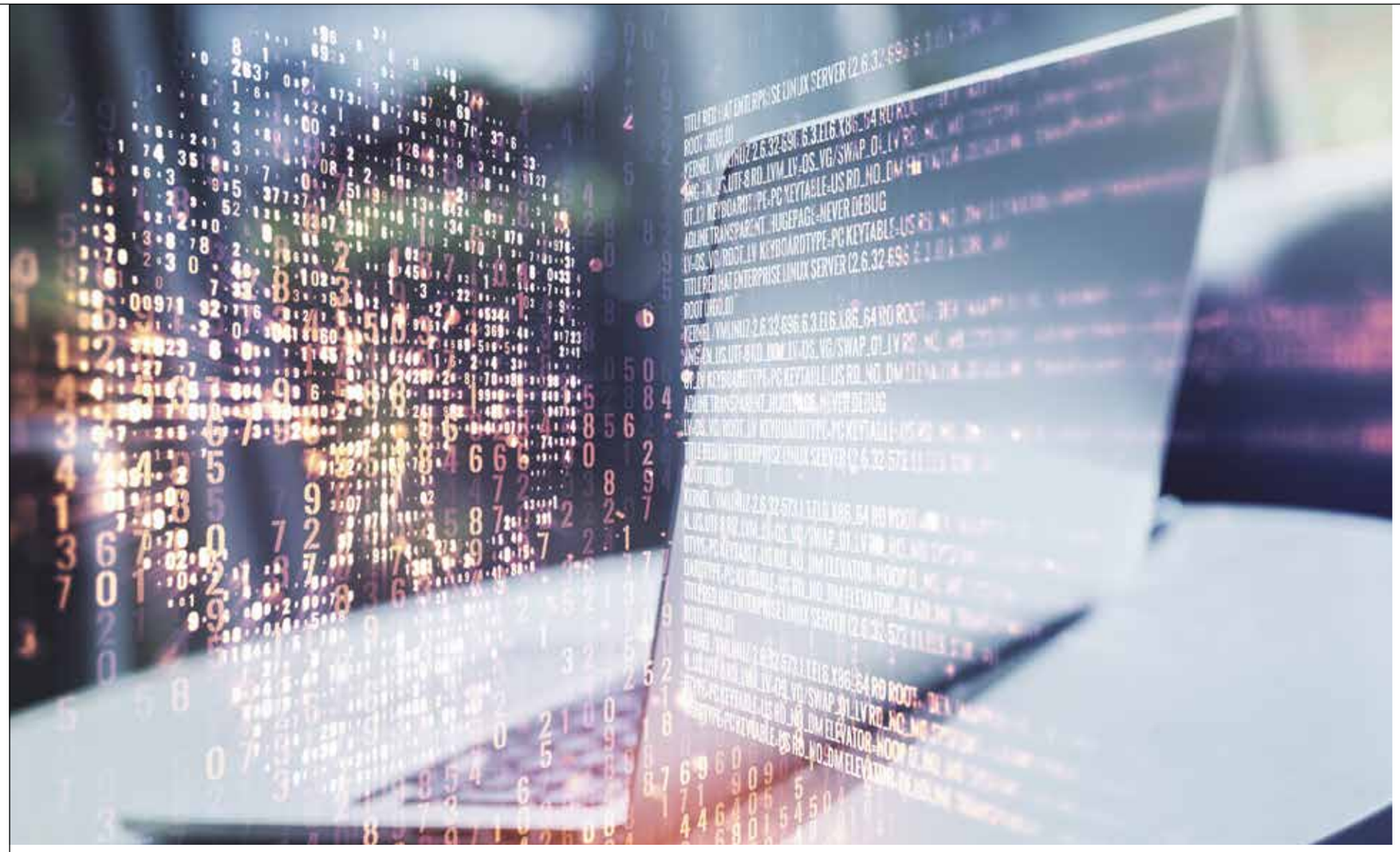

FOREST FIRE!

Dan Lattimer *explores the challenges and misconceptions of AD forest structures*

Microsoft Active Directory (AD) is fundamental to the operational success of most enterprises today. Understanding why involves looking at its origins. Before AD, Microsoft's IT directory servers couldn't scale for medium and large enterprises, requiring multiple servers. For example, a tech company with 1,000 employees might have needed up to 200 servers. Managing these servers was challenging, with each requiring unique log-in credentials and file sharing was cumbersome due to poor communication between servers.

AD revolutionised this by integrating seamlessly with applications and providing single sign-on across a business environment, transforming network management and becoming ubiquitous. Over the past two decades, AD's prevalence has grown, serving as the foundation for most cloud identity systems used by enterprises worldwide.

Today, AD remains the central point for authentication and authorisation for most on-premises applications and data, extending these functions to cloud applications through synchronisation and federation with Entra ID, Okta, and other cloud identity providers.

Given the critical role Active Directory plays in most organisations' IT infrastructures and the significant risks posed by its compromise, the frequency of attacks targeting it is only expected to rise.

To effectively mitigate these threats, organisations must first grasp the complexities and misunderstandings surrounding AD, particularly within forest structures.

Having been designed to address bandwidth and replication limitations, AD's architecture focused on accommodating multiple domains within a forest. However, a prevalent misconception was that each domain within served as a distinct security boundary, leading many organisations to proliferate domains unnecessarily. In reality, this approach has introduced management complexities and heightened vulnerabilities.

With the support of experts, AD migrations can become a seamless endeavour, with no major issues arising throughout the process thanks to proper process management and experience

As technology advanced, it became evident that multiple domains did not inherently bolster security, but instead expanded the attack surface of AD environments. Instead of each individual domain being protected by its own perimeter, it became apparent that the compromise of any single domain within a forest could potentially jeopardise the entire environment. Consequently, many organisations now grapple with the challenges of managing and protecting multi-forest environments – namely, their ability to multiply risk. For this reason, initiatives aimed at removing the complexities associated with AD forests are now essential for security teams to pursue.

Naturally, the most effective strategies often revolve around modernising AD by consolidating multiple forests into a unified environment. By reducing the number of forests, organisations can simplify management, reduce complexity and minimise opportunities for attackers to exploit inherent trust relationships between forests.

Moreover, consolidating forests enables organisations to centralise the enforcement of security policies using tools such as Group Policy Objects (GPOs), Intune or System Center Configuration Manager (SCCM). This centralised approach strengthens security, streamlines management tasks and reduces operational overhead.

Without question, modernising AD in this manner is critical for reducing security risks associated with trust abuse and minimising the attack surface of the environment. Simplifying AD architecture not only enhances security but also improves operational efficiency, thereby bolstering overall cyber security posture and lowering IT management costs.

Embarking on the consolidation process isn't straightforward. Indeed, it demands meticulous planning and foresight. Successful AD consolidation projects entail migrating users, groups, computers and applications from one AD domain or forest to another – a process that requires a systematic and comprehensive approach that considers every facet of the migration process. Therefore, careful consideration of applications, security configurations and the unique sensitivities within organisational environments is paramount.

Planning for challenges and key components of AD migration is vital to ensuring a successful migration aligned with business, IT and security requirements. Adhering to best practices is a must. Not only do you need to take a thorough inventory of all resources and create a detailed migration plan. Equally, you will also need to test and validate the destination environment and provide comprehensive training and support to end users and IT staff. It might sound like a lot, but investing effort in these areas will pay dividends, mitigating risks such as downtime, security vulnerabilities, and post-migration frustrations. So, where should organisations start?

Critically, there are four key phases of any AD modernisation that need to be followed to ensure success.

PREPARATION OF SOURCE ENVIRONMENT

As mentioned, before you begin any migration, you need to develop a carefully thought-out plan that accounts for all the potential factors that could impact the migration's success. Here, it is necessary to identify all resources that the migration will affect, determine the order in which you will migrate them, create a schedule for doing so, and ensure that all the necessary hardware and software needed to support this process is available.

In addition, it's also important to find and fix any existing vulnerabilities so that your new environment doesn't inherit historical technical debt. By assessing your source AD environments using guidance from frameworks such as MITRE ATT&CK, you will be able to identify any security problems such as weak passwords or unsecured systems and remediate them before migrating to the new destination environment.

KNOWING WHERE TO START OR HOW TO EXECUTE EACH PHASE EFFECTIVELY IS TRICKY

PREPARATION OF DESTINATION ENVIRONMENT

With the source environments audited and addressed, you can then turn your attention to the destination environment. Here, domain design must be a primary consideration, ensuring that this caters to any current or future organisational requirements or needs in respect of scalability, performance, security and administrative overheads.

To get this right, it's worth creating an exact copy of the production AD that will enable you to test the migration process and identify potential issues or vulnerabilities before making key changes to your actual environment. This way, unintended changes can also be rolled back, and you can validate that everything works correctly, from domain controllers to group policies, applications and user authentication and access processes.

MIGRATION EXECUTION

With these foundational pieces of the puzzle in place, organisations may proceed with executing the migration, consolidating their AD in a security-conscious way.

Here, there are several aspects to consider:

Migrate users and groups: Ensure minimal disruption by preserving permissions and access rights during AD migration. Add original SIDs from the source forest to the sIDHistory attribute in the destination AD forest to maintain access to original resources. Alternatively, update ACEs for new users and groups.

Migrate user profiles and computer accounts: Conduct an inventory and plan for compatibility issues. During migration, ensure correct configurations and network settings for computers to maintain an optimal user experience. Verify all user data, settings and configurations post-migration.

Examine authentication protocols and encryption algorithms: Ensure compatibility of authentication protocols and encryption algorithms in the destination environment to prevent failures, data loss or unauthorised access.

Enable password synchronisation: Facilitate seamless access to resources in the destination environment by configuring password synchronisation. Test remote connectivity scenarios before and after migration.

Migrate resources: Ensure printers, file shares, applications and other IT resources are correctly

migrated with preserved permissions. Conduct a pre-migration inventory to determine compatibility and work with resource owners to update permissions in the destination environment. Test resources post-migration.

Migrate multi-tier architecture: Address compatibility issues in highly customised multi-tier architectures by accounting for specialised configurations and dependencies. Adapt applications to function correctly in zero trust or least privilege environments.

Migrate applications: Include all AD-dependent applications and systems in the migration to prevent security vulnerabilities. Conduct a pre-migration inventory, ensure stringent security controls in the destination environment and verify successful migration.

IT'S VITAL ORGANISATIONS GRASP THE COMPLEXITIES SURROUNDING THE ROLE ACTIVE DIRECTORY PLAYS

CONTINUOUSLY MONITOR YOUR MODERNISED AD

After completing these steps and finalising the migration, it's crucial to recognise that this isn't the endpoint but rather the beginning of ongoing efforts. Indeed, continuously monitoring the new environment is critically important to maintain its security and resilience against vulnerabilities. In addition to regularly scanning for potential security threats, organisations should vigilantly watch for unauthorised access attempts, changes in permissions or any other abnormal network activities. Regular security audits and penetration tests are also essential to proactively safeguarding the environment.

Furthermore, it's essential to back up the original environments and subsequently decommission them. As part of this process, any unnecessary SID history attributes that could pose security risks should be removed, although it's important to ensure that you retain the ability to swiftly restore these should it be needed. Above all, security must be the guiding principle throughout the entire migration process. Every step that you take must prioritise enhancing the security posture, aiming to establish a more secure and manageable environment.

This latter point is particularly critical given the escalating frequency of high-profile cyber attacks targeting Active Directory infrastructures. Years of configuration drift and lax, outdated security practices have introduced numerous vulnerabilities for many companies, with many facing significant security challenges from managing a complex web of multi-forest environments.

Accumulating technical debt is common across systems, but the criticality and sensitivity of Active Directory magnifies the associated security risks. In this case, a breach in the least secure AD forest could serve as a foothold for attackers to infiltrate more sensitive environments owing to the trusts that exist between different forests within a network. As these misconfigurations have proliferated, so too has the attack surface, highlighting the urgency of AD modernisation for bolstering security.

By following these four key phases, organisations can enhance both security and operational efficiency, thereby improving the user experience within a streamlined AD environment. Of course, this is easier said than done. For many, knowing where to start or how to execute each phase effectively can be tricky. However, with the support of experts, AD migrations can become a seamless endeavour, with no major issues arising throughout the process thanks to proper process management and experience.

Yes, AD modernising and migration is a priority. However, getting it right is equally important. Therefore, it's worth investing in the necessary arrangements to ensure that any migration and consolidation project stays on track, prioritising an improved AD security posture throughout the process. ●

DAN LATTIMER is Area VP, UK & Ireland for Semperis.

Simplifying AD architecture not only enhances security but also improves operational efficiency, thereby bolstering overall cyber security posture and lowering IT management costs.