Modernizing Your Active Directory Environment

Active Directory Modernization is Critical. Here's How to Achieve It.

Written By Darren Mar-Elia, president and CTO of SDM Software and Microsoft MVP

Abstract

Microsoft® Active Directory® (AD) has been on the market ever since the release of Windows 2000. In the early days, AD's main purpose was to provide centralized user authentication and authorization for Windows desktops and servers, and to provide a scalable directory service for organizations running directory-enabled applications such as Microsoft Exchange.

Since then, much has changed in the way organizations use and manage AD, including best-practice recommendations from Microsoft, enterprise AD management styles and the creation of many regulatory requirements that affect it. These changes are prompting organizations to take a fresh look at their AD deployments. By modernizing your deployment, you can improve manageability, security, recoverability, performance, auditability and governance.

This white paper explores why AD modernization is important and what it looks like, highlighting the areas you should focus on to ensure your AD infrastructure can meet your organization's needs now and into the future.

The shifting AD landscape

Both technology and the business environment have changed in important ways since AD was first released. In particular, the following changes to the AD landscape have almost certainly impacted your organization:

- Enhancements and shifting best-practice recommendations from Microsoft
- Multiple people managing AD to different standards
- Expansion of the role of AD in the organization
- Increasing regulatory requirements around security and access control to sensitive data

Each of these changes has a unique role in the need for Active Directory modernization.

Modernizing your AD deployment will enable you to take advantage of Microsoft's new best practices and the new features available to you.

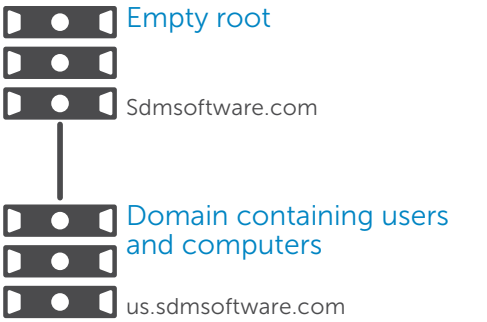

Figure 1. An empty root domain deployment

Changes in Microsoft guidance and AD capabilities

Microsoft's guidance on the use of AD has changed significantly, and so has AD itself. Modernizing your deployment will enable you to take advantage of new best practices and features that are available.

For example, the following two principles were common practice for early adopters but are no longer necessary:

- **Empty forest root domain**: At first, Microsoft encouraged organizations to create a root AD domain that contained no resources, as shown in Figure 1. This recommendation came from the idea that the forest root domain (that is, the first domain built) had a special role to the organization and should be left pristine. This advice has long been abandoned by Microsoft, which now recommends simply creating the domains that meet the needs of your organization, since additional domains increase complexity and present additional security requirements — especially when they are unused. Nevertheless, many shops still have AD forests containing not one, but two (or more) domains, with the root domain largely unused.
- **Domain as security boundary**: Another bit of guidance provided by Microsoft in the early days was that multiple forests should generally be avoided, because of the difficulties of integrating different forests together from a security and administrative perspective, and because of the notion that a single Active Directory domain was a security boundary — that given a forest with two domains, users and resources in domain A could be easily protected from users and resources in domain B. After a series of widely published articles showing how easy it was for domain administrators in one domain to control resources in another domain within a single forest, Microsoft shifted its guidance to make the forest, not the domain, the security boundary; if you need to isolate resources or users in a particular domain, you need to build a new forest. Accordingly, organizations now typically have multiple forests — for example, it is not uncommon to have a development forest that is separate from a production forest, or even to have an internet-facing forest that is separate from the others. Of course, as a result, organizations must deal with the resulting challenges of managing multiple forests.

Other best-practice recommendations have also evolved as a result of enhancements to AD itself. For example, Microsoft has improved AD in areas such as auditing, security delegation, scalability (remember the 5,000 group member limit in Windows 2000?), recoverability (with AD snapshots and the recycle bin) and automation (with Windows PowerShell®-based AD administration). By modernizing your deployment, you can take advantage of these enhancements to improve the way you secure, manage and recover AD.

Changes in administrative model

Another area that has changed is the way AD is administered by most organizations. Years ago, a small group of administrators was typically responsible for all aspects, from its infrastructure to the content that went into the directory. Today, AD plays a greater role in the infrastructure, and its administrative model has grown more complex. Organizations now have many people working in AD: managing users, groups and their properties; managing application-related data; managing security; and so on. Therefore, organizations need to better protect and compartmentalize data in AD by adopting a role-based approach to its management. In addition, with more hands in the pie, many companies need to reconsider their AD structure — how organizational

units (OUs) are arranged and secured. Original AD designs may no longer be relevant, leading to the need to clean up and restructure existing deployments.

The changing role of AD

AD's role in most organizations started out very humbly, providing centralized login and security to Windows desktop users, or as an alternative to or replacement for Windows NT® 4 Security Account Manager (SAM)-based or Novell® NetWare® systems. Today, AD has become the hub for much of what goes on in the IT organization, as shown in Figure 2, providing functionality such as the following:

- Authentication and authorization for non-Windows systems such as Linux® servers and Mac® desktop and laptops
- Authentication and authorization to a variety of application platforms, such as Microsoft SharePoint® websites, Java-based application servers, network attached storage (NAS) devices and administrative tools such as HP Integrated Lights-Out (iLO) out-of-band management connections
- Authorization, through AD security groups, to large amounts of corporate data, including sensitive data
- "White pages" for corporate directory and organizational charts
- Authentication for public-cloud-based software-as-a-service (SaaS) applications

These relatively new uses for AD put increasing strain on its management, security and availability — and require much more attention to your infrastructure and its related pieces than the previous "set it and forget it" mentality that many IT departments used when managing AD.

In fact, for many organizations, AD has become a tier 1 piece of infrastructure, with five-9s of availability demanded, and its security and management at the level of the most critical business platforms in use. In particular, as organizations migrate to a hybrid approach to providing IT services — with some applications residing in company data centers and others with public cloud-providers — the glue that holds these two environments together is often the identity integration that occurs through AD to authenticate and provide access to these disparate platforms. Without a well-managed and secure AD, this glue quickly dries up, and the hybrid model becomes a hindrance to business, rather than an enabler.

Unfortunately, there is sometimes a gap between that critical role AD now plays and the attention it gets from IT. This gap comes in many forms, from a basic lack of governance around AD changes, to an assumption that it "just works" and

AD has become the hub for much of what goes on in the IT organization.

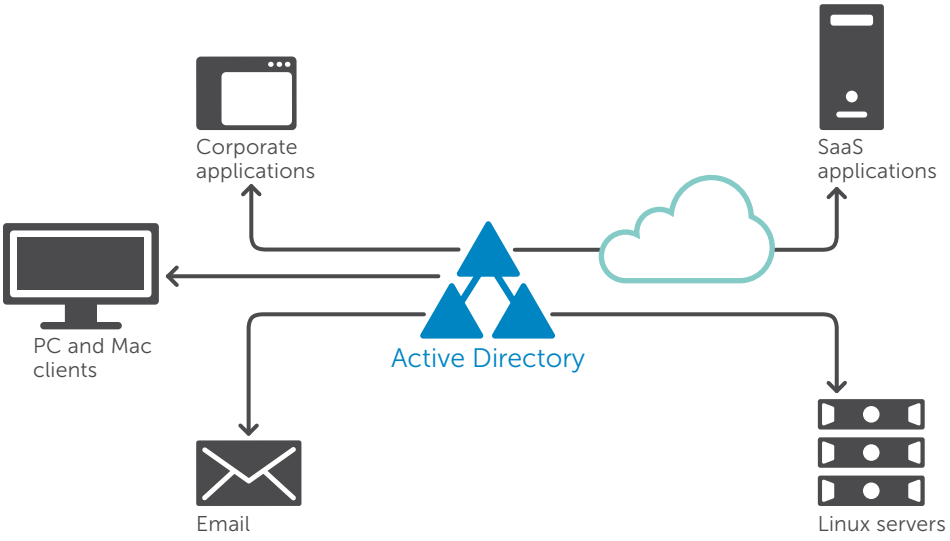

Figure 2. AD has become central to many IT resources.

doesn't require the same care as other enterprise platforms. This assumption does not serve IT departments well as identity in general, and cloud identity in particular, plays an increasingly critical role in the organization.

The shifting regulatory landscape

It would be an understatement to say that the regulatory challenges faced by IT have changed in the years since AD was first released. Today, organizations face a long list of complex regulations — including the Sarbanes-Oxley Act (SOX), the Health Insurance Portability and Accountability Act (HIPAA) and the Payment Card Industry Data Security Standard (PCI DSS) — and AD is often central to compliance. Whether it's the control and attestation of AD security groups that control access to regulatory-related corporate data, or the process by which privileged access is granted to administrators on sensitive systems, the need to control and report on how AD is used has grown by leaps and bounds.

> Achieving, maintaining and proving regulatory compliance requires adopting more sophisticated processes for managing AD and auditing AD-related activity.

Achieving, maintaining and proving regulatory compliance requires adopting more sophisticated processes for managing AD and auditing AD-related activity. It's no longer acceptable not to know who made a given change to it or why the change was made. That kind of ignorance of AD-related activity can have startling implications for not only regulatory reporting, but also the granting of unwanted access to large amounts of corporate data. Because AD has become the hub for authenticating and authorizing access to almost everything within the organization, allowing changes without tight controls, especially to sensitive accounts and groups, is tantamount to negligence in protecting your most sensitive data. Ensuring both regulatory compliance and security requires a modern, well-managed deployment.

Key steps in modernizing your AD deployment

What do we mean when we talk about AD modernization? The term sounds like something we might do to a building — renovating the plumbing or electrical wiring to bring it up to code. And in many ways, that is what modernization is about. Many organizations have had AD in place for a long time, and their legacy structures and practices need to be updated to accommodate the changes and technology landscapes discussed previously.

Here are some of the top areas where modernization can occur, along with the benefits that each area provides:

- Restructuring AD
- Optimizing management and administration
- Securing AD and its data
- Achieving, maintaining and proving compliance
- Ensuring AD availability and recovery
- Implementing AD governance

Restructuring AD

Restructuring of AD has grown increasingly common. Whether you are moving away from older practices (such as empty root domains) or cleaning up domains that resulted from mergers or acquisitions, restructuring your AD environment is a good way to remake the directory to meet your current and future requirements.

In fact, something as simple as shifting OU structures can make a big difference in how you manage and secure AD. Historically, OU structures were aligned to business structures such as company departments or geographic location, or even to delegation models, and other requirements often drove OU design in a direction that didn't necessarily meet other needs of the directory. For example, it may serve Group Policy's

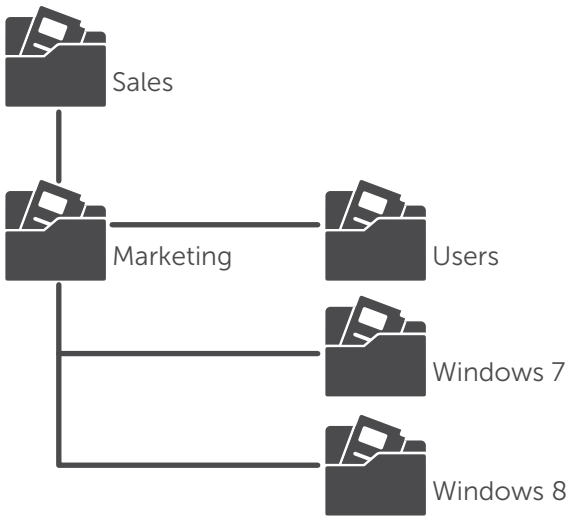

Figure 3. An OU structure optimized for Group Policy rather than delegation

needs well to break out desktop PCs into OUs by OS version, as shown in Figure 3, but if all desktops are managed by a single IT group, that deployment choice makes delegation and administration more complex.

As a result, today's AD designs seek to find a middle ground between these competing needs, as well as the requirements of directory-enabled applications that rely on it to provide authentication and authorization. Taking into account the various needs of your organization is a key part of designing a modern AD structure.

AD restructuring itself can take several forms. Sometimes you must collapse multiple domains and forests into fewer domains to improve manageability and security, or to consolidate after a merger or acquisition. However, in some cases you may decide that for security reasons, you need to break out some resources into a separate forest (a "DMZ forest" for customer-facing resources is a common scenario here). Sometimes you want to start fresh and build an entirely new AD environment, clearing out all the deadwood in the process. Suchrestructuring can be very disruptive, since it can require downtime as you transition users and resources between the old and new environments.

Regardless of the type of restructuring you need, look for third-party tools that help make the change seamless and reduce the impact on your business. This is especially true if you are moving from a poorly documented, poorly managed AD to a more structured one, since you may not be able to predict the impact of the change otherwise.

Optimizing management and administration

Another area of modernization for AD is in the management and administration of the directory. Often, the first step is to reduce the number of administrators with unlimited rights over all of AD. The goal is to achieve a least-privilege model for the its management and administration — where administrators have only the rights they need to modify the parts of AD they are responsible for, which can include:

- **The infrastructure around AD**: These are the servers and services that keep it running, such as domain controllers (DCs), Domain Name System (DNS) and the AD schema.
- **The data within AD**: This can encompass everything from properties on user accounts to key groups that users belong to.

These two areas have different delegation models: Whereas the security model for who can manage the infrastructure elements of AD is not

Taking into account the various needs of your organization is a key part of designing a modern AD structure.

Managing AD delegation requires creating a role-based framework for granting access to AD objects and their attributes.

terribly granular, the security model for the data within it is excessively granular. Therefore, it's important to put controls in place around both the management of AD servers and related infrastructure, as well as Create, Read, Update and Delete (CRUD) operations on the AD data itself.

Given that membership in AD groups can grant everything from server administrative access to accessing HR or financial data, you should be looking at ways to tightly control access to those groups and periodically attest to correct group membership. There are third-party products on the market that can put a proxy in front of all AD management operations to ensure that business rules are followed for changes made to AD.

Securing AD and its data

Another area of AD modernization to consider is delegation — controlling who can make changes to AD objects and their properties. This is closely related to the previous discussion of controlling changes to AD, since only users who are authorized to make changes to AD objects should be able to do so. Too often, oranizations will over-grant access to AD objects in order to solve an immediate problem, and those permissions are rarely cleaned up.

Managing AD delegation requires creating a role-based framework for granting access to AD objects and their attributes. Whether you're controlling who can make changes to the HR Users group or who can change the Managed by property on a given user, delegation is a key part of securing AD, and it must be managed in a coherent fashion, given the native complexity of the security model. Currently, AD creates a role-based template for each task that administrators need to perform against AD, or at the very least, creates role templates for critical tasks, such as changing privileged group memberships or modifying user attributes that control business processes (for example, the department or Managed By attributes). Again, a proxy-based approach can help simplify delegation complexity by forcing all changes to use a proxy account and then granting control to that account on a role-based basis.

Achieving, maintaining and proving compliance

Once you've put controls in place for managing what gets into AD, you must continuously monitor which activities are being performed against it. This auditing need has both internal requirements (for the IT department) and external ones (for the auditors and compliance officers). And while Microsoft Windows Server® and AD natively have the ability to audit events performed against them, these native auditing events can be very verbose, can roll over quickly in busy environments and can be meaningless if taken individually at face value.

Having a coherent AD audit aggregation and analysis capability is a must for spotting inappropriate changes to AD, detecting unauthorized use of AD and corporate resources, and tracking user activity throughout your IT systems. AD auditing provides a change history for all things both within and related to AD — for instance, user logons to desktops and applications are often logged by its servers.

Just as you have change-control processes within the rest of your IT environment, it's also important to put change controls around critical AD -related tasks — including both infrastructure and data changes that could affect the integrity of the directory. Using change controls and auditing as the feedback mechanism for both authorized and unauthorized changes, you can have a good picture of the data changes flowing into your AD deployment. The latest version provides this visibility, so you always know that the right people have access to the right resources using AD.

Recovery type	Description	Impact
Object-level recovery	Typically involves rolling back changes to attributes or deletions of AD objects	Depending upon the type of object, the impact could be minor or it could be significant, such as in the case of the deletion or modification of a security group.
DC recovery	Needed when a DC becomes corrupt or unavailable	Depending upon the situation, restoring a DC could be as simple as promoting a new DC or recovering an existing one from backup.
Domain- or forest-wide recovery	Needed in the rare cases when AD becomes unavailable across a domain or forest	The impact can be substantial, usually including a long outage, since recovery involves systematically restoring DCs from backup in a precise order.

Table 1. The types of AD recovery

Ensuring AD availability and recovery

Another aspect of the modern deployment is high availability. The good news is that AD has proven to be a fundamentally robust and scalable piece of infrastructure, if all the surrounding pieces of it are working well. These pieces include the following:

- AD server replication and replication topology
- DNS
- Microsoft File Replication Service
- Hardware and virtual machine resources

Most, if not all, of these pieces can be monitored using standard or AD–specific monitoring tools. Although AD-specific monitoring is an afterthought for many organizations, it is critical, especially as AD's role in the organization becomes more important. For this reason, it is recommended that AD service monitoring become standard. Service monitoring can include performing synthetic transactions of typical AD operations, such as authentication and searches, to ensure that, even though AD servers are responding to ping tests, the services running on it are also healthy.

In addition to availability monitoring, it's also important to have a good backup and disaster recovery plan. With today's sophisticated third-party backup and recovery tools, including their object-level recovery features, there's no excuse to not be able to recover from everything from minor, inadvertent AD changes to major corruption issues (which are extremely infrequent). There are three levels of recovery to consider related to AD, as shown in Table 1.

Since more organizations are using virtualization technology to run their AD infrastructure, the ability to quickly and easily recover from AD outages is becoming more common, and domain-wide or forest-wide outages are very rare. Still, it's important to plan for the worst case, given the potential impact to your business if AD were to become unavailable. All organizations should have a plan in place, along with tools or processes for recovering from a forest-wide outage with a minimum of downtime.

Implementing AD governance

Once you've done the work to modernize your AD infrastructure, it makes sense to put proper governance in place to ensure it stays that way going forward. There should be well-described rules for how it is used, extended and managed. Another recommendation is to create an AD review board composed of key constituents who support and rely on AD to ensure best practices around AD are codified and supported.

Your AD governance should include the following elements:

- Best practices for the kinds of data that should be stored in AD

Once you've done the work to modernize your AD infrastructure, it makes sense to put proper governance in place to ensure it stays that way going forward.

- Guidelines for when to extend the AD schema, how it should be extended, and when existing attributes can and should be used to store application-related data
- How delegation should be performed in AD
- Guidelines for using security groups to authorize against resources — for example, whether to use nested groups, since some third-party applications can't resolve them
- Standard tools, application programming interfaces (APIs) and ports that are supported for operating against AD
- Best practices for querying AD (for a list, see "Creating More Efficient Microsoft Active Directory-Enabled Applications")

These recommendations are just the tip of the iceberg. The AD infrastructure should be tightly governed, with well-documented standards of behavior.

Conclusion

AD's role in the identity landscape has evolved over time, and Active Directory has become more critical for many organizations. Whether you're providing authentication and authorization to Windows desktops, Linux servers or Java applications, AD needs to be tightly managed, highly available, well performing, secure and audited.

AD modernization is the process by which you transform your deployment to meet these demands. The latest versions of Windows Server can help, but you may also need to turn to third-party solutions to get your AD deployment to the point where it meets its mission-critical job requirements. In all cases, having good governance around AD and a good security and management model will go a long way toward ensuring that AD is always there when you need it.

About the author

Darren Mar-Elia is a Microsoft MVP and president and CTO of SDM Software. He has more than 30 years of experience in IT and software development, including serving as CTO for Windows management solutions at Quest Software (now a part of Dell Software).

Darren has written or contributed to many books on Windows management and is a contributing editor for Windows IT Pro magazine. He also created the popular GPOGuy.com website for Group Policy and is a frequent speaker at conferences on Windows infrastructure topics.

For More Information

About Dell Software

Dell Software helps customers unlock greater potential through the power of technology—delivering scalable, affordable and simple-to-use solutions that simplify IT and mitigate risk. The Dell Software portfolio addresses five key areas of customer needs: data center and cloud management, information management, mobile workforce management, security and data protection. This software, when combined with Dell hardware and services, drives unmatched efficiency and productivity to accelerate business results. www.dellsoftware.com.

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

Dell Software
5 Polaris Way
Aliso Viejo, CA 92656
www.dellsoftware.com
Refer to our Web site for regional and international office information.