Realtime
publishers

Protecting Critical Data by Managing the Active Directory Identity Lifecycle

Darren Mar-Elia

sponsored by

NetIQ™

Introduction to Realtime Publishers

by Don Jones, Series Editor

For several years now, Realtime has produced dozens and dozens of high-quality books that just happen to be delivered in electronic format—at no cost to you, the reader. We've made this unique publishing model work through the generous support and cooperation of our sponsors, who agree to bear each book's production expenses for the benefit of our readers.

Although we've always offered our publications to you for free, don't think for a moment that quality is anything less than our top priority. My job is to make sure that our books are as good as—and in most cases better than—any printed book that would cost you $40 or more. Our electronic publishing model offers several advantages over printed books: You receive chapters literally as fast as our authors produce them (hence the "realtime" aspect of our model), and we can update chapters to reflect the latest changes in technology.

I want to point out that our books are by no means paid advertisements or white papers. We're an independent publishing company, and an important aspect of my job is to make sure that our authors are free to voice their expertise and opinions without reservation or restriction. We maintain complete editorial control of our publications, and I'm proud that we've produced so many quality books over the past years.

I want to extend an invitation to visit us at http://nexus.realtimepublishers.com, especially if you've received this publication from a friend or colleague. We have a wide variety of additional books on a range of topics, and you're sure to find something that's of interest to you—and it won't cost you a thing. We hope you'll continue to come to Realtime for your educational needs far into the future.

Until then, enjoy.

Don Jones

Introduction to Realtime Publishers i

Chapter 1: Active Directory—An Important Part of Identity & Access Control 1

Active Directory's Role in Identity 1

AD in Hetergeneous Identity Environments 3

AD's Increasing Role 5

The Technologies of AD 6

Principles for Secure Management of AD 10

Provisioning 11

Updating 11

De-Provisioning 11

Auditing 12

Least Privilege Access and AD 12

Auditing and Compliance 15

Summary 16

Copyright Statement

Chapter 1: Active Directory—An Important Part of Identity & Access Control

Microsoft's Active Directory (AD) product had humble beginnings. When it first came on the scene in 2000, Novell Netware was the dominant directory service on the market, and was certainly the most popular directory service to leverage the industry-standard Lightweight Directory Access Protocol (LDAP). Fortunately for AD, after a number of missteps on Novell's part, combined with Microsoft's dominant Windows operating system (OS) position in the market, AD has become one of the most popular commercial LDAP-capable directory services on the market today. It's hard to find any IT shop that has a collection of Windows systems that is not running AD in some form or fashion. As a result, AD has become a key component of many organizations' identity management systems.

Active Directory's Role in Identity

But what does that mean exactly? If you run AD on your network, you already know that you're using it to allow your users to log into their Windows desktops or provide seamless access into Exchange, SQL Server, or any number of other Windows-based server products. In addition, when a user browses to a secure internal Web site from their AD-joined Windows desktop, and the user employs Internet Explorer to access an IIS/ASP.Net Web site that usually requires authentication, and the user is put seamlessly through to the site, that is AD single-sign-on authentication and authorization in action. Microsoft's own products are built to seamlessly and quietly pass along your AD credentials to all Microsoft products that require it.

But that is not what has made AD a center of attention for identity in many organizations. What has really helped AD move into the mainstream of identity management is the adoption and support of AD as an important identity store by third-party vendors that provide products that need to support some kind of authentication and authorization. Products as widely varied as Oracle databases, IBM Websphere Java Application Servers, UNIX, Linux, and Macintosh OSs as well as line-of-business applications from companies like Oracle/Siebel and SAP all provide built-in ways to leverage AD for authentication and authorization to those platforms and applications (see Figure 1.1).

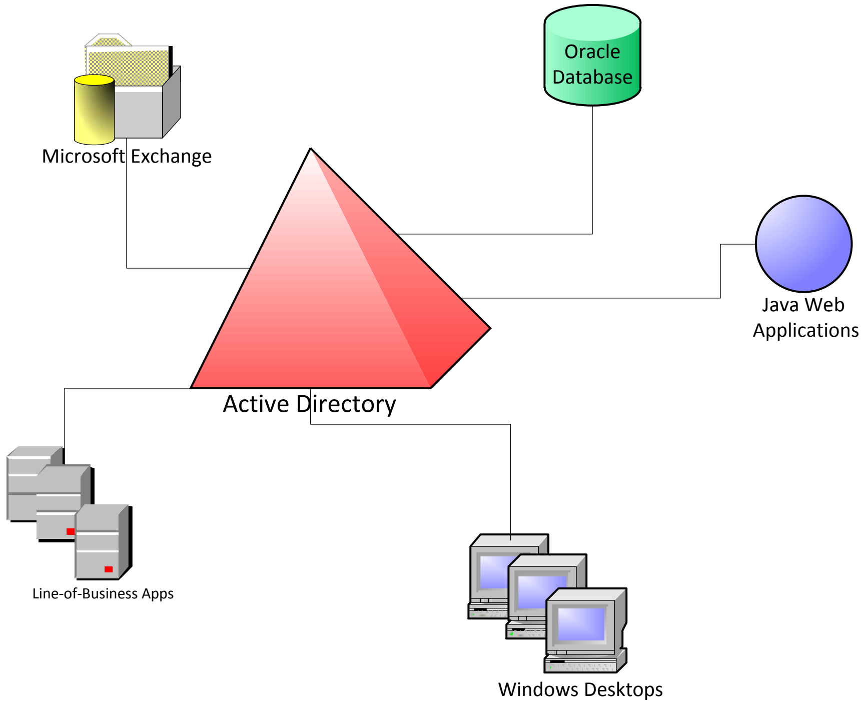


Figure 1.1: AD is used by a variety of platforms and applications today.

All this means that increasingly AD is used as a key repository for identifying users and controlling access to critical corporate data, key intellectual property, and critical business functions. But before we dive into this idea, it's a good idea to set context by talking about two terms that heretofore I've glossed over—namely authentication and authorization:

- **Authentication** is the process by which users identify themselves to a system and prove they are who they say they are. Typically this is done by providing a user name and password to AD, which then authenticates the user by ensuring that their password is correct. Kerberos is the default authentication protocol in AD. However, there are other types of authentication (for example, NT LanMan—NTLM) that can occur, including authentication based on public-key certificates, such as those used in smart cards.
- **Authorization** is about determining whether an authenticated user has the rights required to view and access a resource. That resource could be anything from a file share on a server to a database or a business application running on a Java Application Server. Regardless of the resource, authorization is the process of determining whether the user who is authenticated to AD has been granted access to the resource. In AD, authorization is usually controlled using AD security groups, but could also use other mechanisms, such as "roles," which correspond to the user's business function. This mechanism can include a capability referred to as role-based access control. RBAC encompasses more than just AD security groups but can form part of a strategy for granting access to resources based on a person's job function.

AD in Hetergeneous Identity Environments

With this context around authentication and authorization, let's look a bit more at AD's role in "identity management," which is a term that describes the practice of managing the various identities that we each have at a given organization. The word "identity" also deserves some clarification. It is typically used to represent a "person" or an "actor" within an organization. Any person or actor that needs to identify themselves to an IT system or be authorized to access IT systems can be said to be an identity.

Regardless of whether you are a large multi-national corporation managing dozens of identities for a given employee, or a small business with a single user ID that grants access to all your company resources, identity management, and the task of ensuring that the right people have the right access to the right resources, is critical. AD often plays a key role in that management, but in larger organizations, it is usually not the only player. In fact, AD is often one of several identity stores that a typical large organization might have, and its importance in the overall identity management picture within that organization will vary based on a variety of factors. Many large organizations usually have some kind of Human Resources (HR) application that is often the starting place for any new identities that enter an organization (or the place where existing identities are removed when they are no longer part of the organization, as in when an employee leaves a firm). In addition to an HR system, which can be considered an identity store of sorts, even if it's only a database-drive application rather than a true directory service, many organizations have other directory services that provide identity services. Some examples of these include:

- **"White pages"** are applications that a provide a user lookup directory to internal employees. These applications are usually Web-based systems that are driven by some back-end directory, which could be AD but most often is a product from another vendor.
- **Meta-directories and virtual directories** are different forms of what I call consolidated directory views. That is, many organizations that have multiple identity stores often implement products such as meta-directories and virtual directories that help to join and normalize the data across all of these identity stores. Meta-directories (products such as Microsoft's Forefront Identity Manager—FIM) synchronize data between multiple identity stores such that all directories have the same data about a given person but each directory joined by the meta-directory may be "authoritative" for its own set of data. That is, if you have an HR system that originates new employees and assigns them a unique employee ID, and an AD that assigns that user a login ID to their Windows desktop, you can say that the HR system is authoritative for the employee ID but that AD is authoritative for the login ID. A meta-directory might then replicate the employee ID from the HR system to AD and potentially also the login ID from AD to the HR system. The meta-directory's job is to keep all of its child directories in sync such that there is always a unified view of identity data (or as near as is required) across all directories. Figure 1.2 gives a pictorial example of this relationship.

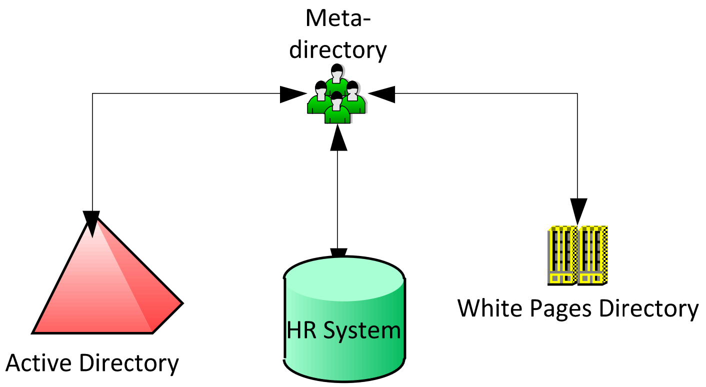


Figure 1.2: Viewing the relationship between a meta-directory and other identity sources.

Virtual directories are slightly different than meta-directories. Instead of replicating directory data to all of the child directories, the virtual directory acts as a master pointer to the various authoritative directories underneath it. If an application needs identity data, it talks to the virtual directory, which refers the request to the underlying authoritative directory source. The application never knows that it's talking to the child directory and has a single view of all directory data. The choice of whether to implement a virtual directory or meta-directory is often driven by business requirements. The bottom line is that many large organizations have one or the other (or sometimes both!) in place.

- **Systems and application-based directories** are directories or identity stores that are associated with a specific application or OS platform. For example, Linux and UNIX systems, in the absence of any other directory technology, store user IDs (and groups) locally on each system in a file-based system. Oracle databases not only hold application data but also user IDs for the people who can use that particular database. And many line-of-business applications keep their own user IDs (usually in a database) that control who can access that application (and what they can access).

All of these so-called standalone identity sources play a role in the overall identity management challenges that large organizations face. The more identity sources that are in an organization, the more places you need to put controls to ensure that the right users are provisioned to access the resources they need. The complexity of having to manage many identity sources can result in holes within your identity management strategy that can impact your ability to control and audit access to critical corporate data.

We'll talk about this theme more throughout the book, but this challenge is one of the reasons AD has gained in prominence over the years. As many organizations seek to reduce the overall number of identity sources they have, consolidating those standalone identity stores into AD has become more popular. As a result, AD takes on more and more critical roles with respect to controlling access to corporate resources and data, and your job as an AD administrator becomes more critical and more subject to scrutiny by parts of the organization that were never very concerned when AD's main job was simply to control access to Windows desktops. This book is about helping you cope with those new challenges and ensuring that you're doing all the right things to keep AD a well-managed, tightly controlled source of access to your organization's precious data.

AD's Increasing Role

The main purpose of this book is to help you manage the life cycle of identity management as it relates to AD, and to help ensure that AD, as an increasingly critical point of control for sensitive corporate resources, is managed in a way that is commensurate with its responsibilities. What are some of those responsibilities in a typical corporate environment today? Let's walk through some examples:

- **Authentication and Authorization for Windows Desktops and Windows Resources—**AD has been doing this task since its inception, and it's especially good at it. You use AD to log into your Windows domain desktop and to access file shares, your Exchange email inbox, Windows servers on your network, IIS Web sites, and all manner of other AD resources. And because the Windows desktop is the users' main portal to much of their corporate data, protecting who can access the desktop is probably one of the most critical tasks you can take on. Once a user gets into a Windows desktop, they have seamless single-sign-on access to any resources that they're authorized to in the Windows world.
- **Authentication and Authorization for Linux and UNIX Servers—**This role is relatively new but increasingly commonplace for AD. More organizations are leveraging third-party and built-in products for integrating their non-Windows systems into AD, such that an AD user account can now log into a Linux server and their access to that Linux server can be controlled through AD group membership just as with Windows. This integration typically leverages the fact that AD uses industry standards for authentication (Kerberos) and directory service access (LDAP) which are platform agnostic.
- **Authentication and Authorization for Non-Microsoft Database Platforms—**Database vendors such as Oracle and MySQL provide various way to integrate into AD such that, instead of maintaining user accounts local to the database, many IT shops are now moving database authentication to AD. With this setup, the same user account that you use to log into AD can now be used to log into those databases.

- **Authentication and Authorization for Line-of-Business Applications—**All manner of third-party business applications today generally support AD for authentication as well as for authorization. Everything from the most complex financials package to employee timesheet applications support AD credentials for single-sign-on.
- **Federated Access to External Partners—**Identity federation is a term that describes sharing identity information between your own organization's identity stores and an external partner. The sharing is done using industry-standard protocols such as Security Assertion Markup Language (SAML) and usually involves granting access from your users to a third-party Web site or service without requiring your users to keep a separate logon at that third-party site. AD supports federation through the Active Directory Federation Services (ADFS) product—a Microsoft solution—and through third-party federation products. Identity federation is becoming more popular and just adds to the list of things that your AD users might be accessing on a daily basis.

This list just scratches the surface of areas where AD is becoming an important identity repository. All of this concentration of identity into AD brings obvious benefits as we start to talk about identity life cycle management. Namely, having fewer identity stores means having fewer places to provision and de-provision user accounts when a new user joins or leaves the company. It also brings additional challenges. It means that your company now relies on AD more than ever for critical business functions—meaning that AD must be highly available and highly secure 24×7×365. In addition, the practices you put in place around provisioning, managing, reporting, and auditing your users in AD must be rock-solid because those AD users now have access to a large percentage of your corporate resources, including everything from sensitive HR and business performance data to potentially non-public customer data. More than ever, managing AD is about managing access to your company's very lifeblood! To that end, let's dive into a little more detail about the technologies associated with AD that can and will have a role in your management and automation of that platform.

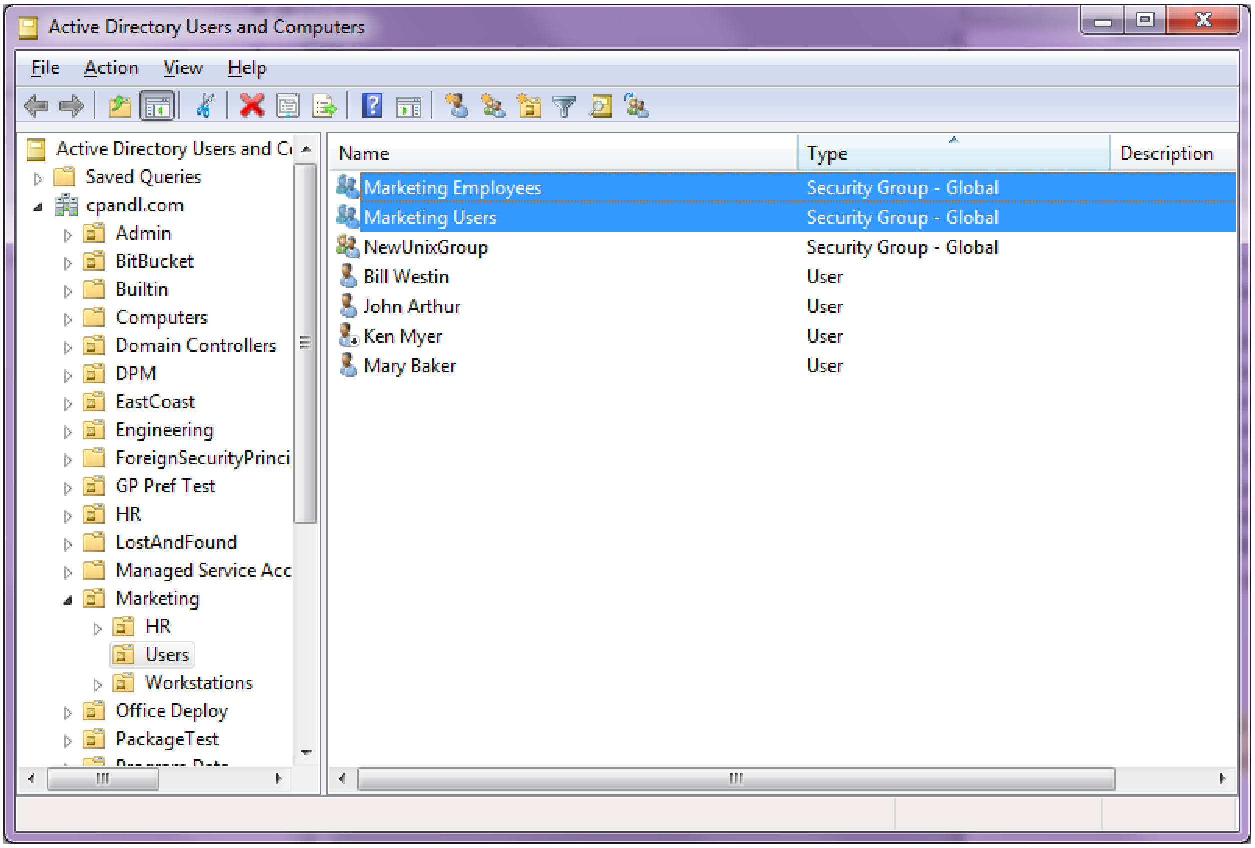
The Technologies of AD

As I mentioned earlier in the chapter, AD heavily leverages the LDAP protocol as the standard way that people can interact with it. LDAP is a platform-agnostic protocol that many popular directory servers use today, and thus AD can be accessed by any platform or application that supports LDAP clients. Note that Microsoft also includes its own proprietary interfaces in AD, including the Active Directory Services Interface (ADSI), which provides similar services to LDAP as well as Microsoft-specific ones that provide access to features that are specific to AD. LDAP lets you authenticate to, search, and modify AD data.

Working side-by-side with LDAP is the Microsoft implementation in AD of the Kerberos authentication protocol. Kerberos is yet another industry-standard protocol for providing secure authentication to systems and applications. Microsoft implements a compatible version of Kerberos that allows authentication interoperability with other platforms, such as Linux and UNIX (in fact, most if not all of the third-party integration products I mentioned earlier for Linux and UNIX leverage open source Kerberos clients to provide AD integration). Kerberos has the responsibility, in AD, of authenticating the user to AD (proving they are who they say they are) and figuring out what groups the user is a member of. This information is then passed along to the various resources the user wants to access to determine whether the user truly does have access (that is, they are a member of the right groups for that resource).

AD also supports alternative forms of authentication, including the legacy Microsoft NTLM authentication protocol and Public-key (X.509) certificates. The former is typically used as a fallback authentication mechanism when a particular service can't support Kerberos authentication; NTLM is generally viewed as less secure than Kerberos. The latter (X.509) is typically used as an interoperability protocol where a Kerberos client is not easily supported but a public-key infrastructure (PKI) is already in place. Smart cards are a good example of technology that leverages PKI to perform AD authentication on behalf of a user.

Another technology, or rather an approach, that is interesting for our discussion of AD life cycle management is a concept I mentioned earlier—mapping business functions to access to resources. This kind of business function or role mapping attempts to manage the authorization part of the equation using the concept of roles. A role is an abstraction that could be represented by, for example, an AD security group (see Figure 1.3), but applications can also have the notion of roles built into them (this is common is database products such as Oracle and SQL Server). Roles usually correspond to a user's role in the organization—either their business or technical role. The goal is to try to organize all of your users' job functions, as they relate to their access to corporate IT resources, into a set of permissions and accesses to a set of resources. Once those roles are defined, you can use them to grant access to those resources.



Name	Type	Description
Marketing Employees	Security Group - Global	
Marketing Users	Security Group - Global	
NewUnixGroup	Security Group - Global	
Bill Westin	User	
John Arthur	User	
Ken Myer	User	
Mary Baker	User	

Figure 1.3: Viewing AD security groups.

Security groups grant access to resources (Windows or otherwise). The idea with RBAC systems is that a given role is associated with an access set that is commensurate with that role. As a user changes jobs (into or out of a given role), their access is automatically changed. Implementing RBAC can be tricky as role-propagation (that is, creating too many or too granular roles to meet all the different access requirements of a given user or job function) can become a challenge, but if well implemented, can also give you excellent control over access to your corporate resources.

One other technology that we should discuss is one that I mentioned briefly earlier—identity federation. Federation is becoming increasingly popular as public "cloud" services become more prevalent in IT environments. Identity federation provides a means by which you can "share" your identity data with a third-party provider in a secure way that does not compromise your identities. One example of federation is as follows: When you federate with a partner—let's say a third-party Web site that handles your organization's vacation tracking system—you are sending your user identity from your corporate directory—they are trusting that the claims you make are good enough to get access to their system and they use that claim to pass you through to that Web application, as Figure 1.4 shows.

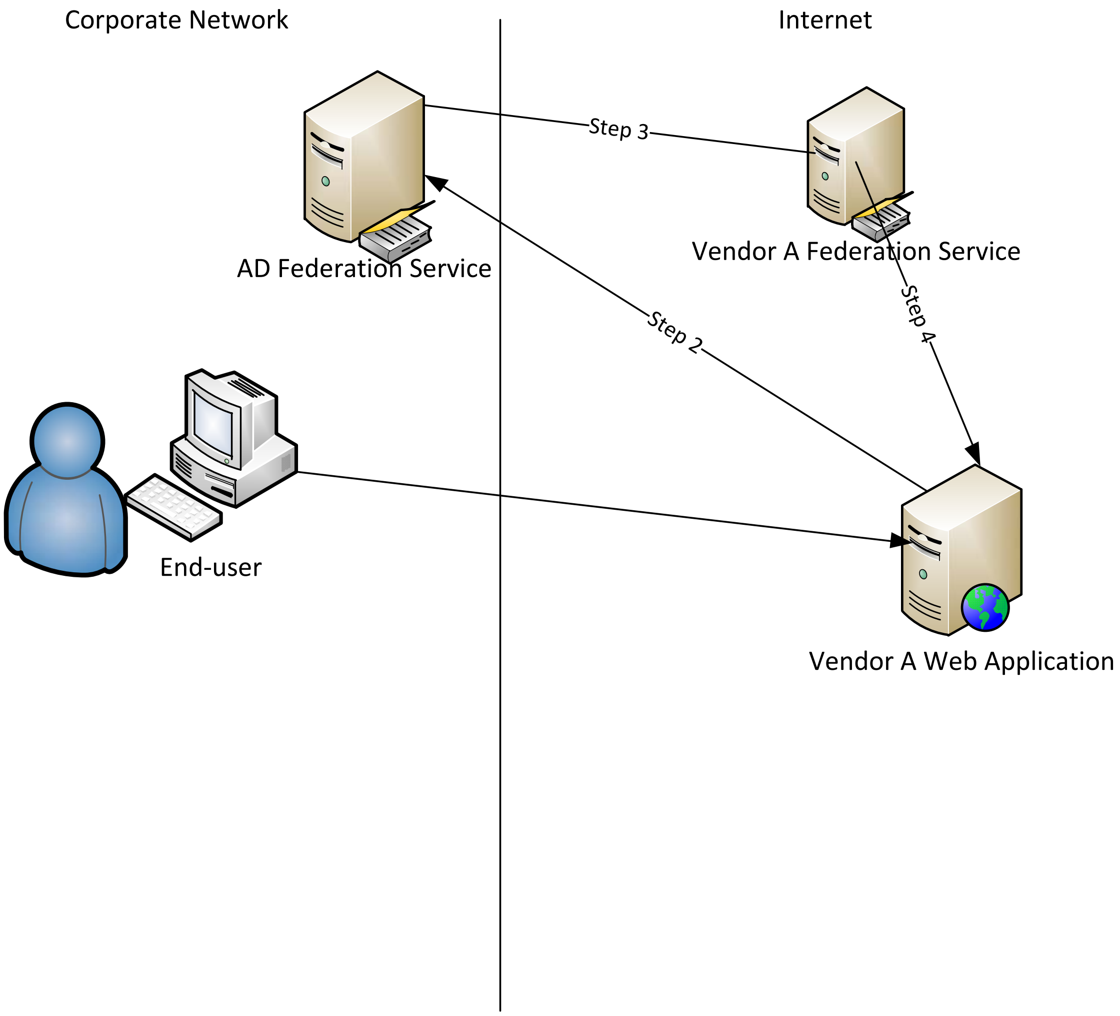


Figure 1.4: Viewing a simple identity federation relationship.

In Figure 1.4, we see a simple federation relationship where a user browses to a public Web site (Step 1) that has a pre-established identity federation relationship with their company. The vendor (referred to as Vendor A) has provided a custom URL for the user that automatically redirects the user back to their own federation service, which validates the user (Step 2) and passes the claim for the user back to the vendor's federation server (Step 3). The claim is then presented to the Web application in a form that it expects (Step 4), and the users is authenticated to the Web application without having to present credentials or maintain a user account at the vendor's site. With the advent of public cloud services, we can expect that this type of identity federation with AD will become more popular, and we'll need ways of ensuring that we can manage this access as we would access to internal resources.

And speaking of managing access, let's shift gears once again and dive into the main topics that we'll be covering for the rest of this book—namely that of managing the life cycle of AD identity in a way that minimizes or eliminates risk to your business and your corporate data!

Principles for Secure Management of AD

This book is about acknowledging AD's role as an important part of many organization's identity management infrastructures and helping you do the right things when it comes to ensuring that the data in AD, and thus the access to your company's sensitive data and resources, is well-managed, secure, and auditable. Because at the end of the day—and this is a key point—managing access to your corporate resources is closely related to how well you manage the data that goes into AD: the users and groups that control authentication and authorization on your corporate network. To that end, there are a number of things that can help you ensure that users and their access are managed in a way that is consistent with your security and compliance goals. The first is to implement identity life cycle management. The diagram in Figure 1.5 shows the key parts of this life cycle.

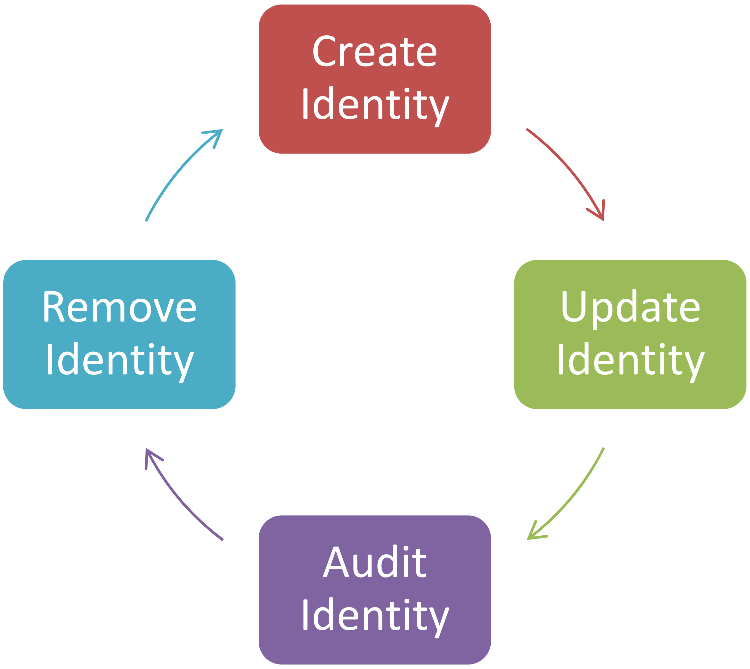


Figure 1.5: The keys parts of the identity life cycle.

As you can see in Figure 1.5, a proper identity life cycle is concerned not only with creating new identities but also how those identities are updated over their lifetime and, perhaps more importantly, how they are audited and ultimately removed. Creation and removal of identities is typically referred to as *provisioning* and *de-provisioning*.

Provisioning

Provisioning is the place most people start when working to automate their identity management. Many larger organizations typically originate new identities in an HR system, so it's pretty common that the HR system will be the first place the new employee or contractor lives and that information is pushed into AD in an automated fashion using either a meta-directory or other database/directory synchronization tool.

This setup is desirable because the creation of new identities in AD happens fast and automatically. If the system is well-designed, the person's business role or function will flow with them into AD and they will be automatically placed in the correct OU in AD and joined to the right groups that grant them access to the resources they need to do their job. What you want to avoid is having every user within the same role look different when they are created in AD, as can often happen when there is no automated process for identity creation. Automation forces discipline over role definitions and ensures that you are thinking about all of the pieces within AD that must be touched to get someone up and running within the organization, with all the access they need to do their job.

That is not to say that there can't still be some approval-based workflow in the mix, where a manager gets to approve adding a new user to a security group that provides access to sensitive data. But even that process can be automated to the point that when the manager gives their approval, the provisioning process continues on its way without any manual intervention.

Updating

Updating of identities is an ongoing process throughout the lifetime of the user within the organization. Users will move physically, change job functions, and get promoted. Each event comes with associated impacts to what the user needs access to and where they need that access, and each of those requirements often has impacts to how that user's data is managed in AD. A user who moves locations to a different office may need to be put in different security groups that are relevant to file share access in that new office. A user whose job changes may need to be removed from groups that their new role no longer requires access to. And a user who is promoted may need new access to sensitive data that their old role did not require. Again, automation of these changes can streamline the process and ensure the correct access is always maintained. Again, the use of some kind of roles for defining a particular job function can come in handy, as a role can define that list of AD security groups that the user should be a member of in order to do their job.

De-Provisioning

De-provisioning, while seemingly less important than creation of accounts (at least as far as users are concerned), is perhaps one of the most important parts of the identity life cycle process you can get a handle on because there is nothing that auditors hate more than user accounts that no longer belong to an employee, that are lying around active—still having access to corporate resources. It's important to ensure that when an employee or contractor leaves the organization, **ALL** of their user accounts and access to resources are removed. This step is critical to ensuring that only valid users can access your data.

Auditing

Auditing what you have in AD to ensure that it continues to be the right people having the right access to the right resources is also a key part of managing your identity infrastructure. This step provides the vital feedback loop to ensure that the processes you have in place for provisioning and updating are working and that no users are being provisioned to the wrong groups or being given access to data that the owners of that data do not approve of. This last piece—ensuring that the owners of data agree that the people who access that data are still valid users—is called **attestation** and is a key part of the identity auditing process. We'll talk more about auditing and compliance later in this chapter and in subsequent chapters; it's an important part of ensuring that critical corporate data does not "leak" through poor management of AD and an important part of meeting your regulatory compliance requirements.

> **Note**
>
> We'll go into more detail around how you can implement this identity life cycle within your enterprise—including AD and its role as an important player in identity management—in Chapter 2.

Least Privilege Access and AD

Another practice that helps you ensure that your corporate assets are protected is the implementation of a least privileges access scheme within your AD infrastructure. I define least privilege as a practice where you grant identities the least amount of privileges required to perform their job function. For example, if you have an AD user that works on a Help desk and whose sole job is to reset the passwords of users who call in, then you would not grant that AD user to be a member of the "Domain Admins" group to do their job—you would only grant them rights sufficient on AD user objects to perform the reset password operation.

The notion of "least privilege" has become more and more common in IT as a result of the various malware exploits that leverage the bad practice of IT shops granting users administrative access to their Windows desktops. Doing so lets the user—and any malware that they download—have free rein to their systems and consequently the corporate network. Thus, there is a strong move afoot to reduce privileged access on all IT systems to only that which is required to do the job at hand and only during periods of time when the job is being done. This practice of least privilege extends equally as well to AD, albeit with different considerations.

Least privilege within the context of AD involves two main aspects: least privilege access controls to the data held within AD and using AD and its capabilities around authorization to ensure users have the least privilege necessary. Least privilege access controls to the data held within AD involves managing the security delegation available in AD to ensure that data held within AD is protected on a "need to access" basis (as illustrated in the earlier example of the Help desk user). This translates into building a delegation model within AD that secures objects and their attributes within AD (e.g., users and their properties, groups, and their members) such that only those users who need to access that data—for reads or writes—have that access.

AD has very granular security options, which we'll dive into more in Chapter 3. Having good controls in place to ensure that delegation is applied consistently to all objects, throughout their life cycle (when they're created and moved around) is a key aspect of least privilege for AD. In the best case scenario, I can only read and access those AD objects that I need to do my job—regardless of what that job is. That includes both "regular" users as well as IT administrators—the latter of whom have the most opportunity to create risks within the organization by virtue of their normal elevated privileges.

To put this in more concrete terms, least privilege for AD starts with not having more members of the Domain Admins group than you need to reasonably support AD—and perhaps none that spend their whole days with that privilege. That's a simple example but one that underscores the goal of least privilege for AD.

The second aspect of least privilege is that of using AD and its capabilities around authorization, to ensure that users have the least privileges necessary to access the resources that they need within their organization. How is this different than the first point? In the first idea, what I'm describing is controlling who can access the data held within AD. In this second point, what I'm referring to is using AD to correctly place users into the groups that provide the users least-privilege access to resources. This translates into users being put in the correct groups to ensure that the users only have access to the resources that they need to do their jobs. Figure 1.6 illustrates this concept.

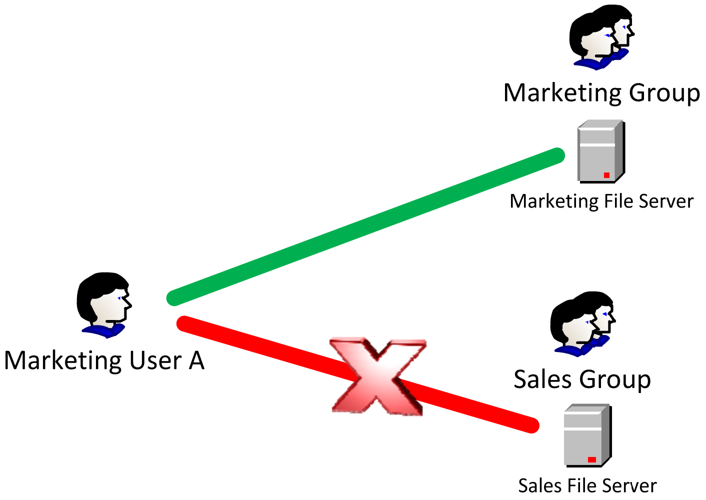


Figure 1.6: Using AD groups to control access to resources.

In the example in Figure 1.6, Marketing User A is a member of the "Marketing Group" and AD security group. This security group is used to permission resources on the Marketing File Server. Because the Marketing User is in this Marketing Group, the user can access the files. But if the user tries to access files on the Sales File Server, she is rejected because that server is permissioned using the "Sales Group." This simple example articulates the value of least privilege. Instead of leaving AD and Windows in their default states, which tend to grant users in AD the ability to at least read many types of resources that are part of the domain, we take on the job of re-permissioning those users and resources that we care about protecting so that the groups the users are a member of grant them access only to those resources that they need access to do their job.

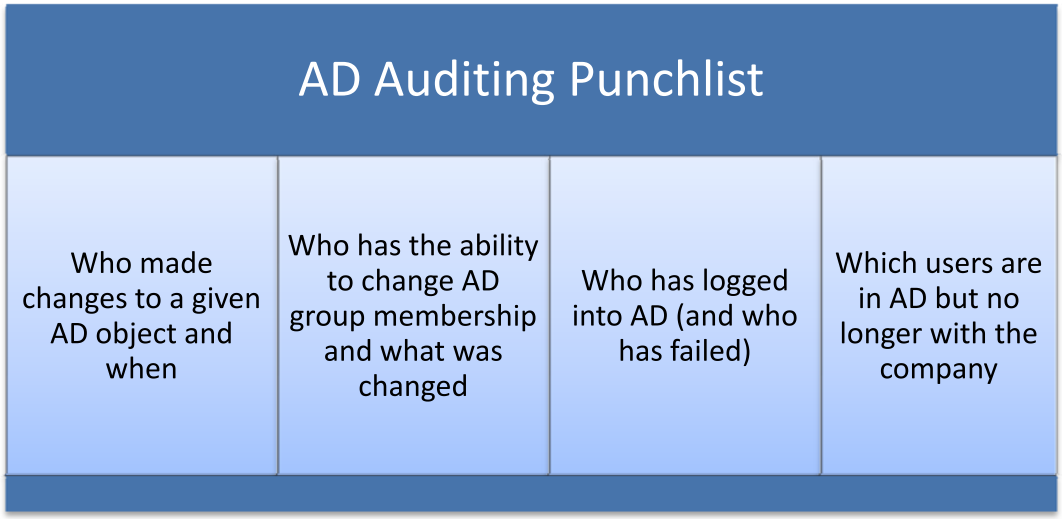
It is true that many types of resources require at least read permissions on them in order to allow the user to function properly, but this should not be assumed to be a universal rule—especially as it relates to critical user data. Correct permissioning not only simplifies users' lives but also reduces the chance of critical corporate data leaks via users who should not have had access to begin with.

On the IT administrator side, least privilege means only having the ability to access and change those servers and applications that are within your job responsibility. If you are the print administrator, you may only be able to stop and start the Windows spooler service on a very restricted set of servers that serve the printing function. Your group membership will not allow you to also reboot the company Web servers just by virtue of being an administrator. This last point is critical to ensuring that your systems stay available and secure, though it is not a mode of operation that most IT administrators are used to. Indeed, many IT administrators live with administrative rights over all systems and like it that way. However, as time goes on and issues such as inadvertent changes causing outages and loss of key company data through both innocent and malicious access become more prevalent, most organizations cannot afford to give all administrators free reign over their systems.

In addition, from a compliance and audit perspective, many IT auditors are now looking for IT shops to show that they have controls in place to know when an IT administrator exercise their privileged access and what they were doing with it. This is where AD can play a key role, by using role-based access and security groups to ensure that only those IT administrators with a valid need can access a given set of servers—and only when they need that access. That brings us to the final aspect of our discussion around managing AD securely—auditing and compliance!

Auditing and Compliance

In this day and age, many of us work at organizations that are subject to regulatory compliance requirements. Whether it is Sarbanes-Oxley (SOX), Payment Card Industry (PCI), the Health Insurance Portability and Accountability Act (HIPAA), or another industry-specific regulation, none of us in IT are immune. AD (and its proper management) plays a key role in this area. Because AD is often a single point of control for many of the areas that we've already talked about, such as provisioning and de-provisioning and role-based access control, auditors go to AD to find out who is doing what and who has access to which resources within an organization. Indeed, as companies consolidate more system and application access in AD, it's become even more critical to have good auditing in place. Figure 1.7 highlights some of the key areas that you need to think about related to AD auditing.



AD Auditing Punchlist

Who made changes to a given AD object and when	Who has the ability to change AD group membership and what was changed	Who has logged into AD (and who has failed)	Which users are in AD but no longer with the company

Figure 1.7: Common items that auditors find of interest in AD.

This table is a sampling of the kinds of thing you'll need to be aware of when you create a plan for auditing changes that are happening within your AD.

> **Note**
>
> Chapter 4 will go into more detail around auditing.

The key here is to think about the kinds of things that AD will be doing within your organization—authenticating and authorizing users to key corporate data and applications. In addition, think about what you would want to know to ensure that no one is abusing that system or that everyone who has access should have access (and that it's the right access).

That is the same kind of information that auditors are interested in, which is why every aspect of your AD life cycle management plan should think about how to audit and show compliance with regulatory rules as they relate to AD. That is why most auditors ask you to show the 5 Ws—Who, What, Where, When, Why as the information relates to access and use of your IT systems. If you can answer those 5 Ws as they relate to AD—its management and usage—you'll go a long way towards ensuring that you can meet your auditor's needs. However, given the complexities of many of the regulations companies are subject to, it's important to understand your organization's audit requirements prior to designing your auditing controls.

Summary

This chapter laid out the groundwork for building a well-managed identity system that has AD as a key component. Whether AD is your only directory or one of several within your organization, it often has a key role to play in terms of being a main source of identity and access control (authentication and authorization). To that end, managing the identity life cycle of create, update, remove, and audit will ensure that the right people have access to the right data. Along the way, provisioning users and resources using the principle of least privilege will help ensure that access to systems and data is truly protected. In addition, the right auditing in place will ensure that any regulatory requirements that come upon you will be met without gaps in key information. For the rest of this book, we will flesh out each of these areas in much greater detail, providing real-world guidance for building out your AD infrastructure as a secure, world-class identity system.