Are You Spending More than You Realize on Active Directory Management?

Curbing Costs with Unified AD Management

Written By Jeffery D. Hicks, Principal Consultant, JDH Information Technology Solutions, Inc.

Abstract

Active Directory is critical to your IT infrastructure, enabling users to log on, access network resources, and much more. But managing Active Directory may be costing you more than you realize if you're relying on native tools and PowerShell scripts. This white paper identifies the six key types of tasks that are essential to Active Directory management, estimates the costs a company incurs each year in each category, and explores how investing in the right tools can make managing AD not only easier but actually more cost-effective.

Introduction

Active Directory is everywhere

Active Directory (AD) is without a doubt one of the most critical elements of your IT infrastructure. So much of daily corporate life is centered on a functioning and efficient Active Directory, from allowing users to log on in the morning, to enabling them to send email and access network resources. When it works, everyone is happy. But when it doesn't, it is very apparent: users can't log on, desktop settings are incorrect, files can't be accessed, delegated admins can't manage their user accounts, and more.

Overview: The six key AD management areas

Accordingly, IT professionals and their management invest a great deal of time and resources into properly managing and maintaining Active Directory. Typically, these tasks fall into one of these critical categories:

- Account management
- Security management
- Auditing and change control
- Group Policy
- Backup and recovery
- Active Directory health

The challenge is finding the most economical and operationally efficient way to tackle each of these tasks. As we'll see, there is a real operational cost to each of these areas. It takes time and

Key Active Directory management tasks are often handled by different teams who have their own tool sets.

money to set up a new user. A botched Group Policy costs a company time and money – not only in recovering a backup GPO or reconfiguring it, but also in lost productivity for the affected end users. In addition, these tasks are often handled by different teams who have their own tool sets, including native tools, such as the Microsoft management consoles; home-grown solutions such as Windows PowerShell scripts; and specialized solutions from independent software vendors. In that case, the organization may be investing more than necessary to fulfill its AD management needs.

About this document

In this paper, we examine what it takes to be both economically and operationally efficient in each of these key areas. It doesn't really matter if the same group of administrators handles all of these tasks or if the workload is distributed. IT professionals and their management need to keep the "big picture" in mind when it comes to feeding and caring for the Active Directory beast.

For this paper, we consider a hypothetical manufacturing company with 500 users and a comparable number of computers spread across two sites, with a few domain controllers in each site. Granted, a company this size would have a few IT administrators, but we're going to analyze what it takes for a single admin with an annual salary of $52,000 to manage all of this.

The six key AD management areas—and their true costs

Account management

There's no question that the core functionality for Active Directory is creating and managing users, computers, and groups. New employees are hired, people are promoted, and some are terminated. All of these events require some interaction with Active Directory. Using the native Active Directory Users and Computers (ADUC) is definitely not efficient. Performing common tasks using ADUC is very time-consuming. For example, it can take up to 10 minutes to create a new user account and put the user in the right groups. It can take even longer if you need to maintain an audit trail, which we'll cover later.

Similarly, a large amount of time is devoted to account changes. Employees get married or divorced and require name changes. People are hired and might need new titles. They move to new offices and need new phone numbers. Depending on your organizational structure, a promotion might also necessitate a move of the user and/or computer object to a new organizational unit (OU), as well as a change to group memberships. All of these changes take time to accomplish manually, are prone to human error, and are expensive.

Using a home-grown tool like a Windows PowerShell script can cut down on some of this time. But even assuming the staff has the time and expertise to develop such a solution, there is still an investment in learning PowerShell, maintaining the script, and training new IT hires. I know from experience that creating a single production-quality PowerShell tool can take 8-16 hours. For our fictitious IT professional, that is an investment of over $400 beyond the time it takes to acquire the necessary experience or expertise. And if the company considers bringing in an outside "expert," the cost will likely be 10 times higher.

For a typical month, our IT professional is most likely going to spend at least 30 hours a month on these basic tasks. Table 1 illustrates a typical month for our 500-user company.

The bottom line is that it is costing the company about $730 a month for basic and essential management – that's over $8,700 a year! A company can't cut back on these tasks so the only thing that can be done is to find ways to be more operationally efficient, which leads

	Per month	Minutes per activity	Total time	Cost
New user/ month	25	10	250	$104.17
User charges/ month	125	10	1250	$520.83
Terminations/ month	20	5	100	$41.67
Group management	15	10	150	$62.50
				Total: $729.17

Table 1. Typical monthly account management expenses.

directly to an economic benefit. For example, if a new user account can be created in one minute rather than 10 minutes, that is a direct savings of $1,125 a year for this single task. When you aggregate savings across this entire set of account management tasks you begin to see some real benefits—and account management is just one of the six types of AD management tasks.

Security management

The second key type of AD management task is security, and one security-related task that incurs significant operation expense is dealing with user passwords. In most organizations, a majority of help desk calls are password-related. Resetting a password or unlocking an account using ADUC takes time – at least five minutes, and more if reporting or auditing is required. Let's make the conservative assumptions that in our sample company, just 15 percent of employees need password help, and handling one event takes an average of five minutes. That amounts to 6.25 hours per month of IT time—an expense of almost $1,900 a year.

Another security-related Active Directory task is delegating control of an organizational unit to another user or group. Delegation can be for the entire OU or for specific types of objects in an OU, such as printers. Delegation can get very granular, for example delegating who can reset user passwords for accounts in an OU. Although delegation is not necessarily a frequent task, it is time-consuming to complete in ADUC, easily taking 10 minutes each time.

If our IT admin spends even 30 minutes a month on delegation, the company is looking at up to $300 a year in direct expenses.

More important, ADUC offers no way to comprehensively show what has been delegated and to whom. To supplement ADUC, therefore, some organizations rely on home-grown PowerShell scripts or command-line tools, which take time to write, or they invest in a management tool, which is typically licensed on a per-user basis.

If you've been keeping score, just account management and security-related Active Directory management tasks alone are costing the company almost $11,000 a year and about one week a month. On one hand it might be argued that this is what the IT administrator is getting paid for. And while that is true to a degree, I think it is short-sighted. If the IT administrator is hampered by inefficient tools and practices, not only is there a direct economic cost, but there is also a cost for things that didn't get done because the administrator was busy figuring out things like who has permissions to change user passwords. If these AD

> Performing common tasks using Active Directory Users and Computers is very time-consuming, with a large amount of time being devoted to account changes.

Group Policy, when done right, can be an asset to a company and save real dollars on the bottom line.

management tasks can be completed more efficiently, the IT pro will have the opportunity to work on other tasks that benefit the company or to develop new skills, and everyone comes out ahead.

Auditing and change control

For many organizations, auditing and some form of change control are critical if not downright mandatory. Can you tell who created a given user account? Who modified a group membership, and when? Frankly, when it comes to Active Directory auditing and change control, there are no native Microsoft tools. Many administrators resort to third-party tools to comb through event logs to gather this type of information, which means licensing costs; or they develop PowerShell scripts, which, as we have seen, takes time and training. On top of these costs, using either of these methods to complete a task like tracking down how many accounts were created, modified and deleted in the last month would probably cost the IT admin 8-10 hours of work.

Moreover, once the information is gathered, it almost always needs to be formatted into some type of report. Again, there are no native tools to do this, so we're left with home-grown scripts, perhaps creating a Microsoft Excel spreadsheet, or hoping that the third-party management tool includes a reporting feature.

Of course, auditing is not limited to monitoring user accounts; IT management usually wants reports on a variety of aspects of the current state of Active Directory. In my career as an IT consultant, I've seen organizations use all of the following kinds of reports:

- **Password age reports**
- What passwords are expiring?
- Who has a non-expiring password?
- **Group membership reports**
- What groups are empty and unused?
- What groups does a user belong to?
- Who belongs to the Domain Admins group?
- **Obsolete computer accounts**
- **Obsolete user accounts**
- **Organizational reports**
- Users by department
- Users by OU
- Users by cost center
- OU permissions

For almost all of these, ADUC is of as little value as it is for change control, so again IT pros often resort to scripts and third-party tools, incurring the same development or licensing costs we've already discussed.

In our hypothetical company the IT administrator can easily spend five hours a month on auditing, change control and reporting, which leads to an annual expense of $1,500. Clearly, anything that can cut that time and cost, without sacrificing quality, is something to be considered.

Group policy

The fourth type of Active Directory management task is the care and feeding of Group Policy. Group Policy, when done right, can be an asset to a company and save real dollars on the bottom line. But sadly, even 12+ years since its introduction, many organizations still don't use it. I believe this is directly related to the lack of solid native management tools. The Group Policy Management Console is fine for basic tasks, but it doesn't scale well. Managing a single GPO with the management console – whether you are backing up the GPO or creating a report – is very time-consuming. Microsoft has a set of PowerShell cmdlets that can be used to manage Group Policy, but they aren't intuitive, and they require some PowerShell experience – and they are still limited. For example, comparing two GPOs is a very complex task that requires some sophisticated PowerShell experience.

Our IT admin needs to regularly back up and occasionally restore GPOs. We'll estimate that requires two hours a month on average. Plus, the admin needs to use Group Policy when troubleshooting a help desk problem from time to time, perhaps comparing

GPO versions to identify potential issues. Some of this can be done with the native management console, but such tasks probably add on another 90 minutes a month, for a total of 3.5 hours of GPO-related work. That means managing Group Policy in Active Directory is costing the company over $1,000 a year. In addition, the company is incurring the risk of downtime and lost employee productivity because of Group Policy problems, which also has a direct cost.

Backup and recovery

The second-to-last AD management task is backup and recovery. Because Active Directory is mission-critical, it requires periodic backup to protect against everything from major problems to human errors—it is very easy to accidentally delete an OU and all of the user accounts.

Unfortunately, backing up Active Directory with native tools is not as easy as it could be. It would be nice if there was an option in ADUC to say "back me up," but there isn't. There are command-line tools, but they are complicated. Even with scripted solutions, Active Directory backups are time-consuming.

Restoring from a backup natively is even worse. Not that long ago, and this might still apply to you depending on your Active Directory version, recovering a deleted item from Active Directory required a slew of steps. You had to reboot a domain controller in AD restore mode. Track down the restore mode password. Track down the backup files. Restore the backup. Use a complicated command-line tool to configure the restore. Reboot and hope for the best. Even if you needed to restore only a single deleted user account, this process could easily take an hour or two. Eventually, Microsoft provided the Active Directory Recycle Bin, which made this process a little shorter, but not necessarily any easier. There is no graphical interface, so using this feature requires Windows PowerShell. You also need to know exactly what it is you need to recover.

The alternative, again, is to invest in an Active Directory backup solution. The downside is that there is yet another licensing cost as well as another new tool for the IT staff to learn.

What does this mean for our beleaguered IT administrator? I would estimate that between backing up Active Directory, periodically testing a restore, and occasionally restoring an object, an IT admin spends four hours a month, which ends up costing the company $1,200 a year. This is definitely an area where the right tool can lead to greater efficiency and ultimately lower costs.

Active Directory health

The final Active Directory management task is keeping tabs on overall health. Are domain controllers running properly? Is replication working as expected? Is name resolution functioning? Are all operation masters roles online? These are just some of the questions our IT administrator must answer nearly every day. Unfortunately, getting those answers requires using several different native tools, none of which has decent reporting features. There are a few command-line tools, but these require some expertise to use properly. Writing a PowerShell script for most of these tasks is an option for only the most experienced scripter. Alternatively, there are third-party tools that can handle some or all of these tasks. But beware of licensing costs. I prefer to translate costs into a per-user basis, even if the product is licensed per domain controller or administrator, assuming I have a reasonable ratio of users to domain controllers and admins.

In our manufacturing company, the IT administrator easily spends eight hours a month monitoring Active Directory, plus a few hours more troubleshooting problems. All told, this is costing the company $3,000 a year because he has to rely on native tools and a few

Unfortunately, backing up Active Directory with native tools is not as easy as it could be. Restoring from a backup natively is even worse.

PowerShell scripts he grabbed from the Internet that he doesn't totally understand.

Choosing the right tools

Native tools

With only manual tools to use, our exhausted fictitious administrator is working 50 to 60 hours a month struggling to manage Active Directory and keep users happy. Let's total the costs of using manual tools for Active Directory management:

By my calculations, AD management using native tools is costing our company, which has only 500 user accounts, almost $26,000 a year, just in administrator time. Of course, the real costs are actually much higher, since, as we have seen, the inefficient tools cause lost productivity for end users. Plus, this is 50-60 hours that the IT admin can't be spending on other projects.

AD management task	Annual cost
Account management	$8,700
Security management	$11,000
Auditing and change control	$1,500
Group Policy management	$1,000
Backup and recovery	$1,200
Active Directory health	$3,000
Total	$26,400

Table 2. Annual costs of AD management using native tools.

Home-grown tools

One quick fix that many companies try to use is to develop home-grown and ad-hoc solutions. In many of today's Microsoft shops this means turning to Windows PowerShell. Now, don't get me wrong: PowerShell is a terrific management tool and can fill in many management gaps. But the effort involved in building full PowerShell solutions is daunting and requires substantial experience, making it a viable option only for the largest of organizations. Even then, developing and maintaining the scripts incurs costs in training and development time, as well as the time spent using them to complete the AD management tasks.

All-in-one Active Directory management solutions

The best approach is an all-in-one Active Directory management solution that addresses all of the six areas discussed above: account management, security, change control, Group Policy, backup and recovery, and health monitoring.

I realize that not everyone is in a position to manage all of these elements. For example, your company might be small enough that you haven't begun using Group Policy in earnest. Still, you need to plan ahead for the day when you will. The goal should be to provide a single tool for the IT staff to learn and use, especially if you use or plan to use role-based access control (RBAC). That way, everyone learns a common tool that maintains the necessary administrative segregation. When crossover or new access is required, the learning curve is minimal. This helps make IT administrators more efficient out of the gate. Naturally, a single management solution isn't worth the investment if it doesn't improve efficiency and ultimately drive down operational costs. The solution should cut task time to literally minutes.

An all-in-one management solution can also be more cost-effective since you're

The effort involved in building full PowerShell solutions is daunting and requires substantial experience, making it a viable option only for the largest of organizations.

dealing with a single vendor. Typically, the application is integrated so that all of the different areas can share a common infrastructure. This should help keep per-user costs down. The benefits of an all-in-one Active Directory management solution can extend beyond the IT pros who administer it on a daily basis:

- Help desks often turn to Active Directory and Group Policy to troubleshoot a problem. Having ready access to Active Directory-related information cuts down on the time to resolve issues, which keeps management costs down and end users efficient.
- Security and compliance teams often need to turn to Active Directory to accomplish their assigned tasks. Having a comprehensive solution is invaluable for these people because native Windows tools for these areas are poor. Licensing yet another product at additional cost makes no business sense.
- Finally, a solid, all-in-one solution can serve IT management. Native tools for any sort of reporting are sorely lacking, but without adequate and actionable information, management can't make informed business decisions. This is another hidden cost that might be hard to quantify, but nonetheless, is real.

Assessing your needs

The bottom line is that Active Directory management comprises many mission-critical tasks. Trying to accomplish these tasks with native Windows tools is time-consuming and error-prone, and doesn't scale well. That's even assuming there is a native tool to get the job done!

We've explored what the operational expenses are for our hypothetical company, with figures based on real-world experiences. We encourage you to use these examples as a guideline for analyzing your own efficiency and expenses. What management tasks are you doing now and how long does it take? What tasks aren't you doing because of the lack of time or resources? What are the operational costs of using your current management toolset? Whether you are using native tools or third-party solutions, there are back-end expenses such as training, licensing, and additional hardware; be sure to include those as well.

In addition, there is the intangible of overall satisfaction. Are employees and management satisfied with the tools they have? Are they being tasked with work that is beyond the scope of their current tool set? How much time and energy are they expending to overcome these deficiencies? Are your IT professionals happy to take care of the Active Directory beast or do they fear it?

There are many ways to tackle Active Directory management. You need to be sure you are properly take care of it in the most economically and operationally efficient manner.

Active Administrator

Active Administrator from Dell is an extensive Active Directory management solution that enables you to address all six types of Active Directory tasks from one integrated console. Centralizing the management of the most important aspects of Active Directory and Group Policy saves administrators time and gives them the most control over their environment.

Active Administrator is an extensive Active Directory management solution that enables you to address all six types of Active Directory tasks from one integrated console.

About the author

Jeffery Hicks is a Microsoft MVP in Windows PowerShell, a Microsoft Certified Trainer, and an IT veteran with 20 years of experience, much of it spent as an IT consultant specializing in Microsoft server technologies. He works today as an independent author, trainer and consultant.

Jeff writes the popular Prof. PowerShell column for MCPMag.com and is a regular contributor to the Petri IT Knowl-edgebase. Jeff is a regular speaker at conferences such as TechMentor and TechEd, often speaking about PowerShell, Active Directory, Group Policy and anything else than can make IT pros more efficient and productive.

About Dell

Dell Inc. (NASDAQ: DELL) listens to customers and delivers worldwide innovative technology, business solutions and services they trust and value. For more information, visit www.dell.com.

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

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