MANAGING THE ECONOMIC AND OPERATIONAL COSTS OF ACTIVE DIRECTORY

Quest®

Introduction

Active Directory is without a doubt one of the most critical elements of your IT infrastructure. Much of daily corporate life is centered around a functioning and efficient Active Directory infrastructure. From enabling a user to log on in the morning or send email to providing access a network resource like a file share or a SharePoint site, Active Directory is everywhere. 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, administrators can't manage user accounts and more.

Quest

To avoid these headaches, 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 these critical categories:

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

The challenge is to find the most economical and operationally efficient way to tackle these tasks. As we'll see later, there is a real operational cost to each of these areas. It takes time and money to set up a new user. A botched Group Policy costs a company time and money not only in recovering from a backup GPO or reconfiguring it, but also in lost productivity for the affected end users.

In addition, the challenge to this challenge, if you will, is that often, especially in larger organizations, these tasks are handled by different teams often with their own tool sets. These may be native tools like the Microsoft management consoles, home-grown solutions such as Windows PowerShell scripts or legacy batch and VBScript files, or specialized solutions from independent software vendors. However, the downside to the organization as a whole is that it might be investing more time and money than is necessary to fulfill these needs. For example, one third-party solution might require additional back-end services, which means another expense. Another third-party solution might require a complex and expensive licensing scheme. And if an organization utilizes multiple solutions to tackle the critical areas listed above, there is likely to be some overlap, which means paying twice for similar functionality.

We're going to look at these key areas and examine what it takes to be both economically and operationally efficient. It doesn't really matter if the same group of administrators handles these tasks or if the workload is distributed; IT professionals and their respective management need to keep the big picture in mind when it comes to care and feeding of the Active Directory beast.

> No matter which team or teams handle Active Directory management, it's essential to be both economically and operationally efficient.

For this paper, we're going to 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 takes to manage all of this with a single Active Directory administrator with an average annual salary of $87,653 (roughly $42.00 per hour). We'll ignore the additional cost of benefits and overtime.

The cost of critical Active Directory management tasks

ACCOUNT MANAGEMENT

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

Creating a single production-quality PowerShell tool can take an IT pro around 16 hours. How much does that cost your company?

Using a home-grown tool like a Windows PowerShell script can cut down on some of this time. But there is still an investment in learning PowerShell, maintaining the script and training new IT hires. Of course, this assumes the staff has the time and expertise in the first place to develop such a solution. 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 $600 beyond the time it takes to acquire the necessary experience or expertise. And if the company has to bring in an outside expert, the cost will likely be 10 times as much.

In addition to setting up new accounts and removing old ones, admins must devote a large amount of time to account changes. Employees get married or divorced and require name changes. They move to new offices and need new phone numbers. People are promoted and need new titles. Depending on your organizational structure, a promotion might also necessitate moving user or computer objects to a new organizational unit (OU) and changes to group membership. All of these changes take time to accomplish manually, are prone to human error and are expensive.

In 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.

Activity	Number per month	Minutes per activity	Total time (minutes)	Total time (hours)	Total cost
New user	25	10	250	4.17	$175
User change	125	10	1,250	20.83	$875
Termination	20	5	100	1.67	$70
Group management	15	10	150	2.50	$105
Total	185	N/A	1,750	29.17	$1,225

Table 1. Typical monthly account management expenses

The bottom line is that it is costing the company over $1,200 a month (more than $14,000 a year) for basic and essential management! 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 directly to an economic

Even a small company can easily spend $14,000 year on basic user provisioning tasks if they rely on native tools.

Quest

benefit. For example, if a new user account can be created in one minute instead of ten, that is a direct savings of over $1,800 a year for that single task. When you aggregate savings across this entire matrix, you begin to see some real benefit.

SECURITY MANAGEMENT

Of course, there's more to Active Directory management than handling new users and groups. Another common operational expense is dealing with user passwords. In most organizations, one of the main reasons for helpdesk calls is password-related issues. Resetting passwords takes time. Using ADUC (Active Directory Users and Computers management console), it can take at least five minutes to reset a user's password or unlock their account. This time can easily and quickly rise depending on additional reporting or auditing requirements. In our sample company, even if we calculate that just 15% of employees need password help, that amounts to 6.25 hours a month of IT time, assuming a conservative five minutes per event. The result is an expense of over $3,000 a year.

Another security-related Active Directory task is delegation. It is not uncommon in larger organizations to delegate 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, like printers. Some delegation can get very granular — for example, delegating who can reset a user password for accounts in an OU. These delegations are time consuming to accomplish in ADUC and not always intuitive. Granted, this is not necessarily a frequent Active Directory management task but it can easily take ten minutes to complete each time.

Where this gets even more difficult is figuring out what delegations are in place and modifying them. ADUC is a poor choice and offers no way to comprehensively show what has been delegated and to whom. Some IT pros rely on home-grown PowerShell scripts or command-line tools. Other companies invest in yet another management tool, typically licensed on a per-user basis. If our IT admin spends even an hour a month on delegation or permission-related tasks, the company is looking at $500 a year in direct expenses.

If you've been keeping score, basic Active Directory management is costing the company over $17,500 a year. 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 lost cost for things that didn't get done because the administrator was busy figuring out who has permissions to change user passwords. Yes, the IT pro is going to be paid regardless, but if they have the opportunity to work on other tasks or projects that can benefit the company or develop the administrator professionally, then everyone comes out ahead.

But we're only getting started. Even to meet bare management needs, native tools just can't cut it.

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 user account in Active Directory? Who modified a group's 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 or rely on PowerShell scripts to do the same thing. Either way, a company must invest in licensing a third-party auditing tool or invest in administrator time. If our overworked IT professional had to track

down how many accounts were created, modified and deleted in the last month, it would probably take 8–10 hours.

And 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.

In addition to change control, it is not uncommon for IT management to want reports on the current state of Active Directory. In my career as an IT consultant, I've seen organizations create reports on all of the following:

- Which passwords are expiring
- Who has a non-expiring password
- Which groups are empty and unused
- Which groups a user belongs to
- Who belongs to the Domain Admins group
- Obsolete computer accounts
- Obsolete user accounts
- Users by department
- Users by OU
- Users by cost center
- OU permissions

> There are no native Microsoft tools to help you with Active Directory auditing and change control.

For almost all of these reports, ADUC is of limited value, so IT pros often resort to scripts and third-party tools. This often means direct licensing costs as well as the time it takes to learn how to use a new tool for each task. 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 over $2,500. Clearly, anything that can cut down on the time without sacrificing quality is something worth considering.

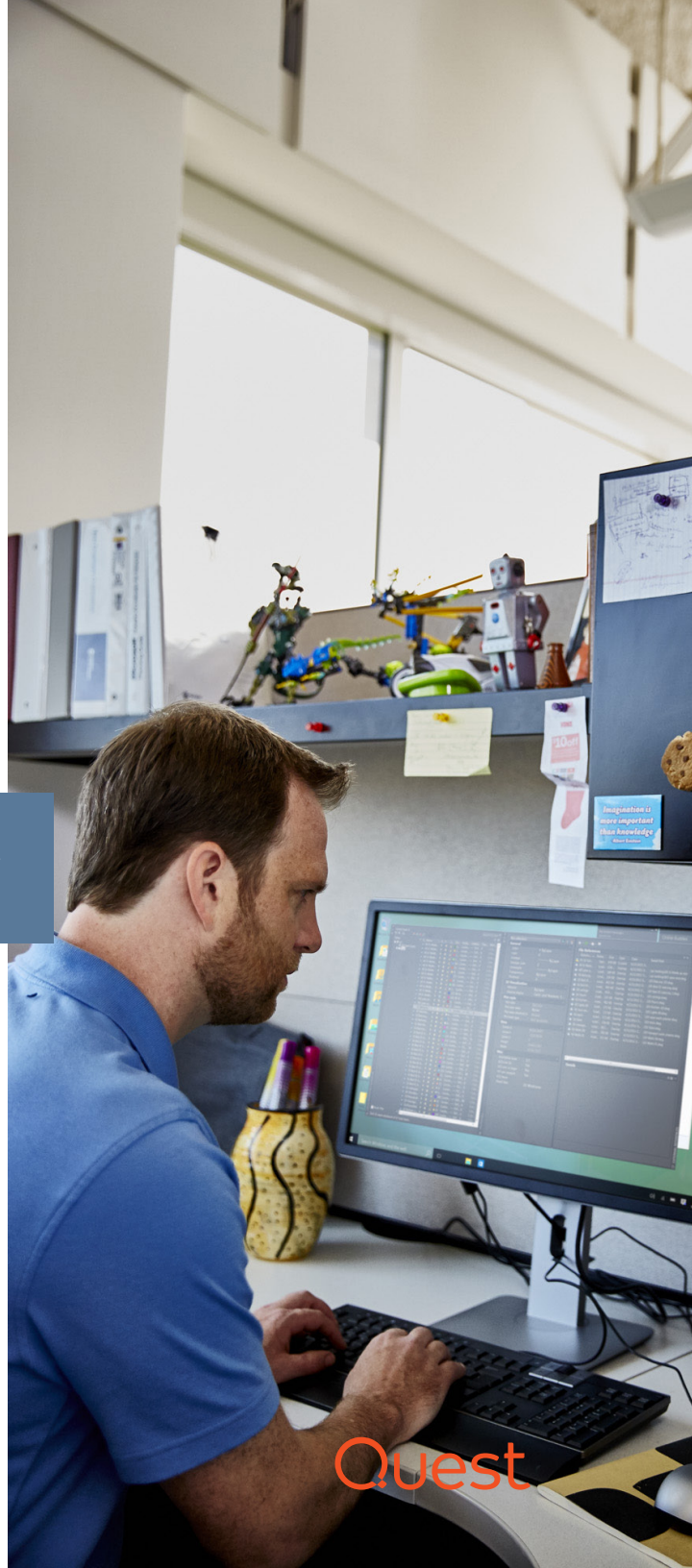
GROUP POLICY MANAGEMENT

Another Active Directory-related task is the care and feeding of Group Policy. Unfortunately, this is another area where native tools are sorely lacking. The Group Policy Management Console is fine for basic tasks, but it doesn't scale well. Managing a single GPO with the management console is very time consuming, whether you need to back it up or create a report. Microsoft has a set of PowerShell cmdlets that can be used to manage Group Policy, but they aren't intuitive, they require some PowerShell experience and they are limited. For example, if you want to compare two GPOs, it is a very complex task that requires some sophisticated PowerShell experience.

Group Policy, when done right, can be an asset to a company and save real dollars on the bottom line. But sadly, even 18+ years since its introduction, there are still many organizations that don't use it, and I believe this is directly related to the lack of solid native management tools and the amount of time it takes. The only alternative is to find a third-party Group Policy tool that meets your needs, and you may end up with more than one.

> The Group Policy Management Console is fine for basic tasks, but it doesn't scale well.

Our IT admin needs to regularly back up and occasionally restore GPOs. We'll estimate he spends two hours a month on average on this, which is an expense of over $1,000 annually. Plus, he needs to use Group Policy when troubleshooting a helpdesk problem from time to time, often comparing GPO versions to identify potential issues. Some of this can be done with the native management console, but it probably takes him about 90 minutes a month in GPO-related work. Suddenly, managing Group Policy in Active Directory is costing the company over $1,700 a year, not to mention the potential downtime to employees because of Group Policy problems, which also has a direct cost.



BACKUP AND RECOVERY

Because Active Directory is mission-critical, it requires periodic backup. Backups are required not only for business continuity but also to protect against accidents and human error. It is very easy to accidentally delete an OU and all of its 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.

And if backup is messy, restoring from a backup 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 was a very time-consuming process. 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 a single deleted user account, this process could easily take an hour or two.

Eventually, Microsoft provided the Active Directory Recycle Bin feature which made this process a little shorter, but not necessarily any easier. Using this feature requires Windows PowerShell, since there is no graphical interface. 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.

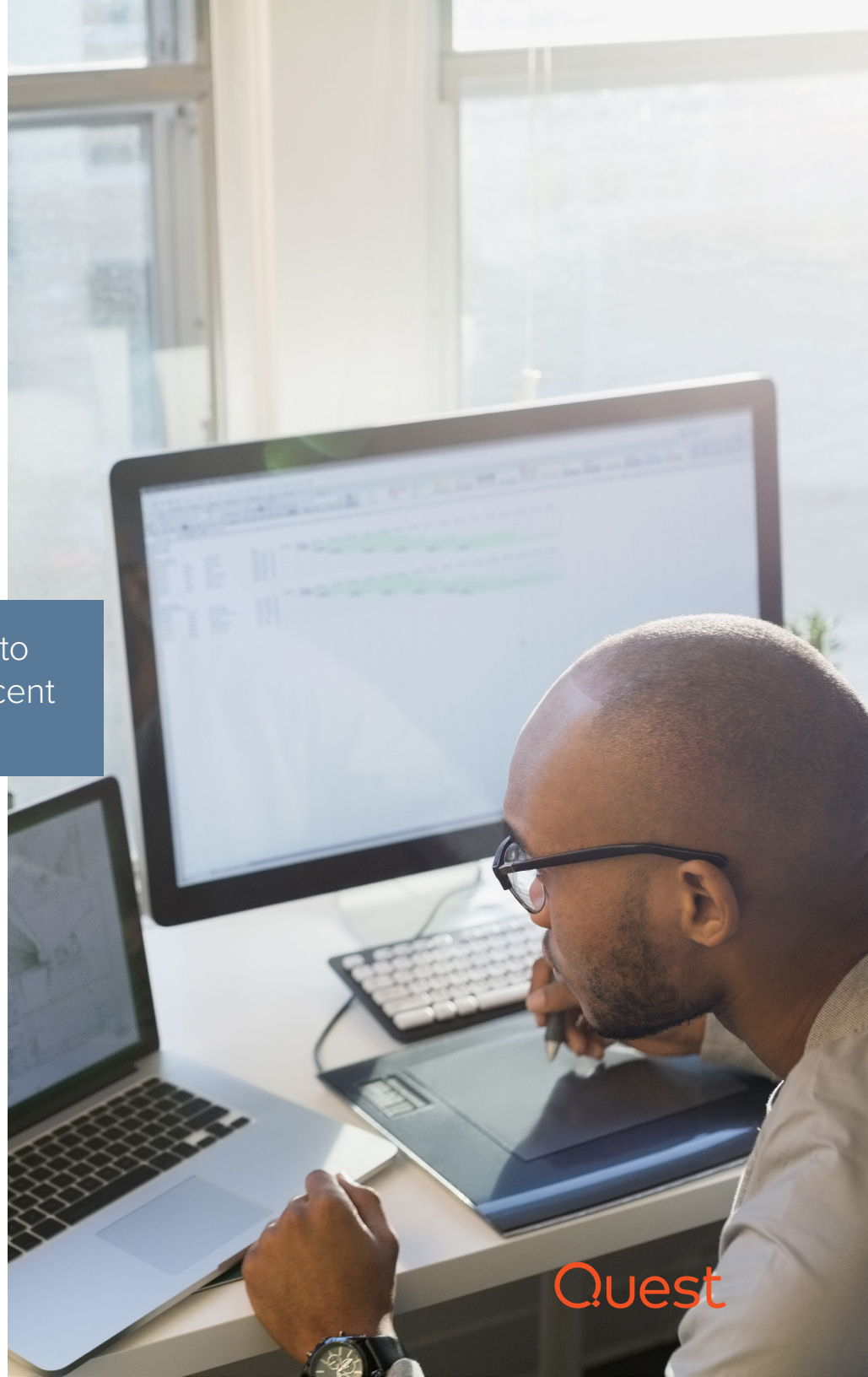
What does this mean for our beleaguered IT administrator? I estimate that between backing up Active Directory, periodically testing a restore and occasionally needing to restore something, he spends four hours a month, which costs the company about $2,000 a year. This is unquestionably an area where the right tool can lead to greater efficiency and ultimately lower costs.

ACTIVE DIRECTORY HEALTH MANAGEMENT

The final typical Active Directory management task is one of the most critical: keeping tabs on overall health. Are domain controllers running properly? Is replication working as expected? Is name resolution functioning? Are all operations master roles online? These are just some of the almost daily tasks our IT administrator must tackle. Unfortunately, when it comes to native tools, he must use several of them, none of which has decent reporting features. There are a few command-line tools, but these require some expertise to use properly, and writing a PowerShell script for most of these tasks is only for the most experienced scripter and administrator.

> To keep tabs on the health of AD, an IT admin has to juggle multiple native tools, none of which has decent reporting capabilities.

As with the other management areas, 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 sample manufacturing company, the IT administrator easily spends eight hours a month monitoring Active Directory, plus a few hours more when troubleshooting a problem. All told, this is costing the company over $4,000 a year because he must rely on native tools and a few PowerShell scripts he grabbed from the internet but that he doesn't totally understand.



Why native tools and point solutions are not a cost-effective approach

At this point, our exhausted fictitious administrator is working 50–60 hours a month struggling to manage Active Directory and keep everyone happy. His efforts from using manual tools are prone to error and time consuming. By my calculations, it is costing the company with 500 user accounts well over $25,500 a year. It would be one thing if inefficiency affected only him, but often someone else — such as an executive or user — is waiting, so the real costs are actually much higher. Plus, this is 50–60 hours of IT time that can't be used elsewhere.

Moreover, I examined only how my hypothetical company manages Active Directory in a handful of areas. Ideally, organizations need to manage all aspects of Active Directory. They need to understand how efficient their current processes are and what the effective cost is. What tasks aren't being done that should because of lack of either human resources or budget? The quick fix that many companies try to make 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, requires substantial experience and is likely only for the largest of organizations. The bottom line is that if you try to manage Active Directory using only native Windows tools, you are expending a great deal of energy, time and resources. These tools were not designed for today's enterprise.

Realizing that native tools just aren't cutting it, the company might decide to invest in dedicated solutions for a few key areas. But there are a few potential pitfalls of this approach. The first is the economic reality of licensing. To keep the math simple, we'll say the tools they purchased have an average cost of $8.00 per user. With 500 users, this means an annual cost of $12,000. This cost can be justified only if it reduces our administrator's workload by 23 hours a month.

> Deploying multiple point solutions is costly, since each one incurs its own licensing fees, installation and maintenance expenses, and training costs.

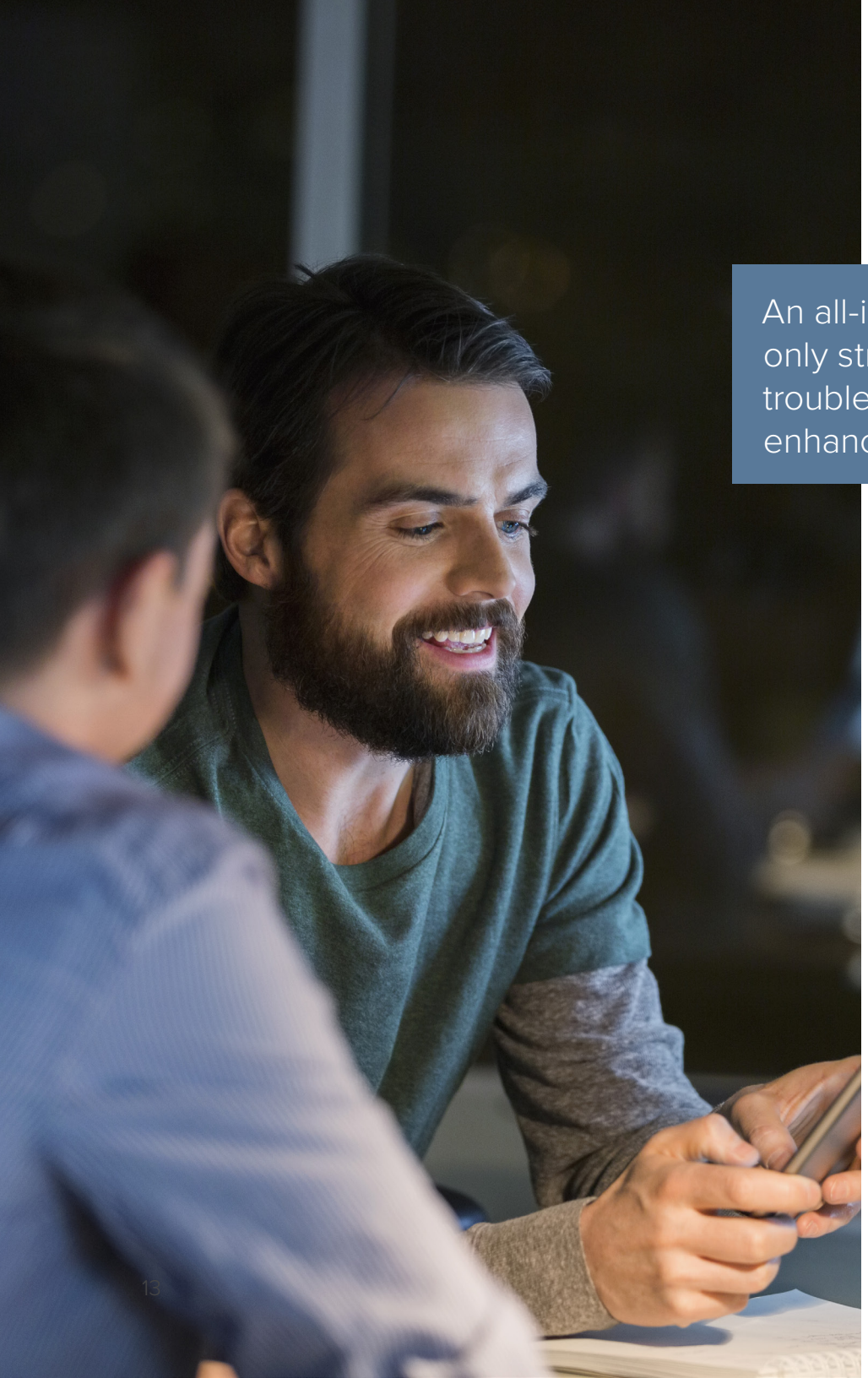
Second, there is the additional cost associated with installing three different tools. Some of the tools might require agents to be installed. Some might require additional back-end expenses like a new web server. Some might need to be installed on the domain controller and others from the administrator's desktop. The point is, multiple tools are going to require multiple resources to deploy and maintain.

Finally, there is the learning curve for three different tools, which must be repeated every time a new administrator is hired. Even though these costs can be hard to quantify, they shouldn't be ignored.

Using an all-in-one Active Directory management solution

So where does that leave our overworked IT professional and his company? The best approach is to invest in an all-in-one Active Directory management tool. This solution should address at least the 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 head for the day when you will. The goal is to provide a single tool for the IT staff to learn, especially if you use or plan on using role-based access control (RBAC). The benefit is that everyone learns a common tool that maintains the necessary administrative segregation, but 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; it should cut task time to literally minutes.

All-in-one management solutions can also be more cost effective since we're dealing with a single installation and configuration — typically, the application is integrated so that all the different areas can share a common infrastructure. This should help keep overall costs down. Where our fictional company was paying over $12,000 in direct licensing costs alone for three point solutions, a single comprehensive management solution might only run $9,000. Of course, such a solution must offer



significant increases in efficiency immediately. In today's agile environments, businesses no longer have the luxury of long-term ROI.

An all-in-one AD management solution will not only streamline AD administration but also speed troubleshooting, improve security and compliance, and enhance decision-making.

An all-in-one Active Directory management solution can extend beyond the IT pros who administer it daily. Helpdesk teams often turn to Active Directory and Group Policy to troubleshoot problems; having ready access to Active Directory-related information will reduce time to repair, which keeps management costs down and end users efficient. Security and compliance teams also 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 or require a lot of ad-hoc development. 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 it is real nonetheless.

Quest

Conclusion

The bottom line is that Active Directory management is an ongoing series of mission-critical tasks. Trying to accomplish these tasks with native Windows tools is time consuming, prone to errors and doesn't scale well. That's even assuming there is a native tool to get the job done! I've demonstrated where the operational expenses are with admittedly hypothetical numbers, albeit ones drawn from real-world experiences. But you should use my examples as a guideline for analyzing your own efficiency and expenses. What management tasks are you doing now and how long do they 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 tool set? Whether you are using native tools or third-party solutions, there are back-end expenses such as training, licensing and additional hardware. Use your own financial data and you will likely be stunned at the expense.

> Take the time to calculate how much you're spending on AD management; you will likely be stunned at the expense.

Last, there is the intangible criterion 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 toolset? 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. Make sure you are properly taking care of it in the most economically and operationally efficient manner.

About the Author

Jeffery Hicks is an IT veteran with almost 30 years of experience, much of it spent as an IT infrastructure consultant specializing in Microsoft server technologies with an emphasis in automation and efficiency. He is a multi-year recipient of the Microsoft MVP Award. He works today as an independent author, teacher and consultant. Jeff has taught and presented on PowerShell and the benefits of automation to IT pros worldwide. He has authored and co-authored several books; writes for numerous online sites; and is a contributing editor at Petri.com, a Pluralsight author, and a frequent speaker at technology conferences and user group meetings. You can keep up with Jeff on Twitter (http://twitter.com/JeffHicks) and on his blog (https://jdhitsolutions.com/blog).

ABOUT QUEST

Quest provides software solutions for the rapidly-changing world of enterprise IT. We help simplify the challenges caused by data explosion, cloud expansion, hybrid datacenters, security threats and regulatory requirements. We're a global provider to 130,000 companies across 100 countries, including 95% of the Fortune 500 and 90% of the Global 1000. Since 1987, we've built a portfolio of solutions which now includes database management, data protection, identity and access management, Microsoft platform management and unified endpoint management. With Quest, organizations spend less time on IT administration and more time on business innovation. For more information, visit www.quest.com.

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

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

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

Ebook-ManagingEconomicCostsAD-US-GM-37551

Quest