IDC
Analyze the Future

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com

WHITE PAPER

Optimizing Infrastructure: The Relationship Between IT Labor Costs and Best Practices for Identity and Access Management with Active Directory

Sponsored by: Microsoft

Al Gillen
Randy Perry
Frederick W. Broussard
Seana Dowling

November 2006

EXECUTIVE SUMMARY

Directory and identity management has emerged as one of the fundamental building blocks used in modern computer architectures. Most modern operating systems now have integral directory services or layered directory services software that is available in conjunction with the operating system. The use of directories has emerged as one of the ways that CIOs address the management of IT costs while improving services to the business and end users.

The integral directory service in Microsoft's Windows product family, Active Directory, serves as the foundation for identity and access management within the Windows environment. Active Directory serves as the primary directory service for client and server domain authentication and is further leveraged for configuration and provisioning and for applying operational group management and configuration policies to client and server systems. In a broader manner, Active Directory also plays a key role in Microsoft's identity and access management strategy, and when used with Microsoft Identity Integration Server (MIIS), third-party directory stores can be synchronized with Active Directory.

To understand what it takes to be successful using directories in large environments, IDC conducted a research project to determine what successful organizations are doing right to achieve these goals. This research was conducted in 2005 and 2006 and focused on 141 for-profit enterprises in the United States with 1,000 to 20,000 PCs. Each organization was interviewed about its IT assets, IT staffing levels, and management practices. The research also captured metrics about the quality and timeliness of IT services. The goal of the research was to identify best practices that could provide guidance to other firms desiring to improve IT operations with the use of Active Directory.

The research focused on three metrics of the IT infrastructure. Together, these three metrics describe the value equation for IT infrastructure:

- IT labor costs
- Service levels
- Business agility

IT labor is defined as the ratio of IT full-time equivalents (FTEs) to PCs multiplied by a fully burdened IT labor rate of $53 per hour.

Service levels represent the quality and timeliness of IT services delivered to the business. Since service levels involve many variables, IDC chose the number of service desk calls per PC per year as a proxy for this category.

Business agility describes the IT department's ability to adapt to changing business conditions. As a proxy for business agility, IDC chose the time it takes to deploy a new application to the desktop.

Based on the IT labor cost per PC, IDC segmented the 141 organizations into the following groups: Basic, Standardized, Rationalized, and Dynamic. These four groups are collectively defined within a framework known as the Infrastructure Optimization Model (IOM). Microsoft was the lead developer of the IOM, an operational benchmark for gauging the maturity of a company's IT infrastructure.

- Basic organizations are the least efficient performers and have high costs and average service levels and agility. These organizations typically use few of the best practices defined in this paper.

- Standardized organizations have somewhat better IT costs with similar service levels and agility when compared with Basic organizations. These firms leverage some of the easier-to-implement best practices.

- Rationalized firms have very low IT labor costs and show modest improvements in service levels and agility compared with the two lower groups. These organizations use many IT best practices and automate and standardize wherever possible.

- Dynamic organizations shift the focus from cost reductions to enabling business with optimal service levels and agility. Dynamic organizations may even choose to accept best practices that increase costs to optimize service levels and agility. Few Dynamic organizations exist today, largely because many of the prerequisite technologies are not available from a single vendor and must be assembled from an array of technologies from multiple vendors. No organizations that qualified as Dynamic were interviewed for this research.

Key findings of this study by IOM level per PC per year are as follows:

IT labor

- Basic: $1,320

- Standardized: $580

- Rationalized: $230

Service levels (Number of service desk calls)

- Basic: 8.4
- Standardized: 8.5
- Rationalized: 7.7

Business agility (Time to deploy a new business application — evaluation, procurement, and deployment)

- Basic: 5.4 weeks
- Standardized: 5.2 weeks
- Rationalized: 4.3 weeks

An organization's IOM level is determined by the adoption rate of best practices. Best practices are optimized IT processes supported by technology that reduce cost and/or improve service levels and agility.

ACTIVE DIRECTORY BEST PRACTICES

In this research, IDC evaluated 10 potential best practices and identified four that are consistently used by top-performing IT departments that optimize their use of Active Directory.

- **PCs managed by Group Policy Objects (GPOs) (labor savings of $120 per PC per year).** Requires PCs to authenticate into Active Directory and individual PCs to receive configuration, software installation, and desktop configuration through GPOs.
- **Comprehensive directory solution (labor savings of $120 per PC per year).** Requires a single directory for authentication, single sign-on capability for all computing resources, and automated password reset.
- **Reduction of third-party application directories (labor savings of $90 per PC per year).** Requires the use of a single directory service both for operating system management and for application directory services. Very few companies in this study reached this goal, but those that did achieved significant IT labor savings.
- **Automated user provisioning (labor savings of $50 per PC per year).** Requires single directory or synchronized directories with a metadirectory service and IT processes for automated user provisioning. Users are provisioned (including adds, removes, and changes) once in a primary directory, and the changes are propagated to all related directories.

The remainder of the white paper goes into more detail and discusses how Microsoft products can be used to help attain these best practices.

SITUATION OVERVIEW

This white paper is one in a series of IDC White Papers based on research across a total of 141 U.S. organizations. The study was based on a subset of the overall total — a sample of 57 organizations with 1,000 to 20,000 PCs in their IT infrastructure.

Data collected from each organization participating in the study was used to categorize the relative level of IT optimization and the sophistication of their practices for deploying and using IT. The companies could then be mapped into the IOM based on their IT utilization and sophistication levels.

The purpose of this mapping exercise is to group companies together to determine the most commonly used best IT practices and to establish a correlation between the best practices and IT cost savings.

The story is not about cost savings alone. Organizations that use more highly optimized infrastructure frequently are able to increase the service levels that end users experience. This may be because end users are less likely to accidentally misconfigure their own systems, or it may be because a PC is configured to be more secure and less likely to be impacted by malware. Better service levels should translate to more productive, happier end users — which in turn also provides benefits to the IT staff.

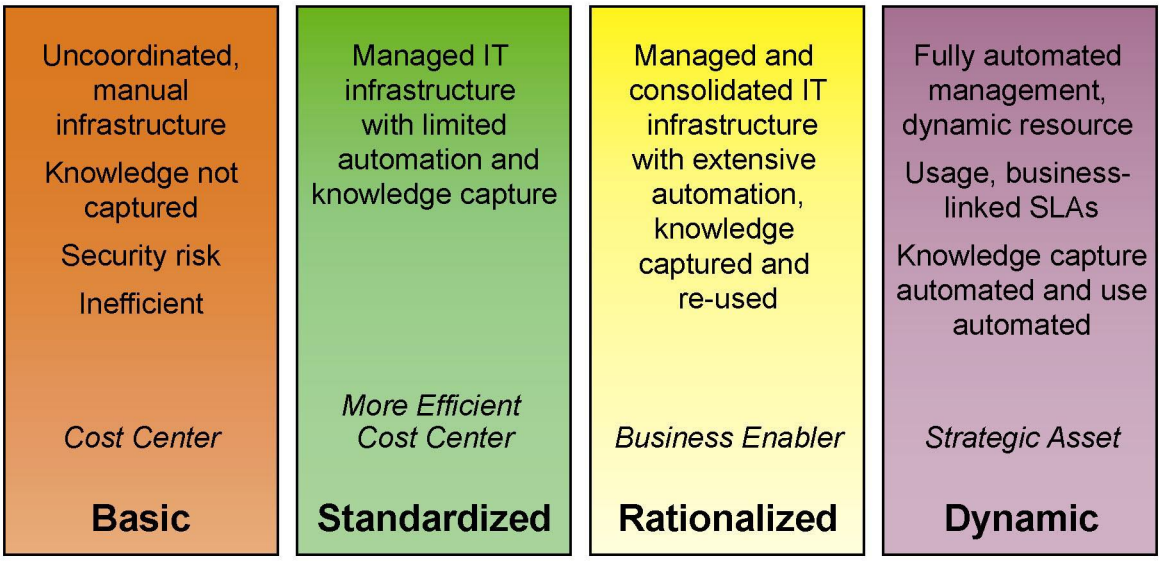
An additional benefit of better IT optimization is business agility. We define business agility as the IT department's ability to adapt to changing business conditions and technology requirements. The study found a number of factors that contribute to agility, including the overall IT optimization, the consistency of desktop operating system selection, the use of Windows Server and Active Directory, and the management practices and tools in place to both support and update desktop systems with patches, fixes, and new software deployments. In theory, the greater the level of IT optimization, the better the agility that an organization can enjoy.

To determine an organization's optimization level, IDC examined the staffing patterns and IT labor levels across organizations in similar industries and of similar size. We then stack-ranked each organization by its IT labor costs for day-to-day desktop operations. We grouped organizations into four categories: Basic, Standardized, Rationalized, and Dynamic. This grouping allowed us to identify common behaviors among organizations that performed well and to contrast them with the behaviors of organizations that performed less efficiently. The common behaviors of our best performers provided our definitions of key best practices.

Figure 1 introduces the concept of the IOM in graphical format.

FIGURE 1

Microsoft's Infrastructure Optimization Model



Source: Microsoft, 2006

This white paper is one in a series of papers that cover the Windows desktop environment, Microsoft Systems Management Server, Windows Server, and business productivity. Another paper will cover the overall IOM. The papers are as follows:

- *Optimizing Infrastructure: The Relationship Between IT Labor Costs and Best Practices for Managing the Windows Desktop*
- *Optimizing Infrastructure: The Relationship Between IT Labor Costs and Best Practices for Managing Windows Servers*
- *Optimizing Infrastructure: The Relationship Between IT Labor Costs and Best Practices for Systems Management Server*
- *Optimizing Business Productivity Infrastructure: The Relationship Between IT Labor Costs and Best Practices for Managing Collaborative and Messaging Systems*
- *Optimizing Infrastructure: Generating Value Through Improving IT Operations with Best Practices*

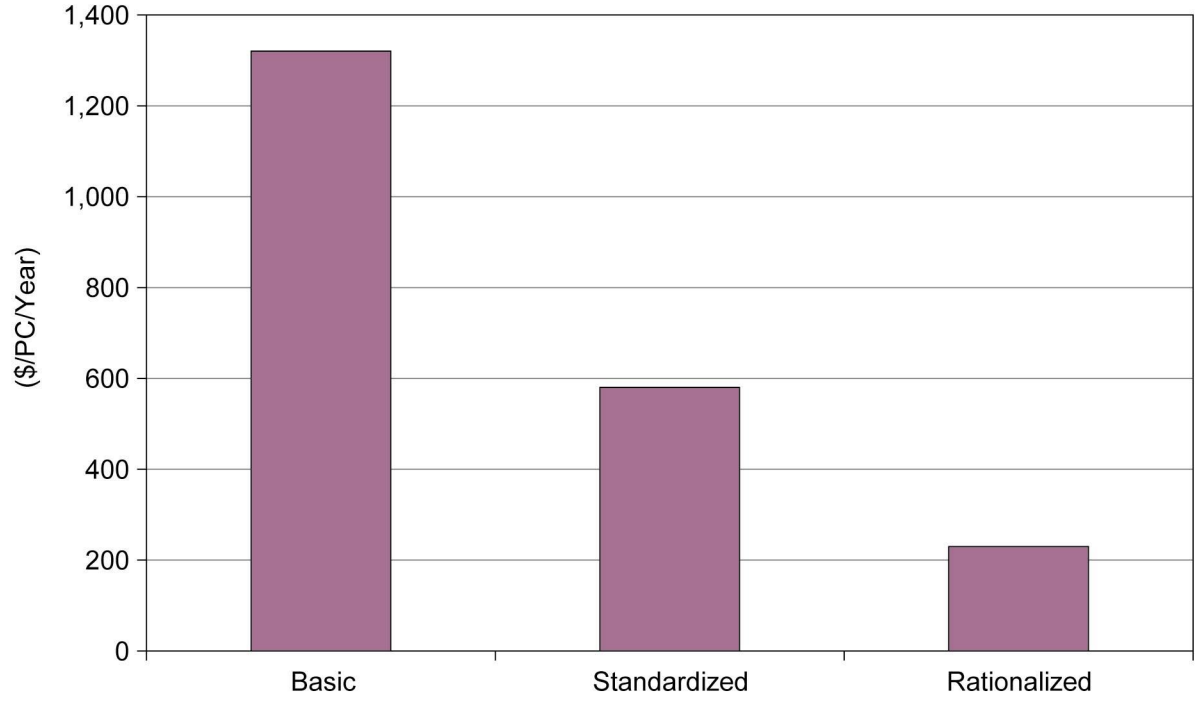
THE IMPACT OF INFRASTRUCTURE OPTIMIZATION ON PC COSTS

In analyzing the impact of best practices for desktop systems, IDC used IT labor costs associated with supporting PCs as a major metric. IT labor costs include items such as service desk staffing, desktop engineering, and ongoing PC management using directories and systems management tools. The costs are derived from an analysis of IT FTE staffing. IT labor levels are more directly affected (positively and negatively) by IT policies than any of the cost elements of total cost of ownership, which includes hardware, operating system, middleware, applications, services, and IT labor.

Figure 2 shows IT labor costs per PC per year associated with desktop systems in use within the organizations studied. The comparison covers staffing costs associated with evaluation, acquisition, hardware and software configuration, image management, hardware maintenance and software deployment, application management, security, and more. The IT labor costs fall by 56% from a Basic environment ($1,320/PC/year) to a Standardized environment ($580/PC/year), and then by an additional 61% from Standardized to Rationalized. These cost reductions result from the streamlining of IT operations through the use of best practices and more common software stacks across PCs.

FIGURE 2

Annual IT Labor Costs Comparison by IT Optimization Level



n = 141

Source: IDC, 2006

The savings potential is significant for an organization that moves from a Basic to a Rationalized environment — over 82%. However, IDC recognizes that such a quantum leap is not practical to implement quickly and that significant investment would be required.

The up-front costs would need to be rationalized through return-on-investment (ROI) calculations. However, the savings appear great enough that a viable ROI story should be achievable for most organizations.

In reality, infrastructure optimization is not a single quantum IT advancement but rather an ongoing process with a series of smaller steps. For example, Basic organizations should first become Standardized and then pause to allow their infrastructure and best practices to stabilize. Then they should focus on getting to the next level.

IDC's definition of the Basic category incorporates a wide range of organizations that other studies may have discounted as outliers. As a result, there is wide variance in the Basic category and generally higher costs compared with previous studies. We believe the current study, being broader and more rigorous, captures a broader range of companies and is thus more representative of the market than previous studies.

In addition, the following factors are potential contributors to the broad variations found in the Basic classification:

- The IDC study included a number of companies that generate revenue with their IT infrastructure and are thus more concerned with availability and capacity and less concerned with costs than the average commercial enterprise.
- A number of highly complex and distributed companies were included that experienced above-average support costs.
- Because Basic is the entry-level category, there are no minimum requirements for attaining a Basic rating. Companies that develop cost-reducing best practices quickly move into the Standardized level. We believe that the average costs per client would rise with the number of companies included in the study because the least carefully managed organizations would fall into this classification.

Table 1 presents a composite view showing the correlation between IT costs, service levels, and business agility for three levels of IT optimization. IT costs are expressed in terms of IT labor costs per PC per year; the metric used to compare service levels is the number of calls to the service desk per PC per year; and business agility is measured in terms of the number of months to deploy a new application to 90%+ of the organization.

TABLE 1

IT Optimization Levels and Related Costs

	Basic	Standardized	Rationalized
IT costs (IT labor costs per PC per year, excluding software and hardware costs)	$1,320	$580	$230
Service levels (number of service desk calls per PC per year)	8.4	8.5	7.7
Business agility (weeks to deploy new application)	5.4	5.2	4.3
n =	28	83	30

Notes:

- Lower values for IT labor costs result in cost savings for companies. IT labor costs are based on a fully burdened labor rate of $100,000 per year.
- Service levels show the number of service desk calls per PC per year. Smaller numbers represent higher service levels.
- Business agility is represented as the time to deliver a new application in weeks and includes evaluation, application development, procurement, testing, packaging, deployment, and troubleshooting. A smaller number represents a higher agility.
- Service levels remain relatively unchanged in the shift from a Basic to a Standardized organization. A dramatic change in service level is experienced only when a company adopts the Rationalized model.

Source: IDC, 2006

As shown in Table 1, a directional consistency and a tangible cost savings are associated with moving from a Basic IT environment toward a Rationalized environment. The companies in the study fell along a continuum from Basic to Rationalized, but, on average, companies in a Rationalized environment enjoyed 60% lower IT labor costs, 9% fewer service desk calls, and 17% faster deployment of business applications than Standardized companies and 83% lower IT labor costs, 8% fewer service desk calls, and 20% faster deployment of business applications than Basic companies. Organizations typically don't begin to focus on service levels and agility until the Rationalized and Dynamic levels.

ACTIVE DIRECTORY FINDINGS

In analyzing the impact of best practices for Active Directory, IDC used IT labor costs associated with supporting PCs as a major metric. IT labor costs include items such as service desk, desktop engineering and support, directory management, and identity management. The costs are derived from an analysis of IT FTE staffing. IT labor levels are more directly affected (positively and negatively) by IT policies than any of the cost elements of total cost of ownership, which includes hardware, operating system, middleware, applications, services, and IT labor.

Relationship of Best Practices and Cost Savings Through the Use of Active Directory

IDC examined the IT environment, strategies, and activities related to Windows PCs of 57 organizations with 1,000 to 20,000 PCs in commercial industries.

From this research, IDC has determined that four key best practices are associated with the use of Active Directory in Windows server environments. Three of the four best practices are related to the cost reductions associated with managing PCs in the Windows environment. The fourth best practice is related to minimizing the number of directories in use within an organization.

Table 2 shows these practices and their associated cost savings.

TABLE 2

Active Directory Best Practices and Related Cost Savings

Best Practice	IT Staff Cost Savings per PC per Year ($)
PCs managed by Group Policy Objects	120
Comprehensive directory solution	120
Reduction of third-party application directories	90
Automated user provisioning	50

n = 57

Source: IDC, 2006

The best practices identified in Table 2 offer a summary view of the way to lower IT labor costs in a Windows environment. For example, managing PCs through GPOs has the effect of creating a more streamlined and consistent installed base of PCs. IT administrators can make valid assumptions about the configuration of desktops within different organizational units and distribute software, change settings, or plan for a refresh of applications or operating system software. Having known states on these systems leads to less IT staff time spent in dealing with one-off problems that random system alterations would create.

A comprehensive directory solution reduces the complexity of authentication, reduces the amount of interaction that users must have with IT personnel when accessing new applications, and requires that a high percentage of PCs (greater than 90%) standardize on a single directory for authentication and sign-on.

A direct follow-on to a comprehensive directory solution is the reduction or elimination of third-party application directories by using Active Directory as the primary repository of identity and access rights information. However, in most organizations, the first step toward elimination of redundant directory stores is through synchronization, rather than elimination, of application directories. This can be accomplished through Microsoft Identity Integration Server or third-party solutions that are widely available in the industry. In the longer term, the best practice identified here suggests that organizations that use synchronization can achieve additional value by working toward the use of a single directory.

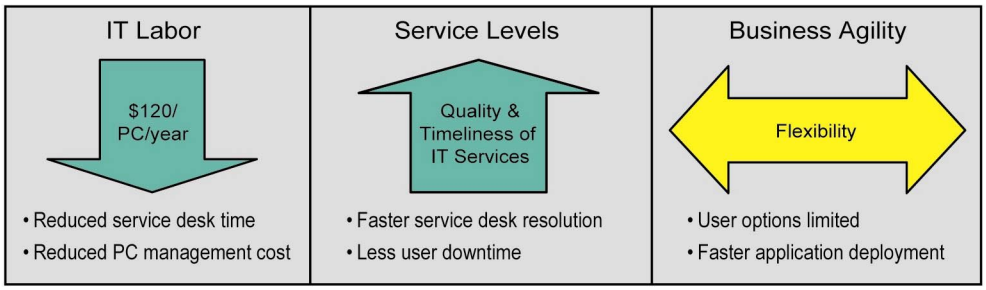
User provisioning enables customers to automate the addition, removal, or alteration of user profiles in a single directory — or across multiple directories and identity stores. This allows the organization to make a change once and have it propagate throughout the organization.

These best practices offer varying benefits; some practices, such as managing PCs by GPOs, reduce the level of day-to-day attention that IT personnel must apply to ensuring that users have the applications they need and that systems are configured and updated in response to changing business, organizational, or security needs.

The sections that follow, including Figures 3–6, drill more deeply into these best-practice areas and discuss the reasons for the positive benefits shown in Table 2.

FIGURE 3

PCs Managed by Group Policy Objects



Source: IDC, 2006

Problem and Challenge

There is a direct correlation between IT labor costs and the number of PC configurations supported by an IT organization. While many shops deploy a standard desktop, within a few hours of deployment, users begin changing settings and installing authorized and unauthorized applications. In some cases, security and reliability are jeopardized by the increasingly ad hoc configurations. The destandardization of PC configurations presents challenges for both desktop engineering and the service desk.

In theory, the solution to the problem is simple: remove administrative rights from PCs and push down configuration settings with group policies. However, many IT departments find this challenging for three reasons. One, many old applications require administrative rights to install and function. If they are critical business applications, it may not be possible to remove administrative rights. Two, many organizations do not have the proper expertise and technology to manage PC settings even if the administrative rights issue is addressed. Three, one of the reasons that PCs have been widely adopted in business is to empower users by allowing them to configure their PCs in ways that optimize their productivity. Limiting the settings users can change may be politically difficult and, for some organizations, may interfere with agility.

Best Practice

Managing PC configurations requires a combination of process and technology. In terms of process, organizations need to deploy a standardized desktop before implementing this best practice. There is less value to using Group Policy Objects to restrict users' systems if the PC configurations are not standardized first. The IT department needs to work closely with the business stakeholders to determine which settings make sense to restrict, based on trade-offs that include IT cost, security risk, and user productivity benefits.

To use this best practice, all users must first authenticate to a single directory. The directory needs to be hierarchical and able to deliver PC configuration settings based on site information and group membership. To prevent users from overriding the policies pushed down by the directory, the IT department must ensure that they are operating in "standard user" mode — meaning they are not given administrative rights.

Applications that require administrative rights must be replaced by newer or better-written applications, or utilities must be deployed to serve as a workaround. IDC notes that third-party software from companies such as BeyondTrust and FullArmor provides workarounds.

While researching this best practice with organizations that used Active Directory and Group Policies, we identified settings used by the top-performing organizations (measured in terms of the lowest IT labor costs).

The following settings were used consistently by the upper half of the sample:

- Users were prevented from editing the registry.
- Approved applications were published in the directory.
- Operating system settings were configured by Group Policy Objects.
- Start menu was configured and some icons were removed.
- Start-up and log-in scripts were pushed to PCs.
- Internet settings were configured by GPOs.
- Security settings were configured by GPOs.
- Application settings were configured by GPOs.

PCs Managed by GPO Best-Practice Findings

IT Labor Impact

On average, adoption of this best practice yielded an IT labor cost savings of $120 per PC per year. The savings from this best practice will be realized by desktop engineering and support personnel and also by the service desk. Desktop engineering and support will be reduced because deployed PCs will now utilize one of a limited number of configurations.

Having a small number of known configurations will reduce the amount of application compatibility testing and resolution time required when deploying new applications and operating system upgrades. Service desk costs will be reduced because fewer users will break their own PCs by making erroneous changes to system and security settings.

Service desk incident resolution times will be reduced because fewer configurations will make PCs easier to troubleshoot. It should be noted that this best practice is a partial duplicate of the "Centrally Managed PC Settings and Configurations" best practice evaluated in the IDC White Paper *Optimizing Infrastructure: The Relationship Between IT Labor Costs and Best Practices for Managing the Windows Desktop.* The two best practices are not additive.

Service-Level Impacts

When users are prevented from changing critical settings, PCs will become more reliable and less prone to security breaches. As a result, users will spend less time on the phone with the service desk or trying to solve their own problems. This means the user experience will generally improve.

Because all security settings are managed centrally, the organization's security risk is reduced, and in the process, business operations and intellectual property are protected.

Agility Impact

The best practice potentially helps and hurts agility in different ways. Agility improves when IT is more quickly able to deploy business applications and patches because of consistent configurations that minimize application testing and reduces failures during the install process. Agility is hurt because users have less freedom to configure their PCs to meet their personal productivity needs, which would likely cause a higher dependency upon IT personnel who have administrative privileges on PCs.

Technologies Required

- Windows 2000 Server or Windows Server 2003
- Active Directory configured and deployed
- Group Policy Objects
- Windows 2000 Professional, Windows XP Professional, or Windows Vista

Implementing this best practice with Windows 2000 Professional or Windows XP Professional may be difficult because some older applications may still require administrative rights. Typical workarounds are third-party utilities that allow the applications to perform under "standard user" context.

Microsoft's newest client operating system, Windows Vista, may offer an alternative to the workarounds. The new product includes directory and registry abstraction that allows older applications to write to virtual administrative directories and registry keys. Windows Vista also has a technology called User Account Control (UAC), which allows some applications to run under administrative context even when the user is running as a standard user.

Designing and implementing Group Policy Objects is another requirement to implement this best practice. But crafting and managing Group Policy Objects in a large organization can be challenging due to conflicting requirements among different groups, divisions, and departments.

Third-party tools have been available to help with the management of complex Group Policies, and Microsoft recently stepped forward to address the issue with its acquisition of DesktopStandard Corp. in September 2006. The DesktopStandard acquisition adds tools to Microsoft's portfolio that help administrators manage complex and overlapping group policies through an easy-to-use interface.

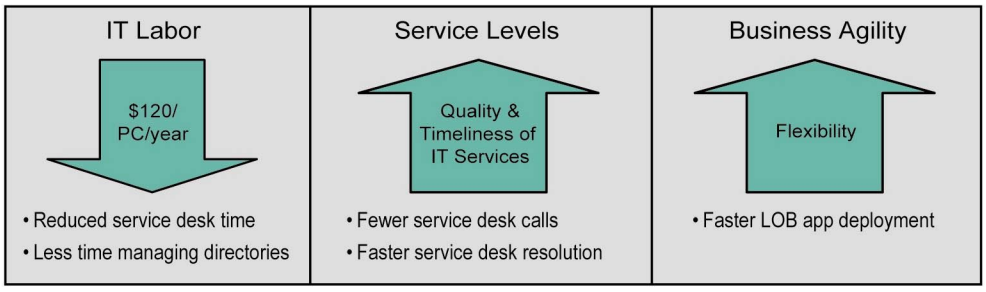
DesktopStandard's management product, GPOVault Enterprise Edition, will be available from Microsoft as Microsoft Advanced Group Policy Management as part of the Microsoft Desktop Optimization Pack offering, which is available exclusively to volume license customers that have Software Assurance. Microsoft is still working on long-term integration plans for the remaining products acquired.

Who Will Want This Best Practice?

This best practice will be attractive to organizations that have the infrastructure to support it and where it is politically acceptable to the user community.

FIGURE 4

Comprehensive Directory Solution



Source: IDC, 2006

Problem and Challenge

Directories are a critical component of any IT infrastructure. They provide identity and management services for users and systems to access network and application resources. Directories also are a vehicle for delivering policies that manage PCs, servers, and network devices.

Over the years, most organizations have deployed multiple directories to manage user, network, and application information. To reduce costs and provide high service levels, organizations need to take inventory and reduce the number of directories they support, although in many cases, it is more practical to invest in a synchronization solution such as a metadirectory for keeping the information across their different directories consistent.

If organizations were starting from scratch, building an effective directory solution would be easy. The reality is that most large organizations will have dozens of directories associated with legacy applications that provide critical business services. Directory sprawl also can occur from mergers and acquisitions, where disparate systems must be cobbled together. Some directories are more easily integrated and synchronized than others.

The bottom line is that most organizations find it challenging to implement a comprehensive directory solution because of their organizational history and the cost of integrating legacy systems.

Best Practice

A comprehensive directory solution provides single or simplified sign-on for users along with utilities for automated password changes and resets. Although there are many permutations on how to achieve a comprehensive directory solution, most use a single directory for network authentication for users, PCs, and servers in conjunction with a metadirectory service that synchronizes and maintains a consistent, enterprisewide view of user information in the network directory with application directories.

Once all accounts are synchronized, the number of passwords that users have can be reduced, resulting in higher levels of security and fewer password-related calls to the service desk.

Comprehensive Directory Solution Best-Practice Findings

IT Labor Impact

On average, organizations that implement this best practice will achieve an IT labor savings of $120 per PC per year. The savings will occur both at the directory administrator level and at the service desk. When directories are synchronized, fewer IT personnel need to be involved in identity and access management.

For instance, when a user record is created in the human resources directory, corresponding user accounts and profiles can be automatically created in other directories and kept consistent based on IT policy. When directories are synchronized, users have fewer issues obtaining password credentials and

accessing IT resources. This reduces service desk costs. Service desk costs are also further reduced by automated password reset systems that give users a self-service capability rather than force users to call the help desk to reset passwords.

Based on our research, we were able to estimate the cost savings per PC of each of the best-practice subcomponents:

- Standardizing on a single directory for authentication ($70 per PC per year)
- Simplified sign-on by synchronizing directories with metadirectory service ($20 per PC per year)
- Automated password reset ($30 per PC per year)

These subcomponents should be considered sequential. Organizations implementing this best practice should first focus on implementing a single hierarchical directory for user, PC, and server authentication. Hierarchical directories are important because they allow delegated administration and policies to be inherited through the hierarchy. This is one of the keys to effective use of group policies to manage users, PCs, servers, and network resources. Using a single directory for user authentication will also provide users with single sign-on capability.

In cases where customers can't get to a single authentication directory, a metadirectory service can also be used to keep information consistent across directories and provide simplified sign-on by allowing the user to have a single user ID and password that spans multiple directories. Most metadirectories are able to connect to a wide variety of user repositories such as LDAP directories, relational databases, legacy authorization systems, human resources systems, and ERP systems using the system's native protocol.

Once single or simplified sign-on is achieved, utilities should be deployed that can provide an automated password reset service. Based on IDC's research, automated password reset utilities provide little value unless they are built into a larger directory strategy.

Service-Level Impacts

Service levels improve with this best practice because users need to remember only one user ID and password. Service desk calls for password resets are also dramatically reduced by one set of credentials and utilities that allows users to reset their own passwords.

Agility Impact

This best practice improves agility in two ways. IT is able to bring new applications online more quickly by using the network directory service for single sign-on and by using the metadirectory service to maintain consistency. Users are also empowered to solve their own problems with automated password reset, thus reducing their reliance on IT.

Technologies Required

- Windows 2000 Server or Windows Server 2003
- Active Directory
- Microsoft Identity Integration Server or other metadirectory solution for directory and password synchronization
- Self-service Password Reset software, which is available from third-party products today
- Windows 2000 Professional, Windows XP Professional, or Windows Vista

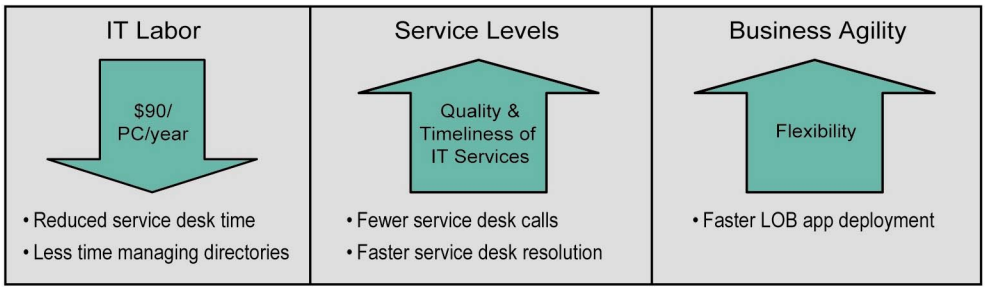
Future versions of Microsoft Active Directory and Microsoft Identity Integration Server will further support this best practice by adding new functionality such as more flexible deployment support in branch office scenarios, better end-user self-service, and simplified delegation and management.

Who Will Want This Best Practice?

Organizations with multiple directories will benefit from this best practice, assuming they have the infrastructure and the technical skills to support it.

FIGURE 5

Reduction of Third-Party Application Directories



Source: IDC, 2006

Problem and Challenge

Most organizations have numerous line-of-business (LOB) applications, and each LOB application typically requires identity and access management to function. Unfortunately, each LOB requires its own directory, and each directory incurs management cost.

Metadirectories reduce many day-to-day IT activities but do not eliminate administration costs. Whenever possible, organizations need to leverage existing directories for new LOB applications instead of installing the proprietary directories that are provided with the product. The same holds true for applications developed in-house by development teams.

The challenge is that many purchased LOB applications do not provide the option of using anything other than the directory provided by the manufacturer. Also, for LOB applications that are already in place, replacing the current directory with an alternative directory is often not cost-effective.

Finally, many in-house developers are not mandated by management or do not have the skills to use the directories already in use within their organizations. In this research, only 22% of organizations reported that they are able to successfully use an existing directory in a new LOB application implementation.

Best Practice

When implementing new LOB applications such as ERP and CRM, organizations should choose vendors that allow their software to leverage existing directory infrastructures instead of installing a new directory with the application.

Windows developers have several different programming interfaces through which to access Active Directory, including LDAP; therefore, Active Directory can be used with a wide range of systems. Integration with internally developed applications using Visual Studio and the .NET framework can simplify the construction of directory and identity-aware applications on Windows.

IDC's research found that only a minority of the companies interviewed in this study had successfully reduced their use of third-party directories, which provides some insight into the difficulty associated with achieving this best practice.

Reduction of Third-Party Application Directories Best-Practice Findings

IT Labor Impact

Organizations that were able to significantly reduce the number of application directories by leveraging existing resources were able to reduce their IT labor on average by $90 per PC per year, compared with organizations that did not have this best practice.

The savings resulted from efficiencies gained by not having to maintain duplicated directories across many applications. Service desk costs were also reduced because of the simplified sign-on capability that results from this best practice.

This best practice does have some overlap with the comprehensive directory solution best practice because both provide simplified sign-on and directory standardization. In fact, the only difference is that the comprehensive directory solution has automated password reset ($30 per PC per year) and this solution does not.

Therefore, these best practices should be considered two paths for reaching the same objective. The benefits are not additive.

Service-Level Impacts

Service levels improve for this best practice because users are able to get to business resources more easily with fewer service desk calls about identity and access management.

Agility Impact

Using an existing directory instead of creating a new one can be a major time saver and improves agility over the longer term. Organizations that use this best practice will be able to deploy new LOB applications more quickly. This applies to both off-the-shelf-applications and applications developed in-house, as long as the LOB application can leverage the existing directory or a metadirectory server is used to bridge the LOB to the core directory service.

Technologies Required

- Windows 2000 Server or Windows Server 2003
- Active Directory
- Visual Studio 2005 and the .NET framework
- Windows 2000 Professional, Windows XP Professional, or Windows Vista

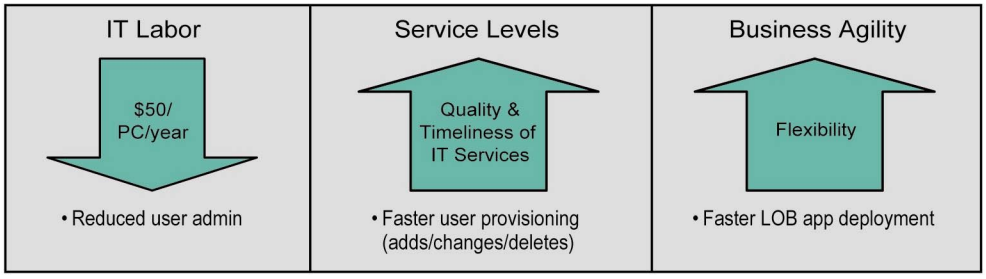
IDC notes that Microsoft's next version of Active Directory, included in Windows Longhorn Server, will include new functionality that will help developers implement this best practice more easily. This functionality includes a richer runtime services and programming model through .NET 3.0 and Windows Communication Foundation.

Who Will Want This Best Practice?

This best practice is a good fit for organizations that are looking to reduce costs associated with maintenance of the information within multiple resources and that would like to boost agility for newly deployed applications and newly hired, newly reassigned, or released employees.

FIGURE 6

Automated User Provisioning



Source: IDC, 2006

Problem and Challenge

Organizations require an effective way to add, remove, and change user accounts and access rights to their IT environments. When a new employee is hired, the organization needs to provide access to IT resources on the first day of employment. When an employee leaves the organization, human resources needs to be able to revoke access to all IT systems within minutes of the separation in order to protect corporate resources.

Doing this quickly (and cost-effectively) necessitates that identity and access management take place centrally in an automated fashion instead of manually across multiple application and system directories. This becomes even more critical when large numbers of interns, vendors, and contractors who use IT systems move in and out of an organization daily.

What makes user provisioning so challenging for many organizations is the existence of a complex and redundant set of application directories, each of which requires unique user IDs and passwords. Worse, many organizations have large numbers of legacy systems that are not easily synchronized with a metadirectory system. The majority of organizations simply do not have the tools or technical expertise to implement a one-step "hire and fire" solution to identity and access management.

Best Practice

This best practice starts with the logical next step of moving to a comprehensive directory solution. Once directory synchronization is achieved through the use of a metadirectory, organizations need to apply business processes to the job of managing employee accounts, access, and passwords, moving to an automated provisioning solution.

In many cases, the human resources system is a good starting point for account provisioning and is one reliable source of authoritative employee information.

When a change is made (add, delete, change) in an authoritative system (e.g., the human resources system, Active Directory, and other user information repositories), the metadirectory picks up the change and takes an action based on policy such as updating all other directories. A human resources application directory contains information about an employee's job role that is used to add or remove the employee from access groups within the application directories.

Automated User Provisioning Best-Practice Findings

IT Labor Impact

On average, this best practice reduces IT labor by $50 per PC. The savings comes from two areas. One, IT staff members no longer need to spend time manually creating, deleting, or changing user access rights. This capability is now automated from the point that a user's information is entered into the human resources system when he or she is hired. Two, fewer mistakes are made because this is an automated process with checks and balances, which in turn reduces the potential for calls to the service desk.

Service-Level Impacts

This best practice dramatically improves service levels. New employees are now brought online faster and thus can become productive almost immediately, and they can remain productive when they enter a new role because the services they need are automatically provisioned. Organizational risk is reduced because access is revoked almost immediately when an employee changes roles or leaves the organization. There is also a slight reduction in service desk calls because it is less likely that users will be given the wrong access.

Agility Impact

This best practice allows an organization to make changes to employee access to resources almost in real time, which significantly improves agility. Business managers can move employees around at will and access to key systems can be configured in minutes through this automated process.

Technologies Required

- Windows 2000 Server or Windows Server 2003
- Active Directory
- Microsoft Identity Integration Server
- Windows 2000 Professional, Windows XP Professional, or Windows Vista

This best practice also requires a human resources software system that can be integrated into Active Directory with Microsoft Identity Integration Server. Future versions of Microsoft Identity Integration Server will make it easier to implement this best practice through new features, including capabilities for better capturing and implementing the user provisioning and access policy in a way that is more intuitive to business users.

Who Will Want This Best Practice?

This best practice is a good fit for organizations that need to quickly and effectively provision and deprovision users who join or depart a company or change functions. It also would be particularly useful among organizations with a large number of temporary workers or volunteers, as well as organizations with high user turnover, such as educational facilities that need to provision on a per-class, per-semester, or per-student basis.

IDENTITY AND ACCESS MANAGEMENT AND PC DEPLOYMENTS

Identity and access management incorporates a comprehensive set of solutions used to identify users in a system (e.g., employees, customers, and contractors) and to control their access to resources within that system by associating user rights and restrictions with the established identity. Web single sign-on, host single sign-on, user provisioning, advanced authentication, legacy authorization, public key infrastructure, and directory services are all critical components of identity and access management.

In the context of new PC deployments, having a pre-existing identity and access infrastructure through Active Directory can significantly speed the installation and configuration of new PCs. To fully leverage Active Directory requires pre-establishment of a directory infrastructure, the logical division of an organization into so-called organizational units, and the development of collections of configuration and provision policies specific to each organizational unit.

Once a PC joins a domain, using Group Policy Objects, a new, unconfigured PC can have the desktop configured, wallpaper applied, security settings adjusted, and firewall turned on, and applications can be either made available or immediately pushed down onto the system. It's also possible to make available documents previously created on a different machine through the use of Microsoft's IntelliMirror technology. This takes place through activities discussed at length in the related IDC White Paper titled *Optimizing Infrastructure: The Relationship Between IT Labor Costs and Best Practices for Managing the Windows Desktop.*

ACTIVE DIRECTORY DEPLOYMENT COSTS

Figure 7 shows the costs associated with deploying Active Directory from four scenarios: migration of Windows NT 4.0 domains to Active Directory, new installation, migration from a competitive product, and upgrade from a previous version of Active Directory.

IDC notes that the incidence of migrations from earlier versions of Active Directory should increasingly be the most common scenario experienced by Windows users, although it is the least common scenario among respondents today. This is due to the fact that Windows NT 4.0 installations are quickly being decommissioned by customers as the product falls further and further from mainstream support.

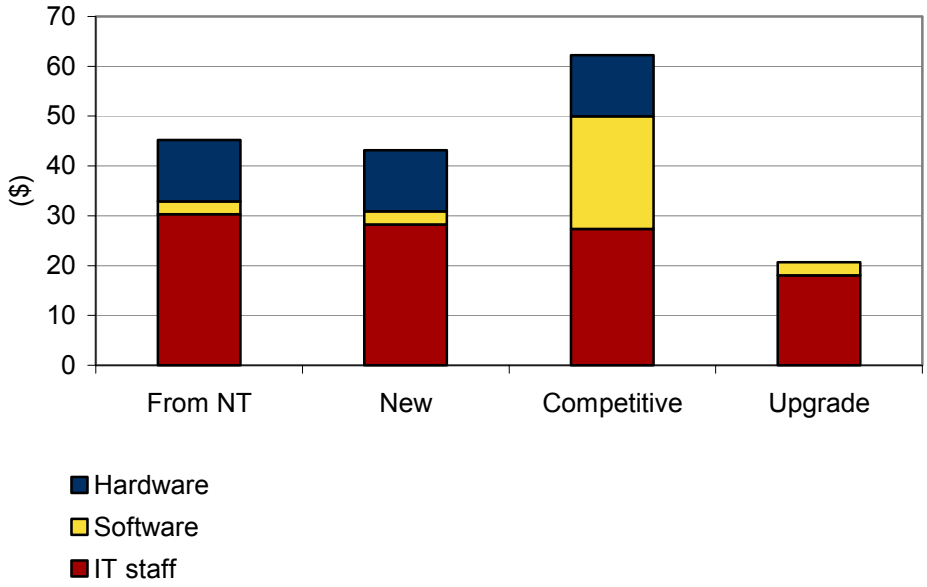
The migration from competitive products may well continue for several more years because a large installed base of organizations has the potential to migrate.

Hardware costs include only the cost to deploy new servers (at an average cost of $5,500 per processor) to support an average of 5,000 users. Software costs include the client access licenses (CALs) that permit using Active Directory (e.g., Windows Server CALs) at an average cost of $20 each. The primary cost differentiator is IT labor, which ranges from $18 per PC for simple upgrade from Active Directory on Windows 2000 Server to Active Directory on Windows Server 2003 to $30 per PC for migration from NT 4.0 domains. Moving from a competitive environment costs an average of $27 in IT staff labor per PC.

Total costs range from under $21 per client for a Windows-to-Windows upgrade to a high of $62 per PC for a migration from a competitive directory environment.

FIGURE 7

Active Directory Deployment Costs per Client



Note: Software costs are based on a client access license at an average cost of $20. Hardware costs are based on 5,000 users.

Source: IDC, 2006

RECOMMENDATIONS FOR ORGANIZATIONS WISHING TO OPTIMIZE THE ACTIVE DIRECTORY ENVIRONMENT

Based on this research, IDC offers the following guidance for organizations that are interested in optimizing their infrastructure through the use of best practices related to Active Directory.

General Recommendations

The results of this study point to the simple conclusion that less is better when it comes to having directories to populate and manage. Minimizing the use of unique directories and synchronizing those directories with metadirectory tools can lower the operational labor costs and can improve the benefits that users receive. Combining directories with group policies allows a secondary benefit from the investment in the directory layer.

This study found a distinct potential to reduce IT labor costs by using Active Directory along with Windows server and client operating environments. Adopting best practices and using technology to drive process improvement yield direct benefits as part of a more efficient deployment strategy.

Basic Organizations

Customers that fall into the Basic level of the IOM do so for one of several key reasons, which can be readily addressed:

- Lack of a primary directory service
- Use of multiple directory services
- Inconsistent or partial use of Active Directory and Group Policies to manage client systems

Guidance for Basic Organizations

The activities reviewed in this analysis suggest that the following best practices should be considered by Basic organizations:

- Add a primary directory service. Even the most Basic organizations will have some application directories in use, but they still have the benefit of having less legacy infrastructure to drag forward, and as a result, they are in a good position to plan for a coordinated and thoughtful approach to integrating a directory and a metadirectory service.
- Move to directory-enabled client systems. Organizations that have residual Windows 9x client operating environments in place need to replace those systems with directory-enabled clients including Windows XP and Windows Vista.
- Drive toward having all client systems authenticate into Active Directory so the infrastructure will support the movement toward a more sophisticated and managed environment.
- Once all client systems authenticate into a directory, plan to develop basic Group Policies for benefits such as desktop management and application provisioning.

Standardized Organizations

Standardized organizations will typically have Active Directory in place and are on their way toward a more optimized infrastructure, but they have done little or nothing to integrate application directories with Active Directory. In addition, while Standardized organizations tend to use some group policies, their use is neither universal nor comprehensive in nature.

- Standardized organizations typically have Active Directory in place for client authentication, but they also have multiple application directories in use that are not integrated or synchronized with Active Directory.
- Standardized organizations have few or inconsistent group policies in use.

Guidance for Standardized Organizations

The practices reviewed in this analysis suggest that the following best practices should be considered by Standardized organizations:

- Continue to invest in extending — and simplifying — Group Policy Object development.
- Focus on extending the application of Group Policy Objects across a greater number of systems to automate management and software distribution activities, preferably close to 100% of PCs.
- Focus on integrating application directories with Active Directory through Microsoft Identity Integration Server or other metadirectory technology, which can lower the administrative burden associated with managing multiple directory resources within the organization.
- Use Active Directory or Active Directory Application Mode in place of third-party application directories in new LOB application deployments.
- Leverage Active Directory and Microsoft Identity Integration Server or another metadirectory server to implement other cost-saving measures, including single sign-on and password synchronization.
- Once all the prerequisites are met, implement automated user provisioning.

Rationalized Organizations

Rationalized organizations are on the leading edge of IT optimization and can be likened to the high-performance version of their counterparts in the Standardized category. However, even within Rationalized organizations, there is usually room for further use of best practices and more complete utilization of tools and process.

- Rationalized organizations are at a critical decision point: Will their business model benefit from pushing IT management practices into the domain of the Dynamic classification, or does such a move extend their IT optimization past |the sweet spot of minimizing costs? IDC analysts believe that moving to a Dynamic environment is more about increasing IT business agility than it is about driving down costs. Indeed, moving to a Dynamic model could actually cost more because some centrally managed IT functions could be pushed out to the business units to increase responsiveness, resulting in a loss of economies of scale.
- More of a good thing is good. Most Rationalized organizations are likely to have some work left to reduce the diversity of applications, the number of application directories in use, and the combinations of operating system software and hardware in use. Reducing these variables can help lower costs further and ensure a rock-bottom cost structure.

Guidance for Rationalized Organizations

Our analysis suggests that Rationalized organizations should consider the following best practices:

- Move beyond the concept of using Active Directory and other integrated directories for one-time provisioning to a model where directory services are used for dynamic provisioning of applications and system resources can be applied to any systems when and where needed and removed when no longer required.
- Recognize that virtualization will emerge as a game changer for system configuration and provisioning. Use virtualization technology, along with Microsoft's forthcoming System Center Virtual Machine Manager and System Center Operations Manager. Together with a strong and integrated directory service backbone, virtualization enables customers to gain significant benefits from their investment in their directory service.
- However, Rationalized organizations that have their sights set on achieving a Dynamic classification should be focused on business agility and understand what that means to their business. Directory service empowers customers to move to a Dynamic environment, but customers want to be sure that this agility can be leveraged to deliver benefits to their organizations because moving to a Dynamic environment is not necessarily a cost-saving step.

CHALLENGES/OPPORTUNITIES

IT Optimization: A Long-Term Investment

The data presented in this IDC research indicates how broad the spectrum is between companies operating at the Basic level and those at the Rationalized level. Infrastructure optimization is a continuum driven by the adoption of IT best practices, and every company can improve dramatically through the implementation of policies and procedures automated through technology.

Use of Active Directory

IDC studies have found that customers that use Windows server are typically well-motivated to deploy and leverage Active Directory. These customers recognize the benefit of using Active Directory for their Windows infrastructure first and foremost.

Nevertheless, many organizations have not leveraged Active Directory for more than basic domain authentication. While it is easy to suggest that customers should embark on a process to integrate application directories with Active Directory, the physical interconnection is easy compared with the data cleansing and standardization that must take place before records can be seamlessly shared and replicated. Each application directory that is integrated with Active Directory will require a multidepartmental, team-oriented approach to review, testing, and final integration.

In many cases, because the costs associated with maintaining these application directories are absorbed by other departments, these expenses are transparent and not a pain point for IT management, which may lower the urgency for this integration on the part of IT personnel.

Group Policy Objects

Active Directory and Group Policy Objects are building blocks for creating a sophisticated and less expensive infrastructure to manage. And just like the building block analogy, a solid foundation of Active Directory, metadirectory services, and integration with third-party directory stores leads to a more powerful directory infrastructure.

One of the most visible and measurable benefits that IT personnel will see from having a directory service is the use of Group Policy Objects. However enticing Group Policies may be, the reality is that they are complex to implement and require corporate-, divisional-, organizational-, and departmental-level buy-in and consensus regarding what the right resultant set of policies should be for a given group of workers.

The holy grail of implementing Group Policy Objects requires a finite number of policies that are broadly deployed across an organization. However good that practice is in theory, in reality it is hard work — including political negotiations — to come to a set of policies that are acceptable to broad groups of people. This issue is not easy to resolve, and therefore it is a challenge to implementation.

FUTURE OUTLOOK

Microsoft is implementing significant upgrades to Active Directory as part of the Longhorn wave of server products. The following improvements are slated for Active Directory with the next release, which will come during the second half of 2007.

- Special use scenarios including a "read-only Domain Controller." Positioned as a solution for customers with branch offices, where the physical security of a Domain Controller could be compromised, read-only Domain Controllers will give central IT higher levels of security by limiting the amount of data that is held locally on the Domain Controller.
- Improved administrative granularity. The Domain Controller administrative role is separated from the Server Administrator role in branch office scenarios.
- Implementation of Domain Controller functionality in the new "Server Core'" functionality. Server Core is a new deployment scenario for Windows servers that strips off much of the general-purpose functionality, leaving the core services in place. The objective is to allow the deployment of a minimally configured system that can be locked down and secured at a higher level than possible in the past.
- New granularity on password policies, allowing certain user groups to have more restrictive password requirements based on their roles.
- Improvements to Microsoft Identity Integration Server, including extensions to permit the policy-based management of application identity and access.

As with other Microsoft technologies, Active Directory is seeing continuous investment as the company updates the underlying Windows Server technology.

CONCLUSION

At the heart of any advanced Windows environment are several key technologies that all best practices will leverage either directly or indirectly. Those key technologies, of course, include the Windows server products, the Windows client products, and, immediately following those two building blocks, Active Directory.

Once the Active Directory infrastructure is in place, multiple best practices can be layered on top of Active Directory, including using Group Policy Objects, single sign-on, and Microsoft Identity Integration Server; leveraging a directory as a comprehensive solution; and in the process, reducing or eliminating the use of third-party directory solutions.

All of these technologies are building blocks, but at the same time, these best practices in turn serve as building blocks from which other technologies can also derive secondary benefit.

The takeaway here is for customers to consider directory utilization as one of the key enablers that make it possible for organizations using Windows products to achieve positive results from best practices that lower costs for the IT department and improves their ability to compete in today's increasingly global world.

APPENDIX

Methodology

For this series of studies, IDC conducted in-depth interviews with IT personnel at 141 organizations in total. For the Active Directory analysis, IT personnel from 57 organizations were interviewed to collect information on their use of client operating environments (COEs) in the context of a comprehensive IT infrastructure. The information was used to develop a metric for the depth and consistency of each organization's use of IT. This metric was subsequently applied against a continuum of IT sophistication to position each company within a spectrum of IT optimization found in the industry.

In conjunction with this work, IDC collected data specific to the Windows desktop environment to compare total IT labor costs for Windows platforms within the context of an IT optimization model.

The interviews, which were conducted during the first half of 2006, were divided into discussions of specific topics, including the use of Windows COEs in managed and unmanaged environments, the use of related IT management technologies, and the use of images for operating systems and layered software. There were also separate discussions of IT labor, the IT adoption and deployment process, and outsourcing habits.

A key element of this study was the accumulation of staff cost data. Staffing costs tracked include the following topic areas:

- Hardware/software evaluation and purchase
- Desktop deployment/replacement (hardware/software)
- Threat assessment and security planning
- Addressing security breaches and viruses
- Hardware configuration/reconfiguration
- User administration and provisioning (adds, deletes, and changes)
- Application management
- Image management
- Software deployment and patching
- Hardware maintenance and configuration/reconfiguration
- Data management, storage planning, and backup and restore
- Help desk
- User downtime

IDC tested the impact of best practices by comparing the IT labor costs of those companies using the best practice with the IT labor costs of those that did not. In some cases, a single best practice by itself resulted in savings. In other cases, we found that the interaction of multiple, related best practices was required to obtain IT labor cost reductions.

Enterprises using at least one best practice tended to also use other best practices. We found that the more best practices an enterprise used, the greater the IT labor cost reduction that was realized. However, some of the best practices correlated in their impact on IT labor. (For example, using directory services is part of standardizing the desktop and centrally managing PC settings and configurations.) Unfortunately, it was not possible to statistically tease out the exact IT labor impact of one best practice (single or compound) versus another.

Therefore, IDC used its best judgment to prorate the relative IT labor savings attributable to each best practice. The data in this white paper is presented to enable the IT professional to weigh the *cumulative* value of adopting multiple best practices.

Additional Resources

In conjunction with this IDC White Paper on Active Directory, additional papers in this series are as follows:

- *Optimizing Infrastructure: The Relationship Between IT Labor Costs and Best Practices for Managing the Windows Desktop*
- *Optimizing Infrastructure: The Relationship Between IT Labor Costs and Best Practices for Managing Windows Servers*
- *Optimizing Infrastructure: The Relationship Between IT Labor Costs and Best Practices for Systems Management Server*
- *Optimizing Business Productivity Infrastructure: The Relationship Between IT Labor Costs and Best Practices for Managing Collaborative and Messaging Systems*
- *Optimizing Infrastructure: Generating Value Through Improving IT Operations with Best Practices*