

Realtime
publishers

"Leading the Conversation"

*The Reference Guide To*tm

Data Center Automation

sponsored by



Don Jones and Anil Desai

Business Processes.....	1
The Benefits of Well-Defined Processes	1
Defining Business Processes.....	1
Deciding Which Processes to Create	2
Identifying Process Goals	2
Developing Processes	3
Documenting Business Processes	3
Creating “Living” Processes	4
Automating Business Process Workflow.....	4
Business Process Example: Service Desk Processes	5
Characteristic of an Effective Process	5
Developing a Service Desk Operation Flow.....	5
Documenting Workflow Steps.....	6
Tracking and Categorizing Issues	6
Escalation Processes and Workflow	7
Creating a Service Desk Flowchart.....	7
Automating Service Desk Management	8
Executive Action Committee.....	9
Goals of the Executive Action Committee	9
Evaluating Potential Projects	9
Defining Committee Roles and Members.....	11
Implementing an Executive Action Process	11
Centralized User Authentication.....	12
Major Goals of Authentication	12
Authentication Mechanisms.....	12
Centralized Security.....	15
Problems with Decentralized Security.....	15
Understanding Centralized Security	16
Understanding Directory Services Solutions	17
Features of Directory Services Solutions.....	18
Directory Services Best Practices	19

Copyright Statement

© 2006 Realtimepublishers.com, Inc. All rights reserved. This site contains materials that have been created, developed, or commissioned by, and published with the permission of, Realtimepublishers.com, Inc. (the "Materials") and this site and any such Materials are protected by international copyright and trademark laws.

THE MATERIALS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. The Materials are subject to change without notice and do not represent a commitment on the part of Realtimepublishers.com, Inc or its web site sponsors. In no event shall Realtimepublishers.com, Inc. or its web site sponsors be held liable for technical or editorial errors or omissions contained in the Materials, including without limitation, for any direct, indirect, incidental, special, exemplary or consequential damages whatsoever resulting from the use of any information contained in the Materials.

The Materials (including but not limited to the text, images, audio, and/or video) may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, in whole or in part, except that one copy may be downloaded for your personal, non-commercial use on a single computer. In connection with such use, you may not modify or obscure any copyright or other proprietary notice.

The Materials may contain trademarks, services marks and logos that are the property of third parties. You are not permitted to use these trademarks, services marks or logos without prior written consent of such third parties.

Realtimepublishers.com and the Realtimepublishers logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners.

If you have any questions about these terms, or if you would like information about licensing materials from Realtimepublishers.com, please contact us via e-mail at info@realtimepublishers.com.

[Editor's Note: This eBook was downloaded from Realtime Nexus—The Digital Library. All leading technology guides from Realtimepublishers can be found at <http://nexus.realtimepublishers.com>.]

Business Processes

An important characteristic of successful businesses is a strong alignment of the efforts between multiple areas of the organization. This arrangement rarely occurs by itself—instead, it requires significant time and effort from organizational leaders. The end result is often the creation of processes that define how all areas of the enterprise should work together to reach common goals.

The Benefits of Well-Defined Processes

Business processes are put in place to describe best practices and methods for consistently performing certain tasks. Often, the tasks involved will include input and interaction of individuals from throughout the organization. Before delving into details and examples of processes, let's first look at the value and benefits.

There are several valuable benefits of implementing processes. The first is consistency: by documenting the way in which certain tasks should be completed, you can be assured that all members of the organization will know their roles and how they may need to interact with others. This alone can lead to many benefits. First, when tasks are performed in a consistent manner, they become predictable. For example, if the process of qualifying sales leads is done following the same steps, managers can get a better idea of how much effort will be required to close a sale. If the business needs to react to any changes (for example a new competitive product), the process can be updated and all employees can be instructed of the new steps that need to be carried out.

Another major benefit of defining business processes is related to ensuring best practices. The goal should not be to stifle creativity. Rather, it's often useful to have business leaders from throughout the organization decide upon the best way to accomplish a particular task. When considering the alternative—having every employee accomplish the task a different way—consistency can greatly help improve efficiency. Additionally, when processes are documented, new employees or staff members that need to take on new roles will be able to quickly learn what is required without making a lot of mistakes that others may have had to learn “the hard way.”

Defining Business Processes

Once you've decided that your organization can benefit from the implementation of business processes, it's time to get down to the details. You must define business processes and determine how they can best be implemented to meet the company's needs.

Deciding Which Processes to Create

An obvious first step related to designing processes is to figure out which sets of tasks to work on. At one extreme, organizations could develop detailed plans for performing just about every business function. However, creating and enforcing business processes requires time and effort, and the value of the process should be considered before getting started. Some characteristics of tasks that might be good candidates for well-defined processes include:

- Tasks that are performed frequently—The more often a process is used, the more value it will have for the organization. For tasks that are performed rarely (for example, a few steps that are carried out once per year), the effort related to defining the process might not be worthwhile.
- Tasks that involve multiple people—Processes are most useful when there is a sequence of steps that must be carried out to reach a goal. When multiple people depend upon each other to complete the task, a process can help define each person's responsibilities and can help ensure that things don't "fall through the cracks."
- Tasks that have consistent workflows—Since the goal of a process is to define the best way in which to accomplish a task, processes are best suited for operations that should be done similarly every time. Although it is possible to define processes when significant variations are common, often these processes lead to many exceptions, which can lower the overall value of the effort.

With these aspects in mind, let's look at additional details related to defining business processes.

Identifying Process Goals

As it's helpful to have a project plan or mission statement, it's important to define the goals of a process before beginning the work of defining it. Examples of typical process goals include:

- To provide an efficient method for tracking customer issues immediately after a sale.
- To increase the quality of technical support provided by the customer service desk.
- To streamline the process of payroll processing.

Effective goals will usually be concise and will focus on the *what* and *why*, instead of *how*. During the development of processes, organizations should regularly refer back to these goals to ensure that all the steps are working towards the requirements.

Developing Processes

When it comes to deciding who should be involved in developing processes, the general rule of thumb is the more, the better. Although it might be tempting for managers to take a top-down approach to defining processes or for a single business manager to document the details, it's much better to solicit the input of all those that are involved. Many operations and tasks have effects that are felt outside of the immediate realm of a single department. Therefore, it's important to ensure coordination with other portions of the business.

Specifically, there are several roles that should be represented during the creation of a process. Business leaders from all areas of the organization should be welcome. Additionally, stakeholders whose jobs will be directly affected by the process should drive the process. This might include employees ranging from hands-on staff members to executive management (depending on the scope of the process). An organized process for implementing ideas and reviewing documentation drafts can go a long way toward keeping the development process humming along. At the risk of sounding like a half-baked management fad, it's often helpful to have a process for creating processes.

Documenting Business Processes

Once the key components of a business process have been defined, it's time to commit the details to a document. A best practice is to use a consistent format that includes all the relevant details that might be needed by individuals that are new to the job role. Figure 7.1 provides some examples.



Figure 7.1: Components of a well-defined process.

Specific details include the owner of the document—the individual or group that is responsible for defining and maintaining the process. Other details include who is affected by the process, and the roles that might be required. The actual steps of the process can be defined in a variety of ways. Although text might be useful as a basis, flowcharts and other visual aids can help illustrate and summarize the main points very effectively.

Creating “Living” Processes

It's important to keep in mind that processes are rarely, if ever, perfect. There is almost always room for improvement, and organizations often have to react to changing business or technical requirements. Instead of looking at processes as fixed, rigid commandments, organizations should see them as guidelines and best practices. Ideally, the group will be able to meet periodically to review the processes and ensure that they are still meeting their goals.

Furthermore, all employees should be encouraged to make suggestions about changes. This open communication can help add a sense of ownership to the process and can help enforce it. It doesn't take much imagination to picture workers grumbling about antiquated systems and steps that make their jobs more difficult and less efficient. Rather than encouraging people to work around the system, they should be encouraged to improve the portions that don't work.

Automating Business Process Workflow

As mentioned earlier, it's common for processes to include steps that require interactions among different individuals and business units. Therefore, it should come as no surprise that organizations can benefit significantly through the use of automated workflow software solutions. These solutions allow managers to define steps that are required and to ensure that they are properly followed.

Approvals processes and workflow often require multiple people to work on the same piece of information. Tasks include reviewing the current state of the information and making comments or modifications. The changes should be visible to everyone involved in the process, and people should be sure to have the latest version of each document. The challenges lie in the ability to coordinate who has access to which pieces of a document, and when.

Many popular software packages and suites offer workflow features. For example, Microsoft's Office system productivity suite and its SharePoint Portal Server product can help make documents and other information available to teams and organizations online. Many enterprises have also invested in the implementation of enterprise resource planning (ERP), customer relationship management (CRM), or custom-built line-of-business applications. And, from an IT standpoint, data center automation tools can be used to ensure that processes related to change and configuration management, security management, deployment, and many other tasks are handled according to the organization's best practices. Regardless of the approach taken, the creation and enforcement of business processes can significantly improve the maturity and efficiency of organizations of any size.

Business Process Example: Service Desk Processes

Having already explored the benefit of business processes and characteristics that can make them successful, let's look at a specific example of a business process—the implementation of a service desk workflow. The goal is to help illustrate how organizations can create and document a common business practice to help streamline operations.

Characteristic of an Effective Process

Before diving into specific details of a service desk process, let's enumerate a few ideas to keep in mind. First and foremost, the process should be defined well enough so that all reasonable procedures are covered. Examples might include what to do in the case of an emergency, or how after-hours support calls should be handled.

Second, it's important for IT departments to communicate their processes to their users. If the turnaround time to resolve low-priority issues is 2 business days, users should be made aware of this ahead of time. Third, it is very important that at any given point in the process, at least one individual has ownership of an issue. This individual should have the authority to make decisions whenever decisions are required. A common cause of poor customer service is when a call or issue should be transferred but instead ends up in a “black hole” somewhere. (It's tempting to think that there's a place in the Universe where these calls go to commiserate).

Some fundamental rules related to documentation should also apply. Consistent use of particular terminology (along with definitions, wherever appropriate) can be greatly helpful. In the area of service desk support, clear definitions of “Level 2 Emergency” or “minor issue” can help everyone better understand their roles. Even terms such as “regular business hours” could use at least a reference to the company's standard work schedule.

Finally, wherever possible, service desk staff should be empowered to act as advocates for their callers. Although their ultimate loyalty should be to the support organization, they should also represent the needs of those that they support to the best of their abilities. Keeping these things in mind, let's move on to some examples.

Developing a Service Desk Operation Flow

Let's start by taking a look at a typical service desk process. For the sake of this example, let's focus on a scenario in which an IT call center is designed to support end users from within the organization. Let's assume that the organization supports approximately 3000 employees spread through numerous sites, and the service desk includes 35 staff members, including management.



Most of the information in this section is adaptable to organizations of just about any size.

Documenting Workflow Steps

The approach we'll take to developing a service desk process is to start with the very basics. You might imagine these first steps as something that might be scribbled in a notebook somewhere. Typical steps in the service desk process can initially be defined by the following high-level steps:

- A Service Desk Representative (SDR) receives a call and determines the nature of the problem.
- If the problem can be resolved by the SDR, assistance should be provided and the call should be completed.
- If the problem requires the caller to be transferred, the SDR should document details and transfer the call to the appropriate specialist.
- If the issue is an emergency, it should be escalated to a supervisor via email (during regular business hours) or via a phone call (outside of regular business hours).
- All other issues should be escalated to a Senior Support Representative (SSR).

Although text-based descriptions can be helpful, this example leaves much to be desired. First, it's difficult to read—it's not clear whether these steps should be performed in sequence or some decisions are exclusive of each other. Clearly, there is room for improvement. Let's continue on the path to an effective service desk business process by looking at more examples of what might be included.

Tracking and Categorizing Issues

One important aspect of providing service desk support is the requirement of always tracking all issues. Apart from ensuring that no request is ignored, this information can be vital in identifying, comparing, and reporting on common problems. Service desk staff should be made aware of common categories of problems. Table 7.1 provides basic examples.

Category	Description	Examples
Minor—Desktop	Minor computer issue that is not preventing use of the system	Intermittent application problems; non-critical or "annoying" issues
Minor—Change Request	Change to an existing system that is not preventing an employee from working	Addition of a new computer; new hardware request; physical relocation of a computer
Medium—Single System	A single computer is unavailable for use by an employee	Hard disk or other hardware failure; operating system (OS) issue
High—Multiple Systems	Multiple systems are unavailable for use	Department-level server failure; network failure

Table 7.1: Examples of service desk issue categories.

In addition, this table could include details about any service level agreements (SLAs) that the IT department has created as well as target issue resolution times. Of course, manual judgment will always be required on the part of service desk staff. Still, the goal should be to capture and route important information as accurately as possible.

Escalation Processes and Workflow

In even small service desk environments, it's likely that the organization has specialists to handle certain types of issues. In some cases, there might be multiple levels of support staff; in other cases, application experts might be located outside the IT organization. Once the nature and severity of an issue has been determined, service desk representatives should know how they should route and handle these issues. Perhaps the most important aspect is to ensure that the issue always has an owner.

Creating a Service Desk Flowchart

Once you have settled on the features to include in your high-level service desk process, it's time to determine how best to communicate the information. A flowchart is often the best way for people to visualize the steps that might be required to resolve an issue and how the steps are related. Figure 7.2 provides an example.

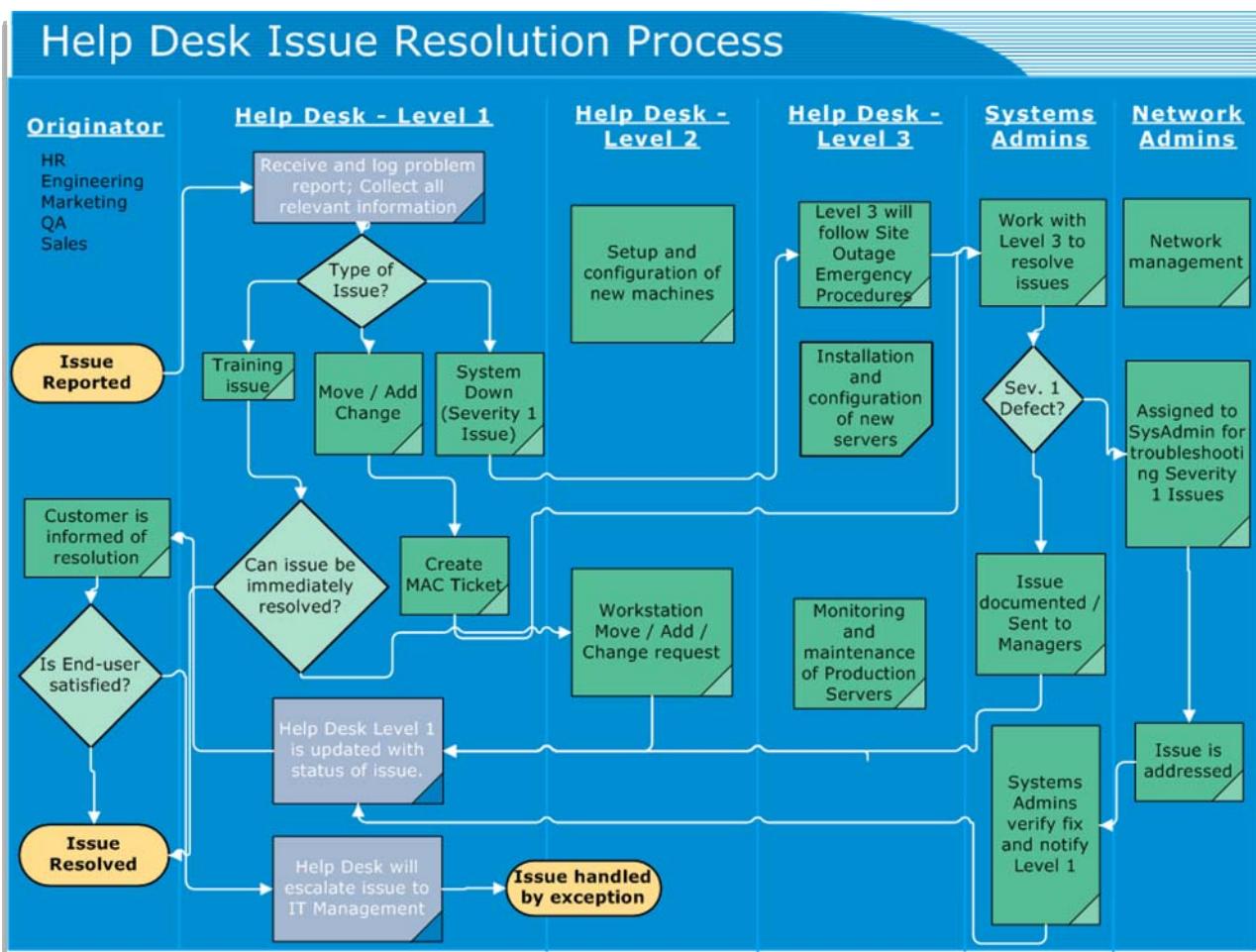


Figure 7.2: An example of a Help desk issues resolution process flowchart.

Notice that in this document, there are many decision points and branching logic that will affect the path to issue resolution. The major areas of ownership start at the left and begin with the reporting of an issue (which can be from any area of the organization). The Level-1 staff is responsible for categorizing the issues and determining the next steps. The issue may be resolved at this level or it may be moved on to other members of the staff. At all points, the issue is owned by an individual or a group. In this particular flowchart, it is ultimately the responsibility of the Level-1 staff to ensure that an issue is closed.

Although this flowchart may not be perfect, it is easy to read and provides a simple overview of many portions of the process. Most IT organizations will also want to accompany the flowchart with additional details such as definitions of terms and steps involved in procedures.

Automating Service Desk Management

Service desk workflow is an excellent example of the type of business process that can be greatly improved through the use of automation. It's important to note that there are many approaches to the task of defining service desk workflows. For example, the IT Infrastructure Library (ITIL) defines a Service Desk, and provides best practices for how IT organizations can best implement policies and processes related to issue resolution

 For more information about ITIL, see the ITIL Web site at <http://www.itil.co.uk>.

Numerous third-party products and software solutions are also available. Some products are very customizable, while others introduce their own suggested workflows, terminology, and best practices.

When evaluating potential service desk solutions, IT organizations should start by looking at their overall needs. For example, some solutions might better lend themselves to the support of customers that are external to an organization (by allowing for fee-based support and related features); others might be more appropriate for internal IT service desks. In some cases, an enterprise might decide to build its own service desk solution. Although doing so can lead to a system that is well-aligned with business goals, the time, cost, and maintenance effort required might not lead to a strong enough business case for this approach.

Regardless of the approach and the technology selected, the implementation of an organized service desk process is an excellent example of how IT organizations can benefit from the implementation of business processes.

Executive Action Committee

A challenge that is common to most IT departments is the goal of meeting organizational requirements while staying within established budgets. In addition to the ever-increasing reliance most organizations put on their IT staff, new initiatives often take up important time and resources. When reacting to demands, it can become difficult for IT management to stay on top of the needs of the entire organization. Instead of working in isolation from the rest of the business, a recommended best practice is to establish an Executive Action Committee.

Goals of the Executive Action Committee

An Executive Action Committee can help determine the course of the business and can help define the role of the IT organization within it. The purpose of the committee is to evaluate current and future IT initiatives and to make recommendations about which projects should be undertaken. The process might start by evaluating active proposals and requests as collected by the IT department. For example, the Sales and Marketing departments might have requested an upgrade of their current customer relationship management (CRM) application, while the Engineering department is looking for a managed virtualization solution to facilitate testing of a new product.

Evaluating Potential Projects

Given time and budget constraints, it's likely that some projects will either have to be cut from the list or be postponed until resources are available. That raises the question of how to decide which projects are most valuable to the organization. Standard business-related measurements can be helpful. Quantitative estimates such as return on investment (ROI) and total cost of ownership (TCO) are key indicators of the feasibility of a particular project. The quicker the ROI and the lower the TCO, the better. Other factors that might be taken into account include risks (factors that might lead to cost overruns or unsuccessful project completion) as well as available resources (see Figure 7.3).



Figure 7.3: Factors related to prioritizing projects.

An adage related to technical project management specifies that organizations can choose to define two of the following: scope, timeliness, and quality. For example, if the project deadline is most important, followed by quality, then it's quite possible that the scope (the list of included features and functionality) might need to be reduced (see Figure 7.4).



Figure 7.4: Prioritizing the goals of a particular project.

Defining Committee Roles and Members

When defining the membership of the Executive Action Committee, it's important to ensure that representation from various areas of the organization is included. Ideally, this will include senior management and executives from various business units. Because investments in IT can affect the organization as a whole, input and comments should be solicited before undertaking major projects. This process can go a long way towards having IT organizations seen as strategic business partners and good team players.

Implementing an Executive Action Process

A crucial first step in implementing an Executive Action Process is to gather buy-in from throughout the organization. Often, the potential benefit—better prioritization of IT projects—is enough to gain support for the process. In other cases, IT managers might have to start the process by calling meetings to evaluate specific projects.

The roles of committee members may vary based on business needs and particular projects that are underway. For example, if an organization is planning to invest significant resources in a new Web-based service offering, leaders from the Engineering department might be most interested in helping to prioritize projects. Figure 7.5 provides some steps that might be involved in regular Executive Action Committee meetings.

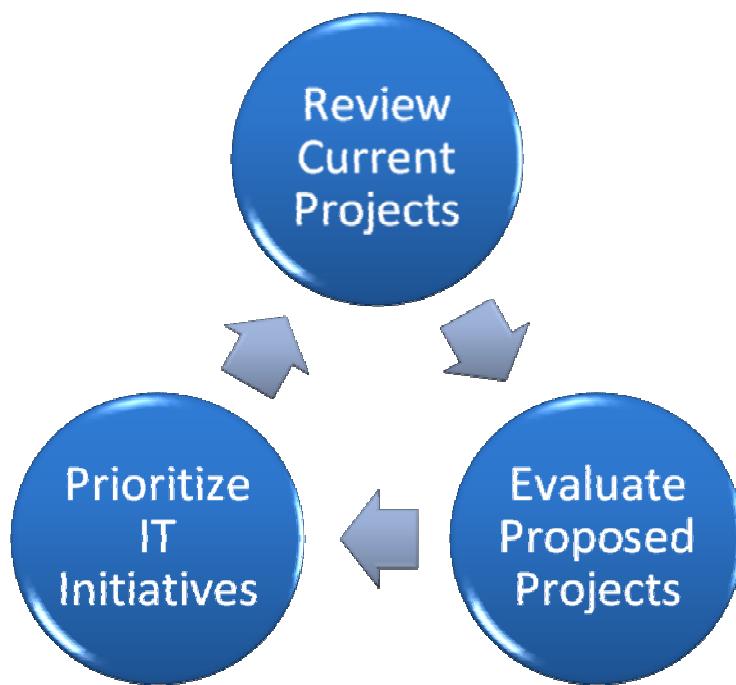


Figure 7.5: Parts of the Executive Action Committee process.

Overall, the goal of the Executive Action Committee is to better align IT with the needs of the organization. By ensuring that input is gained from throughout the organization and by prioritizing the projects that can provide the most “bang for the buck,” enterprises can be sure to maximize the value of their IT investments.

Centralized User Authentication

Taken literally, the concept of authentication refers to establishing that something is genuine or valid. In the “real world,” this is often easy enough—unless you have reason to believe that you’re involved in a complex international plot. Basic physical appearance can help you identify individuals with little room for error. Add in an individual’s voice, and it’s pretty easy to distinguish your manager from other coworkers (perhaps by identifying the tell-tale pointy hair from the *Dilbert* comic strips). The process of authentication in the technical world is significantly more complex.

Major Goals of Authentication

From the standpoint of an IT department, the primary goal of authentication is to positively identify users or computing devices and to ensure that they are who they claim to be. Based on their validated identities, systems can determine which permissions to grant (a process known as authorization). Although the primary goal is easily stated, there is a lot more to it.

Other goals of the authentication process involve minimizing the hassle and intrusiveness of security methods. If you required your users to provide authentication information every time they tried to open a file, for example, it’s likely that the reduction in productivity (not to mention the negative effects on your own life expectancy) might not make it a worthwhile implementation. With strong but user-friendly and easy-to-maintain authentication mechanisms, organizations can gain the advantages of increased security without the potential downsides. With this goal in mind, let’s look at ways in which IT departments can implement authentication.

Authentication Mechanisms

By far, the most commonly used method of computer-based authentication is through the use of a login and password combination. Although this method is relatively easy to implement, it comes with significant burdens. Users are responsible for generating and remembering their own passwords. They should choose strong passwords, but they’re often required to enter them multiple times per day.

From an IT standpoint, devices such as routers and security accounts for use by applications and services also often have passwords. Creating and maintaining these passwords can be a difficult and time-consuming process. From a security standpoint, it can also be difficult to determine whether a password has been shared, compromised, or used in an authorized way. All too often, “secrets” are shared. Considering that organizations often have many thousands of passwords and accounts, this can be a major security-related liability.

Strengthening Password-Based Authentication

An old adage states that a chain is only as strong as its weakest link—should even one component fail, the strength and integrity of the entire chain is compromised. From an IT standpoint, this means that security staff must ensure that authentication credentials are properly maintained. Some general best practices related to managing password-based environments include the following:

- Password length—IT departments should require a minimum number of characters for each password that is used within the environment. Although the specifics vary between IT environments, a minimum password length of at least six characters is a standard best practice.
- Password complexity—A common method for infiltrating computer systems is that of dictionary-based or “brute force” attacks. This approach involves either randomly or systematically trying to “guess” a password. If the potential attacker has additional knowledge (such as names of the user’s children, pets, and so on), the chances of success can be dramatically improved. To counter these methods, it’s important to ensure that passwords are sufficiently complex. The general approach is to require at least two of the following types of characters in every password:
 - Lower-case letters
 - Upper-case letters
 - Numbers
 - Special characters
- Password expiration—The longer a user account and password combination is active, the more likely it is that the account is being used by an unauthorized individual. Because there is little to prevent users from accidentally or purposely sharing passwords and it’s difficult to detect whether a login is being used by an unauthorized individual, it’s important to require passwords to be regularly modified. A typical practice might require users to change their passwords every 3 months. The authentication system can also keep a list of recently used passwords, and prevent their reuse. Finally, some systems might be able to look for similarities in passwords and disallow the change from keys like “P@ssw0rd01” to “P@ssw0rd02.”

- Account lockout policies—Unauthorized access attempts are generally characterized by having many unsuccessful logon attempts. Password-based security solutions should automatically lock an account so that it cannot be used if a certain number of incorrect logon attempts are made. Additionally, the information could be logged so that IT staff can examine the situation. To avoid administrative overhead, an automatic unlock process is often used. For example, after five unsuccessful logon attempts, the user must wait 10 minutes before again attempting to access the system. These methods can dramatically decrease the viability of brute-force attacks.
- User education—A critical but often-overlooked area related to authentication is that of end-user education. Staff members often see security as a hindrance to getting their jobs done, and they can sometimes work to circumvent certain measures. This attitude can lead to significant problems that can eventually increase the vulnerability of an entire organization's computing resources. By informing users of the value of and power of their network accounts, IT departments can gain allies in the process of securing systems.

It's also important to note that IT departments can easily go overboard in implementing security measures. Such Draconian tactics as requiring extremely long passwords or forcing very frequent password changes can often work against the goal of security. Users will often choose the path of least resistance, and may feel the need to write down their passwords in multiple places or to use easy-to-guess phrases. As mentioned earlier, all security implementations should also take into account usability and productivity issues. Perhaps most importantly, all of an IT environment's authentication policies and procedures should be documented and should be made available to members of the organization.

Other Authentication Mechanisms

Although password-based authentication is the most ubiquitous method, other methods are also available. The field of biometrics focuses on the task of identifying individuals based on biological mechanisms. Fingerprint-based identification is now available at a reasonable cost and even consumer-focused devices are available. In order for this method to work in a corporate environment, the fingerprint readers must be readily available wherever authentication takes place. Often, users will have to fall-back to "old-fashioned" username and password combinations, at least occasionally. Other biometric methods range from the use of voice-print analysis to retinal scans. The major barriers to the adoption of these methods include cost and compatibility with existing systems.

Still more authentication mechanisms involve the use of a small device that can generate regularly changing cryptographic values known as secure tokens. This mechanism adds another layer of security by ensuring that a potential user of a system is in possession of the device. Should it be misplaced or stolen, IT departments can find out quickly and cancel old credentials.

Centralized Security

So far, we've looked at several authentication mechanisms (with a focus on password-based authentication). Let's explore the process of creating and managing security credentials in a network environment. We'll focus on the importance of implementing a centralized user authentication system, but first let's look at an alternative (and the many problems it can cause).

Problems with Decentralized Security

Most new computers, operating systems (OSs), applications, and network devices have mechanisms for maintaining their own security. For example, most switches, routers, and firewalls can be protected through the use of a password. Applications might use their own set of logins and permissions, and even individual computers might have their own security settings. Figure 7.6 provides an overview of this security approach.

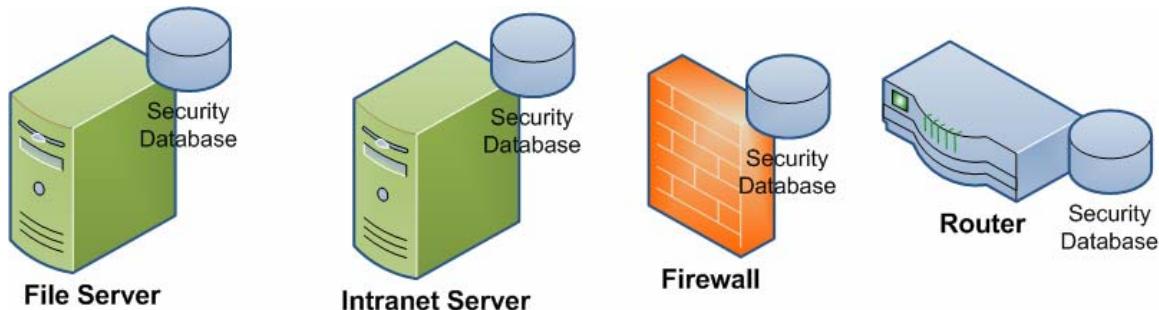


Figure 7.6: A logical overview of decentralized security.

The most important aspect of decentralized security is that there are many security databases within the organization. Each one is independent of the others and contains its own authentication information. For example, every computer might have a separate account named “SysAdmin.” Although it’s technically possible to manually synchronize the login information (that is, to ensure that the same usernames and passwords are used on each machine), the process is tedious and error-prone. Furthermore, maintaining even a few of these systems can quickly become difficult and time consuming. The end result is often that security is not maintained: Simple passwords are used, login information is changed infrequently, and passwords are often written down or recorded in some other way.

Although simply setting up a decentralized security environment can be painful, the real risks are in the areas of manageability. For example, what will happen if a password is compromised? Even if IT staff can scramble to update the passwords on multiple devices, there is still a large window of vulnerability. The new password also has to be communicated to the users that need it—an inherently risky proposition. What if one or more devices are overlooked and continue to run with the exposed authentication information? And this doesn't even take into account the effort that might be required to ensure that other computers and services that rely upon the login are properly updated.

In case all of this isn't incentive enough to see the drawbacks of decentralized security, let's look at one more motivator before moving on: Imagine the difficulty that end users will experience if they must manually log on to each device or application on the network. The decrease in productivity and frustration might be tantamount to not having a network at all. By now, it's probably obvious that decentralized security is not a very effective approach—even for the smallest of IT organizations.

Understanding Centralized Security

In a centralized security model, all security principles (such as users and computers) are stored in a single repository. All the devices in the environment rely upon this security database to provide authentication services. All accounts are created and maintained once (although many different devices might be able to perform the function). Figure 7.7 provides a visualization of this approach.

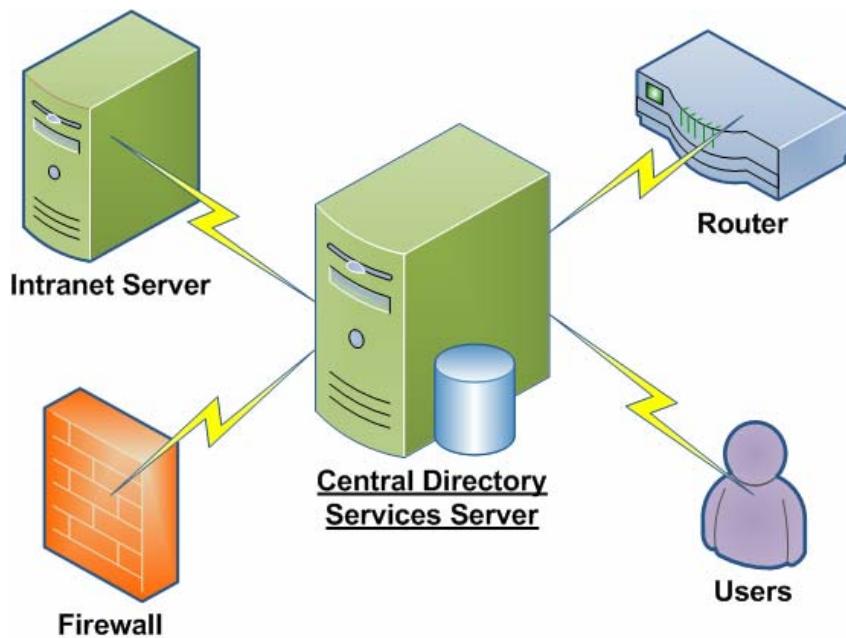


Figure 7.7: A centralized security implementation.

It's easy to see how this method can alleviate much of the pain of maintaining many separate security databases. IT administrators that are responsible for maintaining security can create accounts in the security database. And, if a password or other user setting must be changed, it can be done centrally.

Understanding Directory Services Solutions

Although the benefits of centralized security management are compelling by themselves, so far we've only scratched the surface. Several vendors offer unified directory services solutions that provide numerous additional advantages. One of the most popular solutions is Microsoft's Active Directory (AD—see Figure 7.8).

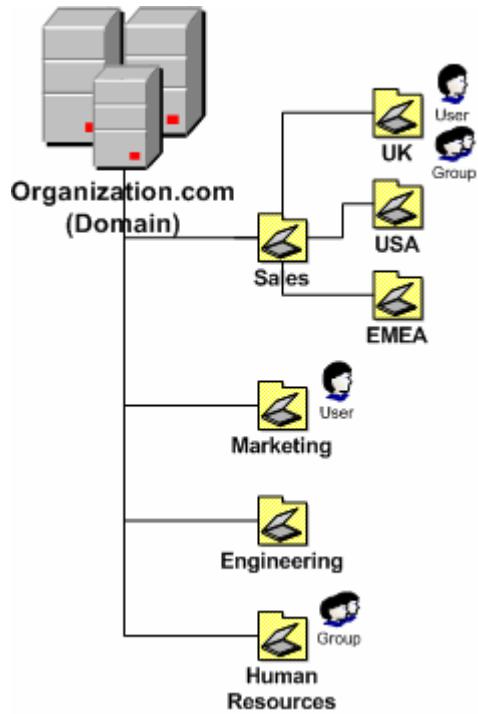


Figure 7.8: A logical overview of a Microsoft AD domain.

AD is designed to be an enterprise-wide centralized security structure that is hosted by Windows Server-based domain controllers. Although built-in authentication mechanisms can differ, practically all enterprise-based hardware, software, and network solutions can leverage AD for verifying user credentials and evaluating permissions. Microsoft's directory services solution is based on a variety of standards and technologies, including the Lightweight Directory Access Protocol (LDAP), Kerberos (for managing authentication tokens), and Domain Name System (DNS).

Setting up a complete directory services infrastructure involves many components and services, so vendors have gone to great lengths to make these systems easy to configure, deploy, and manage. In addition to AD, other vendors offer LDAP-compliant directory services solutions. One example is the Remote Authentication Dial-In User Services (RADIUS) standard that was originally intended for verifying credentials for remote users. Most of these directory services solutions can work in conjunction with AD or by themselves.

Features of Directory Services Solutions

In addition to the important feature of providing a single central security repository, centralized authentication solutions include many features that help simplify the management of user authentication. Some of the features include:

- Secure authentication mechanisms—A significant challenge related to working with password-based security is the problem of transferring password information over the network. Even if the data is encrypted, it's possible that replay-based attacks or man-in-the-middle intrusions can reduce security. Modern directory services solutions use strong authentication and key management systems such as Kerberos. Although the underlying concepts are complex, the main benefit is that actual passwords are never sent over the wire, thereby making it impossible for them to be intercepted or reverse-engineered. Best of all, when it's properly implemented, these features work behind-the-scenes without the intervention of IT staff.
- Cross-machine authentication—Most IT environments support at least a few dozen computers, and many support thousands. It doesn't take much imagination to see the problems with forcing users to authenticate at each resource. To solve this issue, directory services solutions work in a way that allows computers that are members of a domain to trust each other. As long as a user has authenticated with the security domain, the user no longer must manually provide credentials for accessing other network resources.
- Hierarchical management—Most businesses have established departments and an organizational structure to best manage their personnel and resources. Directory services solutions are able to mirror this hierarchy to provide for simplified management. Administrative containers called organizational units (OUs) are created to allow for easily managing thousands or even millions of “objects” such as users, computers, applications, and groups.
- Management tools—Directory services solutions generally provide well-designed graphical tools to manage security settings and accounts. Although IT staff will have no problem using them, some operations can even be handed down to non-IT staff (such as managers or Human Resources staff). By delegating the management of user accounts to trusted individuals, IT departments can ensure that their security database is kept up to date. And, through the use of scripting and programmatic automation, many of the most common tasks can be greatly simplified.
- Application and device support—Third-party applications and hardware devices can take advantage of directory services solutions to authenticate users. This setup alleviates developers from the difficult task of creating secure logon mechanisms and reduces the potential liabilities of security issues for the IT department. Furthermore, as there is generally only a single account per user, IT departments can centrally enable, disable, or modify permissions from within a single security database.

Though this basic list of features of directory service solutions is a long one, it only scratches the surface of the full potential.

Directory Services Best Practices

Taking advantage of directory services solutions is usually a straightforward process. There are, however, some important aspects to keep in mind. First and foremost, enterprise IT staff should look for management solutions, software, and hardware that work with the directory solution that they have implemented. By leveraging the advantages of the directory, IT organizations can lower costs and improve security. The same applies for custom software development: Internal developers should ensure that line-of-business applications adhere to corporate IT standards and that they work with the directory services solution.

Finally, it's important for IT departments to develop, document, and enforce policies related to their security implementations. Processes for creating new user accounts, handling employees that are leaving, and performing periodic security checks are vital to ensuring the overall health and benefit of the directory service.

Overall, directory services solutions can dramatically improve security and reduce administration related to a difficult technical and organizational challenge—managing user authentication. This should make them a vital part of the core infrastructure of all IT departments of any size.

Download Additional eBooks from Realtime Nexus!

Realtime Nexus—The Digital Library provides world-class expert resources that IT professionals depend on to learn about the newest technologies. If you found this eBook to be informative, we encourage you to download more of our industry-leading technology eBooks and video guides at Realtime Nexus. Please visit <http://nexus.realtimepublishers.com>.