



Active Directory Benefits for Smaller Enterprises

Microsoft Corporation

Published: September 2004

Abstract

Microsoft® Active Directory® (AD) has been available since early 2000, and while most organizations have completed their AD deployment and are realizing the many business benefits of having deployed Active Directory, there are still organizations that have either not completed their deployment or have yet to take advantage of some of the important features of Active Directory that yield the greatest business benefits.

This whitepaper is designed to help small and medium-sized organizations understand the business advantages that can be realized quickly and easily through the use of Windows Server 2003 and Active Directory. This paper was written based on feedback from hundreds of business executives on the reasons they chose to migrate to Active Directory, and the ongoing benefits they have realized.

Microsoft®

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2004 Microsoft Corporation. All rights reserved.

Microsoft, Windows and Active Directory are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Contents

Introduction	1
What is Active Directory?	1
Benefits of Active Directory and Windows Server 2003	2
Increasing the Productivity of Users	3
The Power of Group Policy	3
Windows Update Services	4
Remote Assistance	5
System Quarantine	5
Reducing the Burden of IT Administration	6
Server Performance and Reliability	6
Administrative Benefits of Group Policy	6
Remote Installation Services	7
Remote Administration	7
Improving Fault Tolerance to Minimize Downtime	8
The Distributed File System	8
Volume Shadow Copy Service	9
Advanced Server Recovery	9
Enhancing Security to Provide Better Peace of Mind	10
File-Level Encryption	10
IP Security	10
Improved Management Tools	11
Configure Secure Servers	11
Leveraging the Capabilities of Active Directory-Enabled Applications	12
Benefits of Exchange 2003	12
Improved Systems Management with SMS 2003	12
Integrated Capabilities with Third Party Applications	12
Conclusion	13
Related Links	14

Introduction

Microsoft® Active Directory® (AD) has been available since early 2000, and while most organizations have completed their AD deployment and are realizing the many business benefits of having deployed Active Directory, there are still organizations that have either not completed their deployment or have yet to take advantage of some of the important features of Active Directory that yield the greatest business benefits.

This whitepaper is designed to help small and medium-sized organizations understand the business advantages that can be realized quickly and easily through the use of Windows Server 2003 and Active Directory. This paper was written based on feedback from hundreds of business executives on the reasons they chose to migrate to Active Directory, and the ongoing benefits they have realized.

What is Active Directory?

Active Directory is the integrated, distributed directory service that is included with Microsoft Windows Server 2003 and Microsoft Windows 2000 Server. Integrated with Active Directory are many of the applications and services that previously required a separate, distinct directory and userid/password to be managed for each application or service. In Windows NT 4.0, for example, a directory was required for the domain itself, a separate directory for Exchange mailboxes and distribution lists, and separate directories for remote access, database, and other applications. In some cases, separate passwords were required for each application. With Active Directory, the administrator of the organization can add a user to Active Directory and through that single entry enable remote access to the network, enable the same user account for Exchange messaging, that same user for database access for accounting, client relationship management, or other applications. Not only is it possible to use Active Directory as a multi-purpose directory in this fashion but by doing so a company enables single sign-on for its users. Once a user logs in to Windows their Active Directory credential is the key that will automatically unlock all of the applications or services that they have been enabled for, including 3rd party applications that utilize Windows integrated authentication.

By creating a link between user accounts, mailbox accounts, and applications, Active Directory simplifies the task of adding, modifying, and deleting user accounts. When an employee gets married and changes their name, a single change in Active Directory can change the user information for all applications and services. When a user changes their password in Active Directory, they do not have to remember different passwords for their other applications. When a group of users is created such as the "sales group," users can e-mail the group to send a message to all users, administrators can allow security access to resources based on the group name, and users can look-up members of a group by expanding the group information. This is just one example of how Active Directory simplified many administrative tasks and processes that, in the past, involved disparate applications, servers, and services.

Benefits of Active Directory and Windows Server 2003

Windows Server 2003 and Active Directory help small and medium size organizations with a reliable working environment for the end-users, which offers the highest levels of reliability and performance so users can get their work done as efficiently as possible, as well as providing a more secure and manageable environment to make the lives of the IT staff easier.

The following sections will review the advantages of Active Directory in these areas:

- Increasing the Productivity of Users
- Reducing the Burden of IT Administration
- Improving Fault Tolerance to Minimize Downtime
- Enhancing Security to Provide Better Peace of Mind
- Leveraging the Capabilities of Active Directory-enabled Applications

Many clients running older operating systems find their current systems simply not capable of meeting the expectations of their business for a reliable, dependable, secure, or manageable environment. While many organizations have gotten creative at workarounds and adding in a number of add-ons and utilities to “make do” with their current investments, Windows Server 2003 and Active Directory provide the out-of-the-box functionality organizations need to effectively and efficiently run their businesses.

As an example, organizations that need to meet data encryption and information privacy requirements to meet the government regulations of Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), and Sarbanes Oxley can purchase costly third-party add-ons for their older operating system environments and messaging system, or the organization can migrate to Windows Server 2003 and Exchange 2003 and take advantage of the encryption, security, and privacy components that are built-in to these products.

Even something as simple as patching and updating systems can become overly complex when performed through third-party add-ins, scripting, or other tools with older operating systems. These processes can be simplified with the tools included with Windows Server 2003 which can be utilized to automatically perform system updates.

Organizations that have completed their migration to Windows Server 2003 and Active Directory have been able to realize how much time they spent keeping their old networks marginally operational, and appreciate the dramatically minimized administration time and effort required for the new environment while also seeing significant improvements in user productivity.

Increasing the Productivity of Users

In the past, system upgrades were frequently conducted for the sole benefit of specific feature and function benefits. However, as organizations seek to improve their competitive advantage and business effectiveness in the marketplace, they are turning to improvements in user productivity as a driving factor to support the investment in technology upgrades.

This section focuses on some of the ways organizations have been able to leverage the capabilities of Windows Server 2003 and Active Directory to tangibly improve the efficiency in employee tasks, and enhance employee productivity.

The Power of Group Policy

Group Policy in Active Directory allows a network administrator to centrally configure and administer system, user, and application settings. Some might think that if an administrator can make a single configuration setting from their administration console that applies to one, a few, or all users, that the function benefits only the network administrator. However, organizations that have migrated to Windows Server 2003 and Active Directory have realized that the ability for network administrators to leverage the capabilities of Group Policy to change system settings from a centralized location. This allows the network administrator to make changes faster and improve network functionality without requiring user intervention to invoke changes. Not requiring user intervention means users do not lose productivity.

As an example, Group Policy can be used to push out a software update or utility to a group of user workstations. After pushing the application, another Group Policy can be used to set user settings such as home directories, default settings, or configuration settings. By using Group Policy to push out the software and customize the configuration settings, an administrator can add functionality literally in minutes. In the past, the administrator would have to find the time to walk to every computer system, interrupt the user, install the software update, and make setting changes. Because of the time and effort to perform a relatively simple task, but multiplied by dozens of users, network administrators frequently chose to not deploy updates or add-ins because of the effect on user productivity, or the complexity.

Additionally, instead of having a network administrator spend an entire week walking from computer to computer to install an update or make system configuration changes, the administrator can now spend the available time providing help desk services, assisting users, upgrading other systems or services, and work on additional tasks that can help improve user productivity.

If the administrator experiences problems with an update or configuration, just as quickly as the administrator invoked a Group Policy to install the update, the administrator can invoke another Group Policy to uninstall the update.

Group Policy may be implemented completely without user interaction. Some of the tasks that administrators can invoke through Group Policy that helps improve user productivity include:

- **Creating Standardized Configurations, Settings, and Options:** Group Policy allows an administrator to create a series of templates that can be used to establish standard system configurations. Rather than having all computers unique in the environment, standard configurations allow users to easily “roam” between systems. In the event that a user’s computer is not working, they can simply walk up to any other available system, logon, and have the exact same access to network files and applications, and even maintain personal favorites, screensaver settings, and unique profile configurations.

- **Automatic Access to Local Resources:** Through the use of site level policies, organizations with limited IT and Help Desk administration personnel are able to assist mobile users more easily access local network resources without complicated system configuration settings. Group Policy can be used to identify the site and segment that a user has plugged their system in to, and automatically default the user to the nearest printer or file server share.
- **Enabling Features and Functions On the Fly:** Group Policy may also be used to lock down and even hide functions that users do not need to access, thus simplifying the user's desktop and experience at running software applications and utilities. This simplification of system configuration decreases the learning curve for new users, and it also prevents more sophisticated users from accidentally running applications or mis-configuring their system. At any time, the administrator of the network can quickly enable features or functions to add capabilities back to a system if needed.
- **Roaming User Profiles and Redirected Folders:** Roaming user profiles provide the ability to store unique user information such as user favorites, screen saver settings, application icons in a central location that can then be used by the user to get the exact same settings on any other similarly configured system on the network. The ability for users to roam from system to system provides users the ability to sit down at any computer in the office and access the network with the same settings as the system they may normally work from. This common configuration process also serves as a desktop fault tolerance function where users never have to wait for a system to be fixed, repaired, or replaced. A user can simply walk up to any other system on the network and logon. Administrators can also avoid having to spend an entire afternoon rebuilding a brand new system for a user, by having a couple of spare systems available that can be quickly swapped for a user's system.
- **Offline Folders:** With the addition of the offline folder capability in Windows XP that can be enabled by Group Policy, a user can have full access to their network files if they are disconnected from the network. When a user is working on a laptop computer and is traveling and needs access to files, or if the network server or LAN connection fails, the user can still access a copy of the files replicated to an offline folder on their system. When the user reconnects to the network, or when the network comes back online, any modified files will automatically synchronize between the client system and the appropriate servers.

Windows Update Services

Patched and updated systems prevent users from getting viruses or worms that can have dramatic impact on user productivity and potentially the loss of critical information from a workstation or network drive.

Windows Update Services (WUS) enables organizations to control which patches and updates are automatically downloaded and installed on the client workstations and network servers. WUS has the ability to deliver updates for all Microsoft products to help ensure that the desktops, laptops, and servers on the network stay up to date with the approved patches and updates that IT decides to distribute. A quick and automated software update system enables network administrators to quickly deploy updates without having to walk to every computer on the network every time an update is released. Instead of having scarce IT resources walking from computer to computer a simple centralized deployment function through WUS can initiate the update automatically. The administrator of the network can choose to deploy updates a few at a time, a department or site at a time, or in any scheduled deployment strategy desired. You can control which server each Windows client should connect to as well as schedule when the client should perform all installations of critical updates via Group Policy and Active Directory.

To help minimize the impact on the user community, Windows Update Services can be configured to silently install the updates without user notification or interaction. If a reboot is not required after installation the user will not be interrupted and won't even know the updates have taken place. If a

reboot is required after the download, Windows Update Services groups the installation of patches to consolidate multiple reboots into a single reboot.

WUS will also scan systems for missing updates, simplifying the detection of missing patches and allowing administrators to easily determine which systems need to be updated and which updates need to be deployed to the target systems.

Remote Assistance

Remote Assistance is a new feature in Windows Server 2003 and Windows XP that allows a user to request assistance from an administrator or support resource to help with technical issues they are encountering. The support resource can be granted the ability to remotely control the desktop and take control of the system to perform troubleshooting and administrative tasks, without having to be physically at the user's keyboard. This is especially useful when supporting users who might be at their home office, or in another building. Many organizations with limited IT staff find this to be a great time saver for the support of personnel as they spend less time on each support incident. It also allows companies to reduce travel costs and enables user problems to be fixed faster. Active Directory can easily enable, configure and manage this capability across a company's desktops and servers.

System Quarantine

Establishing an automated system to isolate users that potentially can impact the stability of the network, overall network performance, and possibly cause data to be lost or damaged greatly improves the confidence users have in the reliability of the network, and maintains user productivity as they complete their daily tasks. Active Directory can be used to set up the policies related to this feature. Additionally, AD acts as the quarantine's RADIUS server.

Network Access Quarantine Control, available in the Windows Server 2003 Resource Kit, can be used to delay remote access (VPN connection) to an organization's network until the remote system has been examined and validated for proper patches, updates, and anti-virus signature files. When a user tries to connect to the network, the user can be authenticated and assigned an IP address, but the connection is placed in quarantine or isolation mode, and is only given limited network access. A script is then run on the computer and if it verifies the computer is running an approved configuration then the quarantine mode is removed and the computer is granted normal access to the network resources. By testing and validating systems for the most recent updates and anti-virus definitions, organizations can be spared problems from users who remotely connect to the network and inadvertently spread viruses and worms through their remote VPN connection.

Reducing the Burden of IT Administration

This section highlights how the benefits of Windows Server 2003 and Active Directory help reduce the amount of administration time and effort needed to maintain a network. The reduction in IT administration burden translates to more IT time spent testing and implementing more critical business solutions that can benefit users instead of spending time rebooting servers or manually managing individual servers throughout the enterprise.

Server Performance and Reliability

A fundamental way that network administrators and IT managers can benefit from an upgrade to Windows Server 2003 and Active Directory is in the area of server performance and reliability. While some might think that server performance improvements such as doubling the performance of Windows file services access between Windows Server 2003 and Windows 2000 only translates to potentially faster user access to files, many small and medium business have found the increased performance of Windows Server 2003 enabled the organization to decrease the number of servers on the network. With fewer servers to manage and administer, not only has the organization decreased its ongoing cost for hardware, software licenses, and maintenance contracts, but it also decreases the number of systems the IT department needs to manage and administer on a regular basis.

Server stability has been enhanced and Windows Server 2003 has proven to virtually eliminate unexpected server failures (commonly called “blue screens”). Additionally, with improvements in the Windows Server 2003 operating system, system patches, updates, and configuration changes require fewer server reboots and can, in many cases, be installed automatically. This allows an organization to perform many needed system changes without having to interrupt system operations, and it is more likely that the latest patches and fixes will be implemented in a timely basis, improving the resiliency of the environment.

New hardware technology now provides the ability for network administrators to swap out PCI network adapters, faulty memory modules, and even faulty power supplies without interrupting server operations. Windows Server 2003 fully supports the new hardware fault tolerance and hot swappable capabilities that greatly improve an organizations ability to keep a network system running around-the-clock.

Administrative Benefits of Group Policy

While Group Policy was addressed earlier in this paper as having significant benefits at improving the productivity of users of a network, there are also significant administrative benefits of Group Policy to IT administrators in an organization.

Many of the administrative tasks of Group Policy fall in the area of meeting the compliance requirements of current government laws and regulations. In order for an organization to demonstrate compliance with laws and regulations, the administrators of the organization need to match technical policies with business policies.

Group Policy enables network administrators to centrally manage, audit, and report on the adherence to organization policies. Some of the policies include:

- **Password Policies:** A Group Policy can be created to enforce password history (how many passwords are remembered), maximum password age in days, minimum password length in characters, and whether passwords must meet specific complexity requirements. By creating

and enforcing password policies for the organization, the administrators of the network can ensure an appropriate policy has been set for the organization to meet the standards and requirements expected of the organization.

- **Software Restriction Policies:** A Group Policy can be created to enable an administrator to set policies that restrict access and/or execution of application software. For example, if the organization is concerned about users receiving viruses through e-mail, a policy setting can be applied that does not allow certain file types to be executed on a system. That way if there is a known virus on the network, the software restriction policy settings can be used to stop computers from opening the file that contains the virus. The ability to allow and deny user access to certain applications help an organization meet its obligation to comply with applicable laws and regulations.

Remote Installation Services

Windows Server 2003 includes an imaging-deployment product called Remote Installation Services (RIS) which allows administrators to configure both server and desktop images that can be deployed “over the wire” to a destination server or workstation. This means that a standard configuration can be created for different types or groups of users (such as Sales, Marketing, Research, and Accounting) and then installed from a RIS server to that department’s desktop PCs. This can greatly reduce the amount of time taken to configure new workstations for new employees, or to re-image a server in the event that a new system or a replacement system is needed.

RIS also provides the ability to create a backup image of an existing system. By running the “RIPrep” utility, the administrator can image Windows 2000 or XP workstations, or a Windows Server 2003 server to a RIS server. In the event that the system fails, becomes corrupt, or the system just needs to be replaced, a brand new hardware system can be purchased, and a network boot (typically pressing F12 on system boot up) will prompt the RIS server to display the various images that can be installed on the new system. Without the hassle of even loading on tape software or installing application software or data, a RIS image installation can tape all of the information that used to be on a system and copy the image directly on to a new system. This function of RIS allows an organization to develop a quick new system imaging process, and even provides administrators the ability to re-image a users system based on an exact copy of the user’s system configuration as of the last time the system’s image with captured to the RIS server.

Remote Administration

Remote Desktop for Administration, formerly known as Terminal Services Remote Administration mode, allows administrators to log on to a Windows Server 2003 system remotely and view a graphical interface just as if the administrator were logging in locally. This functionality provides an administrator the ability to perform system updates, enact server changes, and install or update components on a server system without having to sit at the server console.

This ease of administration and management allows for faster response to server tasks, and allows an administrator to support more servers since the administrator does not need to physically be where the servers reside to perform the administrative tasks necessary to manage the network.

Improving Fault Tolerance to Minimize Downtime

Features available in Windows Server 2003 also help organizations meet the demands and expectations of a nonstop networking environment. However rather than purchasing third party add-ins to achieve data redundancy and system recoverability, Windows Server 2003 and Active Directory have built-in technologies that help organizations with their business continuity initiatives straight from a standard Windows Server 2003 Active Directory environment.

When many organizations hear about nonstop networking, they envision an environment with expensive Storage Area Network (SAN) devices, clustered servers, or special server configurations that provide data and system fault tolerance. However Windows Server 2003 and Active Directory include several technologies that provide fault tolerance, but without the high cost associated with other technological solutions. The technologies highlighted in this section include:

- Distributed File System (DFS)
- Volume Shadow Copy Service (VSS)
- Advanced Server Recovery (ASR)

With these technologies, an organization can use standard server equipment, typically the equipment currently being used, to create a more redundant network environment

The Distributed File System

The Distributed File System (DFS) provides an organization the ability to store files to a logical shared directory where the information is distributed, stored, and even duplicated to multiple backend file servers. For example, when a user accesses [\\companyabc.com/files](#), they may actually be connecting to one of a number of servers ([\\serverA\\drive](#), [\\serverB\\drive](#), and [\\serverC\\drive](#)). By having a single logical directory that is not directly associated with a specific server, if a server system is offline or has failed, the user could be directed to a mirror copy of the information stored on another server hosting the DFS data. Since the namespace makes file paths transparent from a user's perspective, the user never knows that the primary copy of the data is no longer available. The automatic redirection of the user to a mirrored copy of the information provides the user uninterrupted access to their data.

Network administrators purposely use the distributed nature of DFS to perform routine maintenance tasks on DFS servers without having to disconnect users from their access to their information. When a server is running out of disk space, a new server can be added to the DFS server tree, the administrator can drag and drop files from one server to another server, effectively evacuating data off of a server running low on disk space to a new server that was configured with additional disk space availability. Since the users never directly connected to the original server, the movement of files from one server to another never impacts the users. Their connection to the main DFS directory remains constant even though the data now resides on a different physical system.

The same process can be used to move data from an old failing server to a new server should a server replacement rotation be necessary at migrating data from one system to another.

In addition to merely providing redundancy to data in a DFS environment, mirrored copies of information can be used to leverage the site locality capability of an Active Directory integrated DFS

When DFS is implemented in conjunction with Active Directory, DFS ranks all available client-server connections by the site link cost function defined in Active Directory to identify the closest server to the user accessing the information. If a mirror copy of data that a mobile user is trying to access resides on multiple servers, as the user changes between offices, the user will retrieve the copy of the mirrored information that is on a server closest to them.

DFS provides organizations running Windows Server 2003 and Active Directory a distributed and replicated data environment that enables access to a mirrored copy of information based on the location of the user. Many organizations want this level of data fault tolerance and have considered purchasing very expensive external storage systems and data mirroring utilities to achieve this level of fault tolerance when the technology is built-in to Windows Server 2003 and Active Directory.

Volume Shadow Copy Service

Volume Shadow Copy service (VSS) provides file recoverability and data fault tolerance that eliminates the need for IT to undelete lost or corrupted user data. Volume Shadow Copy takes a snapshot of a network volume and places the copy onto a different volume on the network, allowing read-only access to those files, and enabling the recovery of data from these copies if needed. Thus if a user accidentally overwrites an important file, instead of asking IT to restore the information from tape, the user can easily choose to recover a previous snapshot version of the file themselves.

VSS and its undelete capability provides a significant benefit to users where they can recover previous versions of their files without having to ask IT to recover the file, or place the burden, or blame the delay in completing the requested task, on IT. This not only saves a lot of people time, but also improves user satisfaction when they can perform basic recovery tasks without having to submit a request or call the helpdesk.

Advanced Server Recovery

Another feature of Windows Server 2003, Advanced Server Recovery (ASR), facilitates the restoration of a failed server, and reduces the amount of time an administrator needs to spend building and reconfiguring a new server. ASR is a system recovery utility that allows a server administrator to rebuild a failed server without having to reinstall and reconfigure the operating system. ASR effectively takes a snap-shot of a server, including the operating system, specific system configuration parameters, and even hard drive stripe set information and stores the information for future recovery. In the event of a server failure, assuming the replacement server has the exact hardware configuration; ASR can be used to rebuild the system as it was before the failure.

By using these tools, all included with Windows Server 2003 and Active Directory, a small or medium business can enhance the level of fault-tolerance at the file system level without purchasing any additional third-party hardware or software. DFS makes it easier for the end users to access the data they need while facilitating administration and maintenance of the data, while VSS and ASR assist in data and server recovery situations. Combine these tools with the ability of Windows Server 2003 to use a fewer number of servers to perform the same tasks as on the legacy operating system, and the organization could have the same number of servers as before, but now additional servers are available to provide enhanced fault tolerance and disaster recovery roles.

Enhancing Security to Provide Better Peace of Mind

Security in Windows Server 2003 has been dramatically enhanced to meet the requests of the user community and provide a solid defense in the increasingly hostile internet connected environment. Windows Server 2003 has been made more secure by default upon installation, and there are a number of tools which facilitate applying additional levels of security to the server and the network environment to meet the stringent rules and regulations of current government laws.

While security is one of the most important responsibilities a network administrator needs to consider, very few organizations allocate specific budget for and fund security projects. This makes Windows Server 2003 and Active Directory an important factor in helping organizations achieve the goal of having a more secure environment without having to specifically allocate funds for a security project.

File-Level Encryption

File-level encryption is the ultimate defense against unauthorized or undesired access to data. While someone can potentially gain access to a file server through unauthorized access, if the data stored on the server is encrypted, the individual may be able to download files, but will be unable to open or access the content of the files unless they have a key to decrypt the data.

Encrypted File System (EFS) is especially useful for securing sensitive data on portable computers. For example if a laptop is stolen and the thief removed the hard drive and attempted to read the encrypted files on another computer, they would not be accessible. This type of encryption has satisfied many organizations requirements to comply with current laws and regulations on data encryption and information privacy such as HIPAA, California SB-1386, and FISMA.

With Windows Server 2003 EFS encrypted data and Windows XP EFS encrypted hard drives, information can be copied from a server to the client system, or from the client system to a server and retain the encryption through the process. Maintaining encryption provides administrators the confidence that information is stored, managed, and accessed with the likelihood that the integrity and privacy of the information will not be compromised.

IP Security

IP Security (IPSec) is a mechanism for establishing end-to-end encryption of all data packets sent between computers. IPSec is built-in to Windows Server 2003 and literally takes an administrator just a few minutes to configure a server to send all communications out of the network adapter in a 168-bit encrypted format. The only individuals that can access the IPSec enabled server are users that have workstations running Windows XP that have been issued a certificate from the encrypted server to access the data stream.

With a matched client and server encryption connection, users can be assured that the conversations and data transmitted between the IPSec server and client system are as private and secure as possible. Additionally, IPSec ensures that messages are not modified in transit and are unreadable to network intruders. IPSec is useful for securing servers and workstations both in high-risk Internet access scenarios and in private network configurations for an enhanced layer of security.

Organizations need to comply with privacy and security regulations- like HIPAA - can either purchase software that provides encrypted communications, or they can upgrade to Windows Server 2003 and enable the built-in IPSec encryption. Even organizations that do not have specific laws and regulations

that require compliance need to create an environment that ensures employees of the privacy to their information and limits unauthorized access to data.

Improved Management Tools

Windows Server 2003 includes a wide range of management tools for administrators to more easily support the networking environment. Tools that include log tracking, intruder alerting, policy enforcement, and patch update status help administrators better understand the operations of the network to proactively address network problems, errors, or concerns.

Being more proactive with the administration and management of the network circumvents potential security risks and network failure problems that impact employee productivity and potential data loss. Windows Server 2003 and Active Directory provide distributed and delegated levels of administration and management, through the use of the Delegation of Control Wizard (DoC Wizard), so that an organization can assign common tasks to department managers or other personnel for functions like password resets, assigning department level security, reset print queues, or scan for security vulnerabilities. By distributing administration tasks on an as needed basis, the organization can be more proactive to potential problems, and can quickly respond to system problems.

Configure Secure Servers

Windows Server 2003 provides installation and configuration wizards that help administrators install the appropriate tools and services without having to manually choose the components blindly. By default, Windows Server 2003 has most services disabled or not installed. This helps organizations specifically choose which components they wish to activate for their specific server need. The Configure Your Server (CYS) Wizard tool assists the administrator to choose a server template such as File Server, Print Server, Web Application Server, Domain Controller, or the like and configures the services that are required.

By locking down a server by default, an organization does not have to worry about security attacks to components that are not even installed or activated on the server because they aren't even used on the system. By decreasing the footprint from which a security attack can occur, the organization minimizes the potential for network services interruption due to a failed or attacked system.

Leveraging the Capabilities of Active Directory-Enabled Applications

In addition to all of the benefits built-in to Windows Server 2003 and Active Directory, organizations have also found the newer Active Directory integrated applications like Exchange 2003, Systems Management Server (SMS) 2003, and third party accounting, ERP, and CRM applications provide significant improvements in employee productivity, key application reliability, and operational efficiency.

Benefits of Exchange 2003

For organizations using an older version of Exchange, the benefits of upgrading to Exchange 2003 adds to the list of benefits for upgrading to Windows Server 2003. Some of the major benefits organizations have found as reasons to migrate to Exchange 2003 include:

- **Outlook Web Access 2003:** Exchange 2003 includes a Web view of a user's mailbox that has the same look and all of the core functionality and capabilities as a full version of the Outlook client. This includes access to calendar, contacts, to-do lists, and public folders. Additionally, Web access users have access to a built-in spell checker, rules and filters, drag and drop capabilities, ability to view calendars of other users, and an increase in performance two to three times over earlier versions of the Web client.
- **Server and Site Consolidation:** Exchange 2003 Enterprise Edition provides the ability for a single server to host 20 Exchange databases instead of just one database in Exchange v5.5. Combined with the sophisticated Outlook Web Access client, organizations are even consolidating smaller sites into centralized sites. These two functions typically allow an organization with multiple Exchange servers to consider consolidating mailbox servers to decrease the number of systems needed to maintain, manage, and support. Fewer servers decrease administration and management costs, but also allow an organization to add servers for better reliability and performance, thus improving the user experience to the messaging system.
- **Integrated Messaging Security:** Exchange 2003 includes the ability to encrypt email messages to maintain confidentiality and privacy of email communications. Exchange 2003 also includes the ability to envelope and journal messages to keep encrypted copies of messages to ensure the message that was sent remains to be the message ultimately received and viewed by message recipients.

Improved Systems Management with SMS 2003

Systems Management Server 2003 (SMS 2003) integrates directly with Windows Server 2003 and Active Directory to assist an organization with a proactive means to install software and make changes to client and server systems. As a significant upgrade to previous versions of SMS, the new SMS 2003 simplifies the management of systems by leveraging the directory, user, group, organizational unit, and site capabilities of Active Directory.

With the integration to Active Directory, an organization can leverage the design and implementation of their Active Directory to improve the management, system update, and client and server management system of their network.

Integrated Capabilities with Third Party Applications

In addition to Microsoft's Exchange 2003 and SMS 2003 as Active Directory integrated applications, many third party vendors that make accounting, finance, client relationship management, and ERP applications take advantage of the capabilities of the Active Directory. Applications that directly integrate with Active Directory enable organizations to enable access, secure connections, modify access rights, and disable access capabilities to the Active Directory enabled applications.

Conclusion

This whitepaper covered a selection of the features and capabilities built-in to Windows Server 2003 and Active Directory that provide significant benefits to organizations looking to increase user productivity, lower ongoing cost of operations, simplify administrative tasks, and improve the security and reliability of their information technology systems. Organizations that have already migrated to Windows Server 2003 and Active Directory have found their IT staff spends less time keeping their network operational, and more time improving the functionality of their network to improve employee efficiency and business effectiveness through the simplification of automated and centralized administration tools and technologies.

Additionally, organizations have found the integrated tools and technologies in Windows Server 2003 and Active Directory for encrypted communications and policy implementation provide users with the ability to enhance the privacy and security of stored information and communications, and enable administrators to easily install applications and configure the applications without having to visit each computer on the network.

As organizations become more dependent on their networks, having built-in data mirroring and fault tolerance technologies to maintain system uptime, combined with the ability for users to recover previous versions of their files greatly simplifies the task of data restoration.

Organizations that have migrated to Windows Server 2003 and Active Directory have been able to increase user productivity, simplify daily tasks, improve reliability and integrity of their data, and ensure the storage, access, and communications on the network are kept as private and secure as possible.

Related Links

For the latest information on Active Directory: <http://www.microsoft.com/AD>

For the latest information on Group Policy: <http://www.microsoft.com/grouppolicy>

Migrating from Windows NT 4.0 to Windows Server 2003 – A Guide For Small & Medium Enterprises:
<http://www.microsoft.com/downloads/details.aspx?familyid=e92cf6a0-76f0-4e25-8de0-19544062a6e6&displaylang=en>

Using Group Policy to manage users' desktop environments:
<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/management/cswws2003.mspix>

Windows Update Services & SMS 2003 information:
<http://www.microsoft.com/windowsserversystem/sus/wuscomparison.mspix>

Information on Group Policy & Group Policy Management Console (GPMC):
<http://www.microsoft.com/downloads/details.aspx?FamilyId=D26E88BC-D445-4E8F-AA4E-B9C27061F7CA&displaylang=en>

Distributed File System (DFS):
<http://www.microsoft.com/windowsserver2003/techinfo/overview/dfs.mspix>

For an excellent article describing the functionality of Network Access Quarantine Control:
<http://www.microsoft.com/technet/community/columns/cableguy/cg0203.mspix>

Numerous case studies are available for Active Directory and related technologies:
<http://www.microsoft.com/resources/casestudies/FindCaseStudy.aspx>

For the latest information about Windows Server 2003, see the [Windows Server 2003 Web site](http://www.microsoft.com/windowsserver2003) at <http://www.microsoft.com/windowsserver2003>.

