



Coexistence of Windows Server 2003 and Windows NT 4.0

Microsoft Corporation

Published: November 2002

Abstract

Microsoft® Windows® Server 2003 offers many benefits when used in a Windows NT® 4.0 domain, whether as a file and print server, a Web application server, a remote access server, or for core services consolidation. Because Windows Server 2003 reaches new levels of performance, reliability, and security, it offers an ideal opportunity for hardware consolidation and associated cost savings in infrastructure. This paper describes coexistence of Windows Server 2003 with Windows NT 4.0 in Windows NT 4.0 domains. It addresses upgrading file and print servers, Web application servers, core services such as DNS and DHCP, as well as remote access servers.

This is a preliminary document and may be changed substantially prior to final commercial release of the software described herein.

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 document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, 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.

© 2002. Microsoft Corporation. All rights reserved.

Microsoft, Active Directory, Windows, and Windows NT 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
File and Print Services	2
Distributed File System	2
Security and Data Recovery.....	2
Volume Shadow Copy Service.....	3
Additional File Server Enhancements.....	3
When to Use Windows Server 2003.....	3
Print Server Improvements.....	4
Storage Area Network Support.....	4
Web Application Server	5
Reliability Improvements.....	5
Legacy Web Applications.....	5
Security Enhancements	6
Additional IIS 6 Enhancements	6
Web-Based Application Development	6
UDDI Services	7
When to Use Windows Server 2003.....	7
Secure Mobile Access.....	8
Security Improvements	8
Remote Access Enhancements	8
Small Business Solutions.....	9
Wireless Networking	9
Internet Authentication Service.....	9
Core Services Consolidation	11
Consolidation Benefits	11
DNS and DHCP	11
Management.....	12
Public Key Infrastructure.....	12
Other Consolidation Opportunities	12

Total Cost of Ownership.....	12
Getting Ready for Windows Server with Active Directory.....	12
Summary	14
Related Links.....	15

Introduction

Windows® Server 2003 is the newest and most powerful operating system from Microsoft, offering new levels of dependability, performance, and connectivity. Building on the feedback of customers, third-party partners, and independent testing, Microsoft has made Windows Server 2003 into a highly productive infrastructure platform for powering connected applications, networks, and Web services. Windows Server 2003 improves on and streamlines the solid foundation of Windows 2000 Server, adding new features and technologies to meet the needs of today's customers. Key new technologies include Internet Information Services 6.0 (IIS 6), redesigned and featuring a new process model with new benefits for organizations of every size.

File system management has become easier and more reliable through such improvements as the Distributed File System (DFS) and Volume Shadow Copy service, which work together to keep file servers available and easy to navigate. Security and reliability of Web application servers benefit from the improvements in IIS 6, which has been re-architected to help prevent faulty code or external attacks from taking down other applications or the server itself. Remote Access Server, using such powerful features as Internet Protocol version 6 (IPv6) and Point-to-Point over Ethernet (PPoE) helps to ensure secure networking whether by dial-up, virtual private network (VPN), wireless, or wired connections. In addition, Windows Server includes new and enhanced command-line interface tools, wide support for industry standards like XML, and new features like the Automated System Recovery (ASR).

Windows Server 2003 maintains a high level of backward compatibility with Windows 2000 and Windows NT® 4.0 computing environments, making a gradual upgrade plan feasible and practical. Features such as IIS 5.0 Isolation Mode ensure compatibility with legacy and third-party products. Adding a new server running Windows Server 2003 to an existing Windows NT domain does not require replacing existing software and infrastructure. The improved performance and management of Windows Server make it an ideal platform to consolidate existing services. New and enhanced features for reliability ensure that Windows Server 2003, and any consolidated services, will stay up and available. Businesses can enhance the security and reliability of their existing IT infrastructure while lowering overall computing costs.

This paper discusses various scenarios in which a Windows NT 4.0 network can benefit from the addition of Windows Server 2003. The topics cover file and print servers, Web application servers, core services such as DNS and DHCP, and remote access servers. Because Windows Server 2003 is capable of coexisting with Windows NT 4.0, bringing a computer with Windows Server 2003 into a Windows NT 4.0 domain can provide your business with many advantages in these areas.

File and Print Services

Microsoft has responded to customer feedback by building significant improvements into the file and print server capabilities of Windows Server 2003. Upgrading file and print servers to Windows Server 2003 can bring benefits in the areas of reliability, availability, ease-of-use, and management. Windows Server 2003 has several new and improved features like DFS and Volume Shadow Copy services that make it easier to set up, access, and manage a file infrastructure on Windows Server 2003. Windows Server 2003 also makes servers easier to manage with a new task-based user interface that is designed to make everyday activities easier to carry out. The Configure Your Server Wizard helps automate the setup of a file or print server, and there are wizards for most tasks. The improved Windows Management Instrumentation (WMI) exposes scriptable interfaces for most administrative commands.

Distributed File System

One of the biggest improvements for file servers is DFS, which takes your existing file infrastructure and creates a single logical view of files stored on multiple servers. This system is entirely transparent to users who have the DFS client on their local machine. The DFS client is built into Windows NT 4.0 and all later Microsoft operating systems. DFS makes files much easier to find, because users do not need to know which server a file is on. DFS also improves scalability, making it easy to add file servers or balance the workload among servers without disrupting users' ability to find and access files. Windows Server 2003 enhances the reliability of DFS by allowing a single server to host multiple DFS roots, which means DFS can now be clustered for high availability and load balancing. You can also store multiple copies of file shares for redundancy. File Replication Service (FRS) works with DFS to maintain synchronized copies of data on file shares, so that in the event of a failure, DFS can transparently redirect requests for data to a different server. For better management on the corporate level, administrators can be delegated control of a specific portion of the DFS namespace, rather than the entirety. This streamlines IT processes and makes the entire infrastructure easier to maintain. DFS is fully integrated with Windows NT 4.0 security. One or more servers running Windows Server 2003 with DFS can help you replace or aggregate your existing file structure into a single hierarchy that is easy to use and maintain.

Security and Data Recovery

Windows Server 2003 also brings improvements in the area of performance and security. Encrypting File Service (EFS), improved in Windows Server 2003, allows users to encrypt their data to prevent accidental or malicious access by unauthorized persons. EFS allows you to provide high security to selected portions of your organization by giving them access to a Windows Server 2003 file server running EFS. EFS has been enhanced in Windows Server 2003 with the addition of new, more powerful security algorithms and better performance.

In the event of a more serious hardware failure, the new ASR feature offers an easy solution for data recovery. ASR allows an administrator to rapidly reboot and restore a failed Windows Server 2003 server. This process uses an ASR backup floppy prepared ahead of time. Restoring the hardware is a simple matter of booting from a Windows Server 2003 CD and choosing Automated System Recovery. The server will then restore itself from the existing backup media.

Volume Shadow Copy Service

Volume Shadow Copy service is a new feature in Windows Server 2003 that enhances data management in two primary ways. First, it allows for the creation of point-in-time copies of data on a volume. Backups can be done online, without stopping server activity, and without the problems of inconsistent data or open files being left out. They can also be scheduled to correspond with periods of low network usage. Volume Shadow Copy service maintains a set of previous versions of files, called shadow copies, which can be used for data recovery when a file is damaged through human error, reducing the frequency of restoring files from backup tapes. Shadow copies are incremental backups, only recoding files which have changed since the last backup. This means that backups take up less storage space. Volume Shadow Copy service is also supported with a public Application Programming Interface (API), so developers can write applications that utilize the features of this technology.

The majority of accidental file loss is the result of user error. When a user accidentally overwrites or deletes a file, the result is usually lost time as the user recreates work or contacts a network administrator to restore a file from backup. Users on Windows Server 2003 or the Windows XP Professional operating system can access shadow copies of their files from within the Windows Explorer. This leads to improved productivity and a reduction in the number of support calls for file restoration. Volume Shadow Copy services for users requires the Volume Shadow Copy service client for Windows XP Professional, found on the Windows Server 2003 installation CDROM.

Additional File Server Enhancements

File server management improvements are rounded out by the addition of a Web-based management user interface, enabling server management from any browser, and new command-line tools for managing local storage. In addition, the volume management tools have been improved to make it easier to manage and administer a large number of volumes. These improvements, along with the Volume Shadow Copy service and ASR, add up to fewer support calls and less time spent on administrative tasks. The result is lower total cost of ownership for your file server infrastructure.

The effectiveness of your file and print infrastructure is not simply a matter of new tools and features. Windows Server 2003 has a number of performance enhancements. NTFS has been designed to minimize the circumstances in which CHKDSK needs to be run. Nevertheless, in those rare cases where it is required, CHKDSK performance has been radically improved, reducing the amount of downtime caused by CHKDSK. The defragmentation tool has also been optimized for better performance.

Reliability has also been enhanced in Windows Server 2003 to enable a greater proportion of uptime. If high availability is required in your organization, you can utilize high availability clustering with Windows Server 2003 on your storage servers. High availability clustering can also be combined with Network Load Balancing to enhance the performance of a storage cluster. The NTFS file system also has higher performance and supports larger volumes in Windows Server 2003 than ever before.

When to Use Windows Server 2003

In evaluating a possible upgrade of all or part of your file server infrastructure to Windows Server 2003, the time and cost associated with the upgrade should be measured against the long-term savings of an infrastructure that is easier to use and manage. If you have a large number of file shares, DFS can greatly simplify your environment. This not only enhances user productivity and reduces support calls, but makes your entire infrastructure easier to manage. DFS and the Volume Shadow Copy service both

help improve the availability of file servers by simplifying backup and restore procedures. If your network utilizes Windows XP Professional as a client operating system, support calls due to accidental file loss can be reduced even more by implementing the Volume Shadow Copy Services client for users. The higher performance of Windows Server 2003 and the NTFS file system on Windows Server 2003 may allow you to eliminate redundant hardware, leading to further savings. In addition, you should consider the amount of time your IT staff devotes to managing file servers and responding to support calls. Improved management methodologies in Windows Server 2003 can save significant time and money in the IT department, freeing up staff for more useful tasks.

Print Server Improvements

On the print server side, Windows Server 2003 offers improvements in manageability, reliability, and performance. Print driver management and reliability has been improved with kernel-mode driver blocking, giving administrators control over driver installation on the server. At the same time, the latest enhancements to Plug and Play, and built-in support for over 3,800 printer drivers, greatly facilitate hardware installation, configuration, and upgrading. Printers can be installed and configured remotely and via scripts using WMI in Windows Server 2003, and if you are using a print cluster, you can now install drivers on all nodes in the cluster simultaneously. Administrators have printer scheduling and access controls, enabling them to optimize printer availability and usage. Most printer management functions can now be handled through a command-line interface as well as scripted for automated management. File spooling has been optimized for higher print volume management, getting documents to users faster. Upgrading your print servers to Windows Server 2003 or aggregating your organization's printers on a Windows Server 2003 print server can greatly reduce the headaches and administrative load of maintaining your print infrastructure.

Storage Area Network Support

One final area where Windows Server 2003 has seen major improvements is in supporting Storage Area Network (SAN) configurations. In response to customer demand for more SAN friendly tools, Microsoft has included a number of new innovations in Windows Server 2003, including the Virtual Disk Server (VDS) and Winsock Direct. Virtual Disk Service, a new technology in Windows Server 2003, provides standardized interfaces for handling device virtualization in a SAN environment. VDS enables third-party vendors to write VDS providers, standardizing communications with heterogeneous environments under a unified management interface. Winsock Direct is another new technology in Windows Server 2003 that streamlines communications between SANs and Ethernet-based networks and technologies.

Web Application Server

One of the fastest growing server roles in today's computing environment is that of the Web application server. More and more organizations are finding ways to serve content, disseminate information, and collaborate with employees, partners, and customers over the Web. Many of these organizations are looking at their Web application servers as more than just a way to publish information; they expect them to play a key role in developing new business opportunities. IIS 6 incorporates powerful enhancements in the areas of performance, reliability, manageability, and security that make it the platform of choice for hosting today's Web applications. In addition, IIS 6 supports new and emerging technologies like XML, SOAP, and Microsoft .NET.

Reliability Improvements

Downtime due to faulty applications leaking memory and impacting the entire Web server has been a major problem for many organizations. IIS 6 features a new request processing architecture designed to prevent application issues from taking down the rest of the Web server. The new kernel-mode HTTP listener, HTTP.SYS, is immune to the usual Web service disruptions caused by user-mode code failures because no application code runs within it. It will continue to accept and queue requests in case of such a failure. Customers have reported significant availability gains including as much as 50 percent reduced downtime on Windows Server 2003 and IIS 6 compared with previous Web servers.

Different Web applications and Web sites can now be isolated into separate groups called application pools. Requests for services from each application pool are handled in worker process isolation mode. This means that all application code runs in isolation. As a result, the failure of a problematic Web application cannot affect or disrupt the other applications on the Web server.

IIS 6 offers improved reliability through many features, including the combination of application pools and automatic health monitoring. In addition, IIS 6 can auto-restart failed applications or periodically restart worker processes in order to manage faulty applications. Individual worker processes can be stopped temporarily without affecting the rest of the Web site. The Web server does not need to be restarted when carrying out most maintenance and administrative tasks.

Worker process isolation mode allows a new technique called Web gardens. By default each application pool is served by one worker process, but multiple processes can be assigned to an application pool so that if one process hangs, others are available to accept and process requests. This capability lies at the heart of Web gardens. A Web garden is roughly analogous to a Web farm except that it resides on a single server. Web gardens help improve availability and scalability because application requests can still go through even if one process hangs.

Legacy Web Applications

Many organizations already use a previous version of IIS to serve Web content or applications. Although legacy applications may have some limitations inherent to the platform they were built for, most applications will benefit considerably by being moved to IIS 6. Most applications will run just fine under IIS 6, as the programming model and interfaces are fundamentally unchanged. However, some applications written for previous versions of IIS may have compatibility issues, such as expecting to have exclusive access to the resources they require. To handle these legacy applications, IIS 6 can be set to a process model called IIS 5.0 isolation mode.

IIS 5.0 isolation mode allows applications written for an earlier version of IIS to run as designed without interrupting other applications on the server. The IIS architecture still prevents an application crash from causing the whole Web server to crash. In addition, applications in IIS 5.0 isolation mode will still retain the full benefit of kernel-mode request queuing and kernel-mode caching offered by the new HTTP.SYS.

It is expected that most applications will not require IIS 5.0 isolation mode. When moving legacy applications to Windows Server 2003, evaluate each application and determine whether it can run natively on IIS 6 or whether it should be run in IIS 5.0 isolation mode. For the few applications that currently require IIS 5.0 isolation mode, a modest development effort may enable the application to take full advantage of IIS 6. Even applications that do require isolation mode will likely experience some performance and reliability improvement on IIS 6.

Security Enhancements

IIS security has also been enhanced in IIS 6 to meet the higher demands of today's connected environment. By default, IIS is not installed on Windows Server 2003, and when it is installed, it is installed in a lockdown mode that serves only static content. An administrator must explicitly choose to install IIS and enable greater functionality as needed by the applications. In addition, administrators can exercise a high level of control over what functionality is enabled on an IIS 6 server.

All worker processes in IIS 6 by default run under NetworkService, a new low-privilege user account, to minimize the effect of potential attacks. With only 5 privileges, compared to more than 20 in IIS 5.0, IIS 6 includes more layers of defense. Worker process isolation mode prevents any Web application from being used to disrupt another. Secure Sockets Layer (SSL) has been improved in IIS 6 to provide better performance and security. All these improvements and other enhancements work together to make IIS 6 more secure right out of the box.

Additional IIS 6 Enhancements

IIS 6 also features improvements in the area of management and administration. Setting up a Web server is easier than ever. Using the Configure Your Server Wizard that ships with Windows Server 2003, an administrator can specify a Web Application Server role for a server and most setup tasks are completed automatically. IIS 6 also includes new management tools and capabilities. An administrator can backup, restore, or edit the new XML-based metabase dynamically without interrupting service even while the Web server is running. With the XML metabase and command-line options, administrators have new choices and options for Web server management. IIS 6 includes a number of metabase tools that make it easier to discover and diagnose server or application problems. The IIS administration MMC snap-in has also been redesigned to be easier to use.

Web-Based Application Development

IIS 6 will be of particular interest to organizations that develop Web-based applications. With its full integration of Microsoft .NET, IIS 6 is the ideal platform to distribute Web-based applications and XML Web services. XML Web services are building block applications that can be assembled to provide business solutions. IIS 6 running on Windows Server 2003 is complemented in this role by Visual Studio® .NET, the latest release of Microsoft's development tools. Visual Studio .NET includes all the tools needed to create XML Web services in any of a number of computing languages, including reusable code libraries and debugging tools.

IIS 6 is also fully integrated with Microsoft Passport. This enables developers to take advantage of the huge customer base of Microsoft Passport without having to manage user account management issues themselves. IIS 6, Visual Studio .NET with the Microsoft .NET Framework and Windows Server 2003 together comprise the next generation platform for creating Web-based applications.

UDDI Services

In Windows Server 2003, Microsoft introduces UDDI Services, a dynamic and flexible infrastructure for XML Web services. This standards-based solution enables companies to run their own Universal Description, Discovery and Integration (UDDI) directory for intranet or extranet use, making it easy to discover and re-use Web services and other programmatic resources on the network. With UDDI Services, developers can quickly and easily find Web services available within their organization. IT administrators can efficiently catalog and manage programmable resources in their network. Enterprise UDDI Services also helps companies build and deploy smarter, more reliable applications.

When to Use Windows Server 2003

Web servers hosting mission-critical applications or applications that require very high performance will probably be your best choices for an upgrade to Windows Server 2003. Mission-critical applications can take advantage of the robustness of IIS 6 to reduce downtime and improve reliability. You may also want to consider aggregating Web servers onto IIS 6 to save hardware and simplify administration. Since IIS 6 does a better job of isolating applications, a number of aggregated applications will not interfere with one another. This allows you to eliminate redundant hardware and centralize management and security of your Web application servers.

Secure Mobile Access

More and more companies are making use of remote access and wireless LAN not only to connect people and resources, but also to enhance productivity and create new business opportunities. In response to the explosive growth and diversity of networking technologies, Microsoft has expanded and improved its support for various kinds of remote access, including dial-up connections, VPN, and wireless connections. Remote access creates new ways for companies to communicate with users, partners, and customers, while increasing the efficiency of the workforce by providing them with access anywhere. Windows Server 2003 has the features required to implement and maintain secure mobile access in today's environment. Depending on your current implementation, you may benefit from upgrading existing servers to Windows Server 2003 or using Windows Server 2003 to implement new technologies.

More and more companies are making use of mobile access to increase the productivity of users by giving them flexible access to networked resources. Routing and Remote Access and the WLAN support offered by Windows Server 2003 can be used to give users secure wired and wireless access to the network from home, in the office, or while on the road without compromising security. Windows Server 2003 has a number of flexible offerings, which can be configured to meet varying needs. Understanding your remote access and wireless needs is the first step towards a successful implementation of Windows Server 2003 secure mobile access.

Security Improvements

As the foundation to a secure mobile access infrastructure, Windows Server 2003 introduces numerous improvements in the area of networking. Networking with Windows Server 2003 improves the performance, efficiency, and ease-of-use of your networked systems. Point-to-Point tunneling protocol (PPTP) and Layer 2 Tunneling Protocol over IPsec (L2TP/IPsec) provide organizations with the means to create a secure remote access, standards-based solution for connecting remote users and branch offices. A client for L2TP/IPsec is available for Windows NT 4.0, but it does not offer the two factor, certificate-based authentication available through Windows Server 2003.

Windows Server 2003 includes the standards-based Public Key Infrastructure (PKI) in the form of Certificate Authority (CA). Third-party PKI may be used, but for optimum integration and lowest cost of ownership, CA is the better solution. Windows Server 2003 also supports third-party authentication methods, such as smart cards and biometrics. Windows Server 2003 includes built-in support of the 802.1X standard for wireless LAN, which is the most robust security standard in the industry. If you are concerned about security and need to give remote or wireless LAN access to users, you should consider implementing Windows Server 2003 Remote Access Servers.

Remote Access Enhancements

Windows Server 2003 also makes remote access easier for administrators to deploy and users to use. VPN and RAS include an enhanced connection manager for Windows Server 2003 and Windows XP clients, which makes it easier to set up and use remote access. The Microsoft Connection Manager Administration Kit (CMAK) includes a set of tools and technologies to customize profiles for remote access users. This and a variety of other user interface and experience improvements help users be more productive, reducing support calls from remote users. Another enhancement to Routing and Remote Access in Windows Server and Windows XP is the quarantine feature for the client. Before

providing full network access to a client, the client has to undergo a status check in quarantine state. Based on the policies of the organization, if the client is up-to-date full access is provided otherwise access is denied until the client is updated.

Small Business Solutions

Windows Server 2003 includes a number of features targeted at home and small business users that make networking easier and more secure in those environments. Internet Connection Sharing (ICS) is a feature that can be used to allow multiple computers on a home or business network to share a single dial-up or broadband Internet connection. Internet Connection Firewall (ICF) is a basic firewall built into the operating system that allows you to secure communications to an unsecured network through Windows Server 2003. These features are designed for smaller businesses and should be evaluated in terms of the size of your organization.

Wireless Networking

Wireless networking is a technology that is now emerging into maturity. In the past, creating a secure wireless networking environment that is easy to implement, use, and maintain has been extremely difficult. With Windows Server 2003, wireless networking has been made significantly easier and more secure. Windows Server 2003 supports the IEEE 802.1X standard, which uses a certificate-based network authentication and authorization model. New to Windows Server 2003 is support for the Protected Extensible Authentication Protocol (PEAP). Presently an IETF draft, PEAP creates an encrypted tunnel for wireless connections before authentication so that passwords are not compromised. PEAP also allows you to use secure wireless access without requiring an extensive PKI implementation.

Windows Server 2003 also has a number of enhanced features to help support roaming wireless users that adjust the configuration of the wireless connection when the user moves between wireless zones.

Windows Server 2003 also includes support for the Extensible Authentication Protocol - Transport Level Security (EAP-TLS). This protocol allows safe and secure access to wireless networks for both employees and guests while extending the authentication functionality to a dedicated server. Using EAP-TLS, the authentication requests are routed to a server running Internet Authentication Services (IAS) for network access. EAP-TLS can also be used to redirect unidentified wireless connections, corporate visitors, or other guests to a restricted LAN. It can also be used to redirect connections that do not have a certificate to a particular virtual LAN for configuration. If your installation needs to support unauthenticated wireless users, you should consider implementing Windows Server 2003 with EAP-TLS.

Most wireless networks use some kind of certification structure to identify clients. This can be provided by an existing certification infrastructure, or by a certificate authority created by a Windows Server 2003-based server running Certification Services.

Windows XP Professional is the recommended operating system for wireless clients and supports the widest range of wireless devices. There are also a variety of wireless hand-held devices that run the Windows CE operating system that can be used in a Windows Server 2003 wireless environment.

Internet Authentication Service

As the number of remote users and their methods of access increase, a centralized management methodology becomes more and more important. IAS in Windows Server 2003 fills this role. IAS fully

supports the Remote Access Dial-in User Server (RADIUS) protocol and can act as a RADIUS server for various kinds of access (including dial-up, VPN, and wireless) or as a RADIUS proxy. A RADIUS server manages authentication and authorization of remote and wireless users. IAS collects information about remote or wireless users as they log on, and provides configuration information that determines how they may connect to the network. This not only makes it easier to manage users, but gives you flexible options for handling users as well as greater control over the security of your network.

The IAS proxy includes the ability to forward requests between RADIUS servers, load balancing capabilities, ability to force clients to use a secure tunnel, and selective forwarding. An IAS-based RADIUS proxy can authenticate users from another domain, even if that domain does not have a trust with the domain in which the IAS RADIUS proxy is located. These features make a number of scenarios possible. A corporation can partner with an ISP to forward remote access requests from its employees to the corporate RADIUS server. This enables the corporation to outsource their dial-up server. ISPs can form a confederation to provide these kinds of services nationally or internationally.

IAS also includes powerful logging and user management features. These include the ability to log information to a SQL Server™ database. This provides rich information that can be used to analyze remote access usage and diagnose any problems that arise. IAS gives administrators a high level of control over user access. For example, IAS can be used to enforce smart card logon or check for valid certificates. This lowers the total cost of managing and maintaining remote access while giving administrators a higher level of granular control. Larger organizations in particular will want to use Windows Server 2003 to improve the management of their remote access implementation.

IAS also includes scriptable APIs. Development tools and a software development kit (SDK) available from Microsoft enable you to build custom solutions on IAS that are suited to your organization's needs.

Core Services Consolidation

Many companies are achieving significant savings by consolidating their core services on Windows Server 2003. Windows Server 2003 is fully integrated with Windows NT security, networking and logon, making coexistence relatively painless. Although the most pronounced benefits can be achieved by doing a full upgrade of your domain infrastructure to Windows Server 2003 with the Active Directory® service, there may be reasons that you do not want to do this immediately in your organization. You should consider consolidating core services, such as user logon, Dynamic Host Configuration Protocol (DHCP), Domain Name Service (DNS), and so on if you want to take advantage of the features and performance of Windows Server 2003 while preserving your existing Windows NT 4.0 domain structure. Reasons for doing this may include the need to support legacy systems that cannot be upgraded or a desire to upgrade systems incrementally.

Consolidation Benefits

The benefits of a core service consolidation include increased performance, higher availability, reliability and access to new features and technologies. Windows Server 2003 can provide faster and more efficient logon and networking and name resolution for a Windows NT 4.0 domain. This also provides an opportunity for hardware consolidation as redundant servers are eliminated. In addition, a consolidated environment is easier to manage, not only because it is more centralized, but also due to the powerful management features of Windows Server 2003. The overall benefits of this scenario are lower costs and greater productivity. Microsoft and Microsoft partners also provide numerous resources to assist in a consolidation scenario, including roadmaps, technical expertise, and quick start guides to help you carry out your consolidation as quickly and easily as possible.

Core services can be migrated to Windows Server 2003 without compromising your existing Windows NT-based domain structure. Windows Server 2003 uses the Windows family logon and authentication, so it is fully interoperable with existing systems. Windows Server 2003 can interact seamlessly as a member server in a Windows NT domain.

Windows Server 2003 is the most reliable operating system that Microsoft has ever released. Moving core services to Windows Server 2003 is an excellent way to take advantage of this reliability in your organization. Windows Server 2003 can be clustered to provide high availability and load balancing. If reliability is a key concern, you should consider migrating your mission critical services and applications to Windows Server 2003.

DNS and DHCP

A Windows Server 2003 domain member server in a Windows NT 4.0 domain can be used to host DNS for the domain. This enables you to take advantage of the higher reliability and performance of Windows Server 2003 DNS, as well as improvements over Windows NT 4.0 DNS. Windows Server 2003 DNS has security improvements including secure dynamic update and support for IETF RFC 2535 DNS security extensions. DHCP improves mobility and makes it easier for users to connect to the network wherever they are while also making IP address management considerably simpler for administrators. Windows Server 2003 includes enhanced management tools for DHCP, including automated backup and restore and migration of the DHCP database. This eliminates many time consuming tasks that formerly had to be done by hand. Generally speaking, when using Windows Server 2003 for DNS and DHCP, the main consideration for determining how many servers you will

require will not be server performance, but rather geographical locations and network performance between them. In many organizations, this can mean eliminating the bulk of their existing servers resulting in hardware savings.

Management

Microsoft has created tools and wizards that make preparing a server for the DNS, DHCP, and other server roles as simple as possible, including debugging and reporting tools to help you identify and resolve problems as they arise. The new Configure Your Server Wizard allows an administrator to configure key server roles, such as DNS and DHCP, quickly and easily. Windows Server 2003 includes powerful management tools like the Microsoft Management Console (MMC) and a new task-based interface that reflects the way that network administrators actually work.

Public Key Infrastructure

Windows Server 2003 comes with Certificate Services and has certificate and trust management capabilities that can be used to enable secure communication across insecure networks such as the Internet, corporate network, or extranet. Certificate Services allows an administrator to set up and manage certification authorities and grant and revoke X.509 v3 certificates. Although Active Directory may be required to realize the full potential of Windows Server Certificate Services and PKI, a Windows Server 2003-based server can act as a standalone certificate authority. The advantage of this is that you can use Windows Server 2003 to provide certificates for internet authenticated users, wireless servers, remote access users, and so on. Windows Server 2003 can also be used to provide support for smart card login.

Other Consolidation Opportunities

In addition to core services, Windows Server 2003 is an ideal platform to consolidate other applications, such as line-of-business applications, databases, messaging, and Web-based applications. Microsoft SQL Server 2000 and Microsoft Exchange 2000 provide high-performance platforms for database and messaging consolidation respectively. Windows Server 2003 also supports new tools and technologies such as XML, SOAP, and the .NET Framework. These technologies in conjunction with Internet Information Services 6.0 make Windows Server 2003 an ideal platform for Web-based applications. In addition, you can take advantage of technologies like Windows Server 2003 Terminal Services by using Windows Server 2003 in your existing Windows NT 4.0 domains.

Total Cost of Ownership

The primary consideration in evaluating any consolidation scenario is total cost of ownership. Windows Server 2003 can allow you to reduce the overall cost of your network by eliminating redundant hardware, centralizing and simplifying management tasks, and improving user productivity. Consolidation also provides additional benefits in the form of increased performance, support for new features and technologies, and higher reliability.

Getting Ready for Windows Server with Active Directory

Finally, core services consolidation has the advantage of being an important incremental step on the way to an upgrade to Windows Server 2003 domains and forests running with Active Directory. Ultimately, many organizations will want to take advantage of the opportunities provided by implementing Active Directory. An incremental upgrade offers an alternative to the complexity of

upgrading your entire infrastructure at once. Core services hosted on Windows Server 2003 will be easier to integrate into Active Directory in an eventual domain upgrade. This is particularly true in the case of DNS, because upgrading your DNS servers is a necessary step towards a domain upgrade. Active Directory provides single-logon capability and a central repository for information for your entire infrastructure, vastly simplifying user management and providing superior access to networked resources.

Summary

Windows Server 2003 offers many benefits when used in a Windows NT 4.0 domain, whether as a file and print server, a Web application server, a remote access server, or for core services consolidation. Because Windows Server 2003 reaches new heights in performance, reliability, and security, it offers an ideal opportunity for hardware consolidation and associated cost savings in infrastructure. It interoperates well with earlier Windows-based server computers and domains, providing many critical improvements in productivity and manageability to the entire network. It includes key new technologies, such as Internet Information Services, redesigned and optimized for existing and future Web server needs. It also has the flexibility and robustness to scale upwards not just for immediate consolidation but also for future growth.

In addition, implementing Windows Server 2003 as a member server in your Windows NT 4.0 domain is a first step towards a more general upgrade of systems. Upgrading your domains and forests to Windows Server 2003 domains and forests with Active Directory is the optimal way of getting the maximum functionality out of Windows Server 2003. This enables you to take advantage of the advanced management features of Active Directory. For organizations that need to support legacy systems or that do not want to upgrade in a single step, a variety of partial and incremental upgrade scenarios are available. The new Active Directory Application Mode lets you run Active Directory as an application in your Windows Server 2003 domains. This lets you provide a portion of the functionality of Active Directory to applications and services without requiring you to upgrade your domain controllers. For more information on Active Directory in Application mode, see [Introduction to Active Directory in Application Mode](http://www.microsoft.com/windowsserver2003/techinfo/overview/adam.mspx) at <http://www.microsoft.com/windowsserver2003/techinfo/overview/adam.mspx>.

Related Links

See the following resources for further information:

- [Why Upgrade From Windows NT 4.0 to Windows Server 2003](http://www.microsoft.com/windowsserver2003/evaluation/whyupgrade/nt4/nt4townet.mspx) at <http://www.microsoft.com/windowsserver2003/evaluation/whyupgrade/nt4/nt4townet.mspx>.
- [Top 10 Features of Windows Server 2003 for Organizations Upgrading from Windows NT Server 4.0](http://www.microsoft.com/windowsserver2003/evaluation/whyupgrade/top10nt.mspx) at <http://www.microsoft.com/windowsserver2003/evaluation/whyupgrade/top10nt.mspx>.
- [Moving Windows NT Server 4.0 and Windows 2000 Applications to Windows Server 2003](http://www.microsoft.com/windowsserver2003/techno/serverroles/appserver/movingnt4.mspx) at <http://www.microsoft.com/windowsserver2003/techno/serverroles/appserver/movingnt4.mspx>.
- [Introduction to Active Directory in Application Mode](http://www.microsoft.com/windowsserver2003/techno/overview/adam.mspx) at <http://www.microsoft.com/windowsserver2003/techno/overview/adam.mspx>.
- [Microsoft Windows NT Web site](http://www.microsoft.com/ntserver/default.asp) at <http://www.microsoft.com/ntserver/default.asp>.

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