



Technical Overview of Terminal Services

Microsoft Corporation

Published: July 2002

Abstract

Windows Server 2003 includes the Terminal Services features of Windows 2000, the client and protocol enhancements found in Windows XP, and a number of other additional features. This technical article is intended for server administrators who are already familiar with Terminal Services in Windows 2000.

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, ActiveX, MSDN, Win32, Windows, , the Windows logo 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
Benefits	1
What's New in Terminal Services	2
Client Features	2
Server Features	2
Client Features.....	3
Improved Client Interface	3
Remote Desktop Connection	3
Moving Between a Remote Session and the Desktop	3
Customizing the Remote Connection.....	3
Optimize Performance Over Lower-bandwidth Connections	4
No Separate Connection Manager	4
Automatic Reconnects.....	4
Client Resource Redirection	4
Client Resource Redirection Features	5
Client Deployment Options	6
Installing RDC on Other Platforms.....	6
Remote Desktop Web Connection	6
Windows CE Version of RDC.....	6
Server Features	7
Improved Server Management	7
Remote Desktop for Administration	7
Connecting to the Console.....	7
Activating Remote Desktop and Terminal Services.....	7
Additional Management Features	9
Group Policy.....	9
Windows Management Interface Provider.....	9
Active Directory Service Interfaces	9
Printer Management.....	9

Terminal Services Manager	10
Terminal Server License Manager.....	10
Single Session Policy	10
Client Error Messages	10
Security Enhancements	10
Remote Desktop Users Group	10
Security Policy Editor	10
128-Bit Encryption.....	10
FIPS Compliance.....	11
Software Restriction Policies	11
Session Directory	11
Summary	12
Related Links.....	13

Introduction

The Terminal Services component of Microsoft® Windows® Server 2003 builds on the solid foundation provided by the application server mode in Windows 2000 Terminal Services, and includes the new client and protocol capabilities in Windows XP. Terminal Services lets you deliver Windows-based applications, or the Windows desktop itself, to virtually any computing device—including those that cannot run Windows.

Terminal Services in Windows Server 2003 can enhance an enterprise's software deployment capabilities for a variety of scenarios, allowing substantial flexibility in application and management infrastructure. When a user runs an application on Terminal Server, the application execution takes place on the server, and only keyboard, mouse and display information is transmitted over the network. Each user sees only his or her individual session, which is managed transparently by the server operating system, and is independent of any other client session.

Benefits

Terminal Services in Windows Server 2003 provides three important benefits.

Benefit	Description
Rapid, centralized deployment of applications	<p>Terminal Server is great for rapidly deploying Windows-based applications to computing devices across an enterprise—especially applications that are frequently updated, infrequently used, or hard to manage.</p> <p>When an application is managed on Terminal Server, and not on each device, administrators can be certain that users are running the latest version of the application.</p>
Low-bandwidth access to data	<p>Terminal Server considerably reduces the amount of network bandwidth required to access data remotely.</p> <p>Using Terminal Server to run an application over bandwidth-constrained connections, such as dial-up or shared WAN links, is very effective for remotely accessing and manipulating large amounts of data because only a screen view of the data is transmitted, rather than the data itself.</p>
Windows anywhere	<p>Terminal Server helps users become more productive by enabling access to current applications on any device—including under-powered hardware and non-Windows desktops.</p> <p>And because Terminal Server lets you use Windows anywhere, you can take advantage of extra processing capabilities from newer, lighter-weight devices such as the Pocket PC.</p>

What's New in Terminal Services

Windows Server 2003 adds a number of important new features to provide improved management of terminal servers and Windows Server 2003-based computers.

These include features include:

Client Features

- [Improved Client Interface](#)
- [Client Resource Redirection](#)
- [Client Deployment Options](#)

Server Features

- [Improved Server Management](#)
- [Security Enhancements](#)
- [Session Directory](#)

Note This article is an overview of a number of topics that are detailed in other white papers, the Windows Server 2003 Deployment Guide, the product help files, and other resources. It does not attempt technical depth in all areas. See the [Related Links](#) section of this document for additional resources

Client Features

There are several new client features that provide improved management of terminal servers and Windows Server 2003-based computers.

Improved Client Interface

The Terminal Services client provides substantial improvements over previous releases.

Remote Desktop Connection

The Terminal Services client, called “Remote Desktop Connection,” (RDC) provides substantial improvements over previous releases, including greater functionality through a simplified user interface.

RDC is the same program that’s used to connect to a Windows XP Professional-based computer running Remote Desktop, and can be used to connect to previous versions of Terminal Services (Windows NT® 4–Terminal Server Edition and Windows 2000)¹.

To use RDC, simply type the name of the remote computer and select **Connect**, as shown in Figure 1 below.

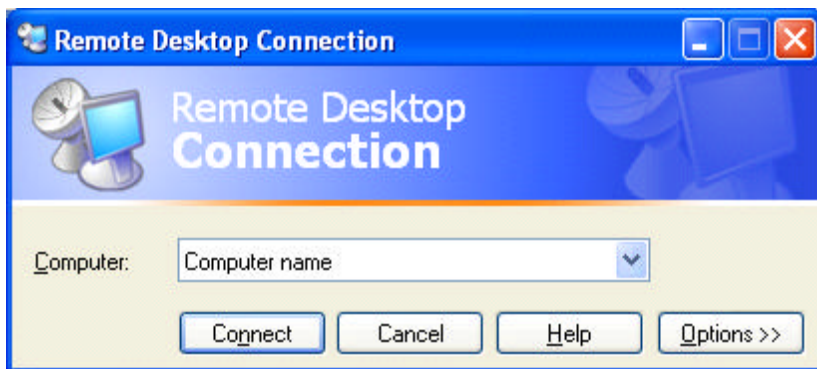


Figure 1. Connecting to a remote computer using Remote Desktop Connection

Moving Between a Remote Session and the Desktop

By default, a remote session is full-screen and high-color. The Connection Bar at the top of a full-screen RDC session enables you to move easily between the remote session and the local desktop.

Customizing the Remote Connection

If you want to change the various options for configuring the remote connection, a tabbed property sheet exposes the controls for **Display**, **Local Resources**, **Programs** to run on connection, and other **Experience** settings, as shown in Figure 1 above.

¹ Newer features such as high color and file system redirection are only supported on Windows XP and Windows Server.

Optimize Performance Over Lower-bandwidth Connections

To optimize performance over lower-bandwidth connections, you can choose your connection speed, and strip away unneeded components of the remote session—for example, themes, bitmap caching, and others). These choices are made using the Experience tab of the RDC, as shown in Figure 2 below.

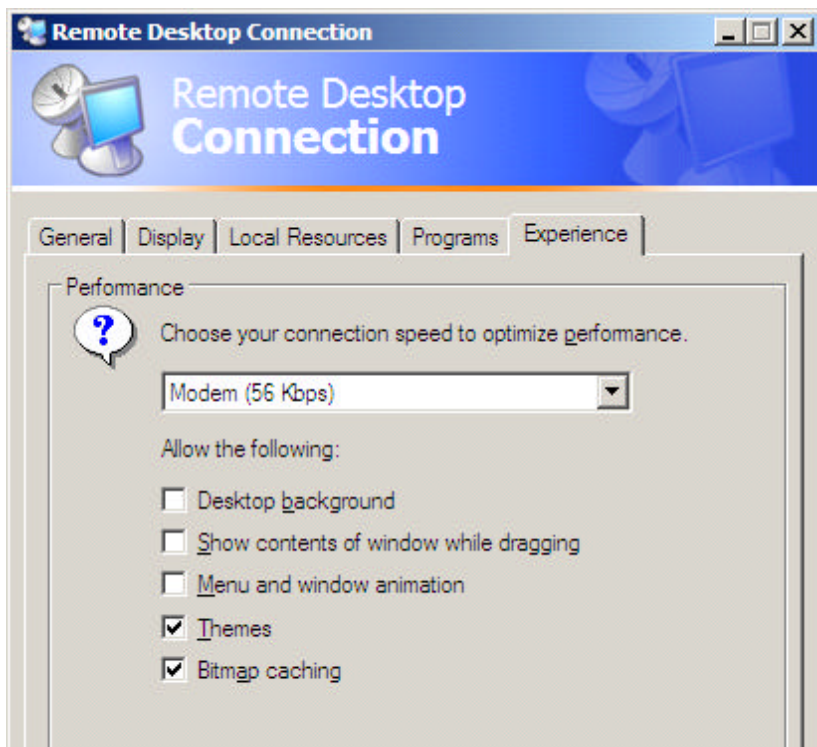


Figure 2. Optimizing performance over lower-bandwidth connections

No Separate Connection Manager

Connection Manager is no longer necessary because its functionality has been enhanced, and integrated directly into the RDC. This enables users and administrators to save and open connection settings files, which can be used locally and/or deployed to other users. Passwords that are saved are securely encrypted, and can only be decrypted on the computer on which it was saved.

Automatic Reconnects

To better protect against network dropouts (especially in wireless and dial-up environments), RDC will automatically attempt to reconnect to a server when a network interruption caused the session to be lost.

Client Resource Redirection

Remote Desktop Connection supports a wide variety of data redirection types. For security reasons, each of these can be disabled by either the client or the server. A security alert is displayed when file system, port, or smart card redirection is requested; the user can cancel the connection or disable the redirection at that time.

Client Resource Redirection Features

Unless specified below, client resource redirection features are only available to clients connecting to the Windows Server 2003 family or computers running Windows XP Professional. Any computer that can run Remote Desktop Connection can use these new features.

File System	Client drives, including network drives, are mounted inside the server session. This lets users open or save files on their own computers' disk drives, in addition to opening and saving files on the server.
Ports	Client serial ports can be mounted to the server. This enables a variety of hardware on the client computer to be accessed by software on the server.
Printers	All printers installed on the client are visible to the server—including network printers. With Windows 2000 Terminal Services, only locally-connected printers were redirected. Redirected printers are given names that are easier to read. For example, users might see: "printername on printserver (from clientname) in session 9"; whereas in Windows 2000, they would have seen "_printserver_printername/clientname/Session 9." Printer redirection also works when connecting to Windows 2000-based servers.
Audio	Sounds such as "error" and "new mail" notification events are redirected to the client.
Smart Card Sign On	A smart card which contains Windows logon credentials can provide those credentials to a Windows Server 2003 remote session for log-on. This feature requires a client OS that can recognize the smartcard first: Windows 2000, Windows XP, and Windows CE .NET.
Windows Keys	Keys such as Alt-tab and Control-Escape are sent to the remote session by default. The Control-Alt-Del combination is always interpreted at the client computer for security reasons. Note These redirections also work when connected to a Windows 2000-based terminal server, but only when using Windows NT-based client operating systems. They do not work with Windows 9x-based operating systems.
Time Zone	A RDC client computer can provide its time zone to the server, or users can manually set their own time zones. This enables an administrator to use one server for multiple users across different time zones. It's also helpful for applications that support features such as calendars. Note This feature is off by default, because it relies on a properly-set time zone on the client computer.

Virtual Channels	Virtual Channels can be used to move data between client and server computers. This feature is available in both Windows Server 2003 and Windows 2000 Server. Information about using Virtual Channels is available from MSDN® at http://msdn.microsoft.com/default.asp .
------------------	---

Client Deployment Options

Remote Desktop Connection is built into Windows XP and Windows Server 2003.

Installing RDC on Other Platforms

For client computers that don't have RDC installed, but want to do so, use one of the following options:

- Use tools such as Microsoft Systems Management Server or Windows 2000 Group Policy to publish/assign the Windows Installer-based RDC.
- Create a client install share on Windows Server 2003. (This can also be done with Windows 2000 Server.)
- Install directly from the Windows XP or Windows Server 2003 CD, using the 'Perform Additional Tasks' selection from the CD's autoplay menu. (**Note** This does not require installing the operating system.)
- Download the RDC from <http://www.microsoft.com/windowsxp/remotedesktop/>.

Remote Desktop Web Connection

Remote Desktop Web Connection is an improved safe-for-scripting ActiveX® control/COM object. It can be used by application service providers (ASPs), and other organizations, that want to deploy Web pages built with Web applications that include Win32® components. (See <http://msdn.microsoft.com/default.asp> for information about scripting this control.)

Windows CE Version of RDC

A Windows CE version of RDC is included in the Windows CE .NET Platform Builder to give Windows CE hardware vendors the option of including it with their devices.

Server Features

There are several new server features that provide improved management of Terminal Services and the Windows Server 2003 family.

Improved Server Management

With Windows Server 2003, it's easier than ever to manage servers, whether Terminal Services is installed or not.

Remote Desktop for Administration

Remote Desktop for Administration builds on the remote administration mode of Windows 2000 Terminal Services.

In addition to the two virtual sessions that are available in Windows 2000 Terminal Services remote administration mode, an administrator can also remotely connect to the real console of a server. Tools that would not work in a virtual session before, because they kept interacting with 'session 0', will now work remotely.

Connecting to the Console

To connect to the console, administrators can choose one of the following methods:

- Use the Remote Desktop Microsoft Management Console (MMC) snap-in.
- Run the Remote Desktop Connection (mstsc.exe) program with the /console switch.
- Create Remote Desktop Web Connection pages that set the ConnectToServerConsole property.

Activating Remote Desktop and Terminal Services

Unlike Windows 2000 Server which had a dual mode Terminal Services component, Windows Server 2003 separates the remote administration and Terminal Services functionality into separate configurable components.

Remote Desktop for Administration is enabled through the **System** control panel's **Remote Tab** as shown in Figure 3 below.

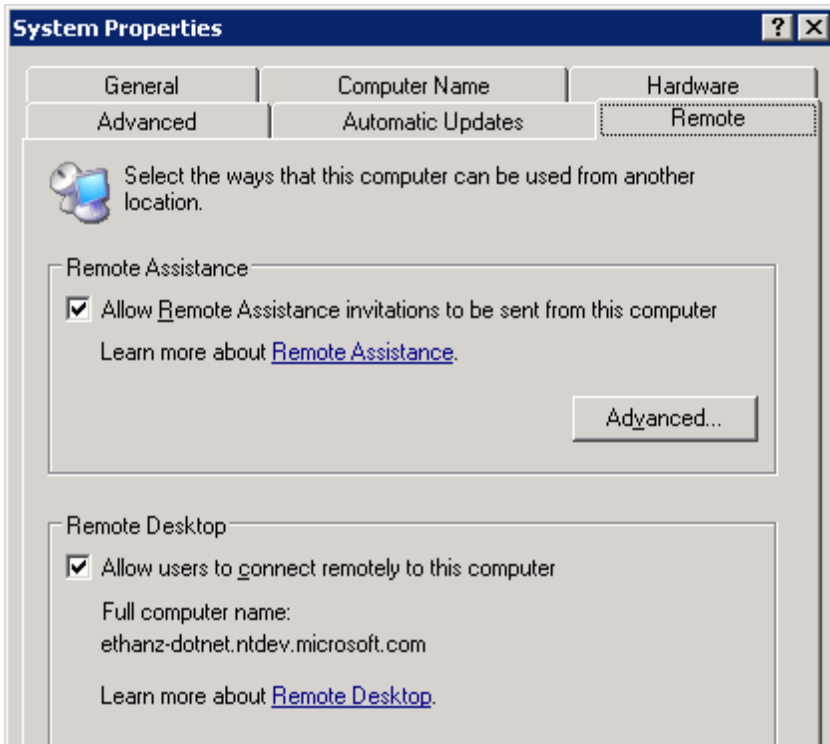


Figure 3. Enabling Remote Desktop for Administration

Terminal Services is enabled by adding the “Terminal Server” component using the Windows Components portion of the **Add/Remove Programs** wizard as shown in Figure 4 below.

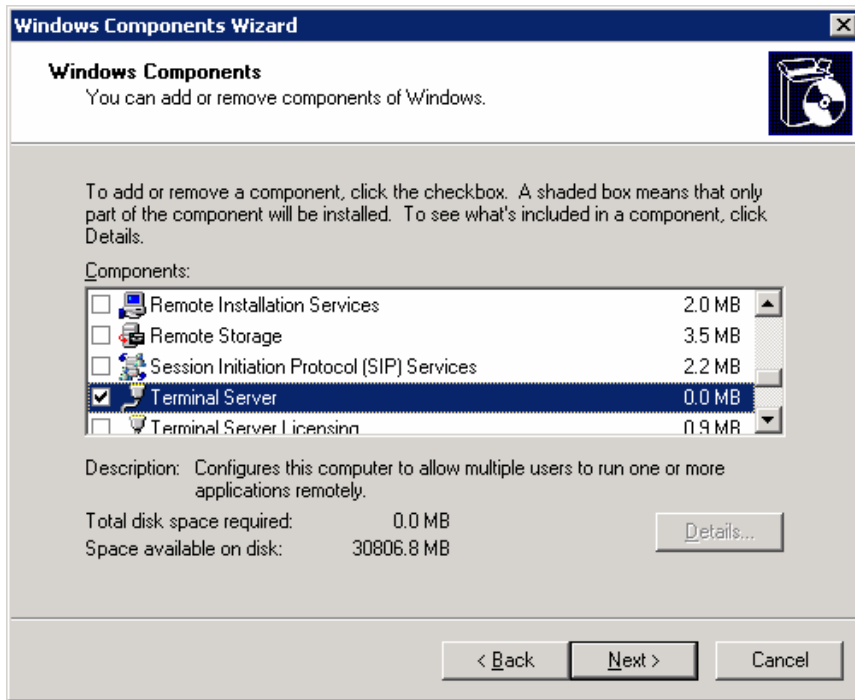


Figure 4. Enabling Terminal Server

Additional Management Features

The following features enhance the manageability of Terminal Services in Windows Server 2003:

Group Policy

Group Policy can be used to control Terminal Services properties. This enables configuration of groups of servers simultaneously, including settings for new features such as per-computer Terminal Services profile path, and disabling wallpaper while connected remotely.

Windows Management Interface Provider

A full Windows Management Instrumentation (WMI) provider allows for a scripted configuration of Terminal Services settings. A number of WMI aliases are included to provide a simple front end for frequently used WMI tasks.

Active Directory Service Interfaces

An Active Directory Service® Interface (ADSI) provider gives programmatic access to per-user, Terminal Services profile settings such as Home Directory, Remote Control permissions and others.

Printer Management

Printer management has been improved the following ways:

- Printer driver mapping has been enhanced to provide better matching in near-miss cases.
- When a driver match can't be made, the Trusted Driver Path lets you specify other standard printer drivers that you sanction on your terminal servers.
- The print stream is compressed for better slow-link performance between a server and client.

Terminal Services Manager

An improved Terminal Services Manager allows for easier management of larger arrays of servers, by reducing automatic server enumeration. This gives direct access to arbitrary servers by name, and provides for a list of favorite servers.

Terminal Server License Manager

The Terminal Server License Manager has been dramatically improved to make it easier to activate a Terminal Server license server, and assign licenses to it.

Single Session Policy

Configuring the single session policy lets an administrator limit users to a single session, regardless of whether it is active or not—even across a farm of servers.

Client Error Messages

More than 40 new client error messages make it easier to diagnose client connection problems.

Security Enhancements

The Terminal Server access model now conforms better to Windows Server management paradigms.

Remote Desktop Users Group

Instead of adding users to a list in the Terminal Services Connection Configuration (TSCC) program, you simply make them members of the Remote Desktop Users (RDU) group. For example, the administrator can add the "Everyone" group to the RDU group to allow everyone to access the terminal server.

Using a true NT Group also means access to terminal servers can be controlled through Group Policy across groups of servers.

Note To use per-NIC permissions on multi-NIC servers, administrators must still use TSCC.)

Security Policy Editor

For additional customization, Terminal Services user rights can be assigned to individual users or groups, using the Security Policy Editor. Doing so will give those users the ability to log on to a terminal server without having to be a member of the Remote Desktop Users group described above.

128-Bit Encryption

By default, connections to terminal servers are secured by 128-bit, bi-directional RC4 encryption—when used with a client that supports 128-bit. (RDC is 128-bit by default). It is possible to connect with older

clients using encryption lower than 128-bit, unless it's specified that only high-encryption clients are allowed.

FIPS Compliance

An additional encryption level, labeled "FIPS Compliant" has been added to Terminal Server in Windows Server 2003. This level of security encrypts data sent from the client to the server, and from the server to the client, with the Federal Information Processing Standard (FIPS) encryption algorithms using Microsoft cryptographic modules. This new level of encryption is designed to provide compliance for organizations that require systems to be compliant with FIPS 140-1 (1994) and FIPS 140-2 (2001) standards for Security Requirements for Cryptographic Modules.

Software Restriction Policies

Software restriction policies in Windows Server 2003 enables administrators to use Group Policy to simplify locking down terminal servers (and any other Windows Server 2003-based computer) by only allowing certain programs to be run by specified users.

See <http://www.microsoft.com/windowsxp/pro/techinfo/administration/restrictionpolicies/default.asp> for more information.

This built-in Windows feature replaces the AppSec (Application Security) tool used in previous versions of Terminal Services.

Session Directory

Terminal servers can be organized into "farms." This configuration allows clusters of load-balanced computers to appear to their users as a fault-tolerant service.

The new Session Directory feature in Terminal Services allows users to reconnect to the specific disconnected session they've left within a farm, rather than just being directed to the least loaded server when they connect.

Session Directory can use the Windows Load Balancing Service, or a third-party load balancer, and the service can run on any Windows Server 2003-based computer. However, members of the terminal server farm must be running Windows Server 2003, Enterprise Edition.

Summary

Terminal Services in Windows Server 2003 builds on the foundation of Windows 2000 Terminal Services by providing organizations with a more reliable, more scalable, and more manageable server-based computing platform. Terminal Services offers new options for application deployment, more efficient access to data over low bandwidth, and enhances the value of legacy and new, lighter-weight devices. An improved client interface, support for a wide variety of data redirection types, and an array of client deployment options, combined with new and improved server management tools and security enhancements, make it much easier to manage Terminal Services and Windows Server 2003- based computers.

Related Links

See the following resources for further information:

- [What's New in Terminal Server](http://www.microsoft.com/windows.netserver/evaluation/overview/technologies/terminalserver.msp) at <http://www.microsoft.com/windows.netserver/evaluation/overview/technologies/terminalserver.msp>
- [Windows Server Family Overview](http://www.microsoft.com/windows.netserver/evaluation/overview/default.msp) at <http://www.microsoft.com/windows.netserver/evaluation/overview/default.msp>
- [Windows Server Features Guide](http://www.microsoft.com/windows.netserver/evaluation/features/) at <http://www.microsoft.com/windows.netserver/evaluation/features/>
- [Introducing the ".NET" in the Windows Server Family](http://www.microsoft.com/windows.netserver/evaluation/overview/dotnet/default.msp) at <http://www.microsoft.com/windows.netserver/evaluation/overview/dotnet/default.msp>
- [Using Software Restriction Policies to Protect Against Unauthorized Software](http://www.microsoft.com/windowsxp/pro/techinfo/administration/restrictionpolicies/default.asp) at <http://www.microsoft.com/windowsxp/pro/techinfo/administration/restrictionpolicies/default.asp>
- [Windows Powered Thin Clients](http://www.microsoft.com/windows/powered/thinclients/default.asp) at <http://www.microsoft.com/windows/powered/thinclients/default.asp>
- [Application Deployment Using Microsoft Technologies](http://www.microsoft.com/windows2000/techinfo/howitworks/management/apdplymgt.asp) at <http://www.microsoft.com/windows2000/techinfo/howitworks/management/apdplymgt.asp>

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