Microsoft

William R. Stanek
Series Editor

Windows® Small Business Server 2011

Craig Zacker

Administrator's Pocket Consultant

Windows® Small Business Server 2011

ADMINISTRATOR'S POCKET CONSULTANT

The practical, portable guide to Windows Small Business Server 2011!

Portable and precise, this pocket-sized guide delivers ready answers for administering Windows Small Business Server 2011 Standard. Zero in on core support and maintenance tasks using quick-reference tables, instructions, and lists. You'll get the focused information you need to solve problems and get the job done—whether at your desk or in the field.

Get fast facts to:

- Install Windows Small Business Server 2011 on-premise
- Use Active Directory® to manage computers and users
- Handle core administrative tasks with the console
- Use permissions to control access to network resources
- Manage your data storage resources
- Administer email with Microsoft® Exchange Server 2010
- Monitor the performance of your servers and workstations
- Build an intranet with Microsoft SharePoint® 2010
- Migrate an existing network

About the Author

Craig Zacker is a writer, editor, and educator who has written or contributed to dozens of books on operating systems, networking, and PC hardware, including several college texts. Craig is the author of the *Windows Small Business Server 2008 Administrator's Pocket Consultant*, and coauthored the Microsoft Press® *Training Kit* for Exam 70-686.

ISBN: 978-0-7356-5154-8

90000

9 780735 651548

U.S.A. $44.99
Canada $51.99
[*Recommended*]

Operating Systems/ Windows Server

Windows® Small Business Server

Microsoft®

Microsoft®

Windows® Small Business Server 2011

Administrator's Pocket Consultant

Craig Zacker

Published with the authorization of Microsoft Corporation by:
O'Reilly Media, Inc.
1005 Gravenstein Highway North
Sebastopol, California 95472

ISBN: 978-0-7356-5154-8

1 2 3 4 5 6 7 8 9 M 6 5 4 3 2 1

Printed and bound in the United States of America.

Microsoft Press books are available through booksellers and distributors worldwide. If you need support related to this book, email Microsoft Press Book Support at mspinput@microsoft.com. Please tell us what you think of this book at http://www.microsoft.com/learning/booksurvey.

The example companies, organizations, products, domain names, email addresses, logos, people, places, and events depicted herein are fictitious. No association with any real company, organization, product, domain name, email address, logo, person, place, or event is intended or should be inferred.

This book expresses the author's views and opinions. The information contained in this book is provided without any express, statutory, or implied warranties. Neither the authors, O'Reilly Media, Inc., Microsoft Corporation, nor its resellers, or distributors will be held liable for any damages caused or alleged to be caused either directly or indirectly by this book.

Acquisitions Editor: Ken Jones
Developmental Editor: Linda Laflamme and Ken Jones
Production Editor: Holly Bauer
Editorial Production: Octal Publishing, Inc.
Technical Reviewer: Andrew Edney
Copyeditor: Nancy Sixsmith
Indexer: Lucie Haskins
Cover Design: Twist Creative • Seattle
Cover Composition: Karen Montgomery
Illustrator: Robert Romano and Rebecca Demarest

Contents at a Glance

Contents

Introduction

When local area networks (LANs) first appeared in the business world, their primary functions were to share files and printers. These are still critical applications for most business networks, but networks are able to provide many other functions as well. Virtually all business owners want to provide their users with access to the Internet and email, but they must be able to do so securely. Many businesses also want to host their own websites and run specialized applications. Windows Server 2008 R2 provides many of these functions, and other Microsoft products provide those that it does not provide. For example, Microsoft Exchange Server 2010 SP1 provides comprehensive email services and Microsoft SQL Server 2008 R2 provides a robust database management environment.

Installing and configuring these Microsoft products usually requires a certain amount of experience and expertise. Companies with the appropriate resources purchase the products they need and hire IT personnel to install and maintain their networks. However, there are a great many small businesses that cannot afford to keep full-time IT people on staff, or even purchase some of the more expensive networking software products. It is for this reason that Microsoft developed the Small Business Server 2011 product.

Microsoft Small Business Server (SBS) 2011 is a combination product that includes Windows Server 2008 R2, Exchange Server 2010, several other components, and (optionally) SQL Server 2008 R2, all for an attractive price. Even more attractive to the small business owner, however, is the fact that the product includes a setup program that installs and configures all the software components at once, using a standardized configuration that requires almost no user interaction.

In addition to the setup program, Windows SBS 2011 includes Windows SBS Console, a management program that provides simplified access to the most commonly used administrative controls. The end result is a sophisticated network environment that can support up to 75 users, and that many small businesses can afford to purchase, deploy, and maintain without full-time professional IT talent.

Who This Book Is For

Windows Small Business Server 2011 Administrator's Pocket Consultant is designed to help new and relatively inexperienced network administrators deploy and maintain a Windows SBS 2011 network. However, experienced administrators who are new to Windows SBS 2011 can also benefit.

How This Book Is Organized

The book first takes you through the process of planning a small business network, evaluating and purchasing the required hardware, installing Windows SBS 2011, and performing the required post-installation tasks. For first-time network administrators, there is a chapter called "A Networking Primer" and a section called "An Active Directory Primer," which provide background information on basic networking and directory service concepts. More experienced administrators can skip these sections or refer to them as needed.

Once you have planned, assembled, installed, and configured your network, *Windows Small Business Server 2011 Administrator's Pocket Consultant* takes you through the process of administering the various network applications using the tools provided with Windows SBS 2011. Windows Server 2008 R2, Exchange Server 2010, and SQL Server 2008 R2 are all large and complex products, each of which can support a book of its own. In fact, there are separate Administrator's Pocket Consultants for all of these products available from Microsoft Press.

Because it would not be possible to provide comprehensive coverage of all the Windows SBS 2011 components in one book of this size, *Windows Small Business Server 2011 Administrator's Pocket Consultant* concentrates primarily on the basic administrative tasks you are likely to perform frequently, using the Windows SBS Console and other tools that are exclusive to Windows SBS 2011. For example, the book only covers the process of creating user and computer objects in Active Directory Domain Services (AD DS) using the Windows SBS Console, but you can also create them using the Active Directory Users and Computers console.

Conventions Used in This Book

A variety of elements are used in this book to help you understand what you need to know and to keep it easy to read.

- **Note** To provide additional details on a particular point that needs emphasis.
- **Tip** To offer helpful hints or additional information.
- **Caution** To warn you about potential problems you should look out for.
- **More Info** To point to more information on the subject.
- **Real World** To provide real-world advice when discussing advanced topics.
- **Best Practice** To examine the best technique to use when working with advanced configuration and administration concepts.

Support and Feedback

This section provides useful information about accessing any errata for this title, reporting errors and finding support, as well as providing feedback and contacting Microsoft Press.

Errata

We've made every effort to ensure the accuracy of this book and its companion content. Any errors that have been reported since this book was published are listed on our Microsoft Press site at oreilly.com:

http://go.microsoft.com/FWLink/?Linkid=224059

If you find an error that is not already listed, you can report it to us through the same page.

If you need additional support, email Microsoft Press Book Support at *mspinput@microsoft.com*.

Please note that product support for Microsoft software is not offered through the addresses above.

We Want to Hear from You

At Microsoft Press, your satisfaction is our top priority, and your feedback our most valuable asset. Please tell us what you think of this book at:

http://www.microsoft.com/learning/booksurvey

The survey is short, and we read every one of your comments and ideas. Thanks in advance for your input!

Stay in Touch

Let us keep the conversation going! We are on Twitter:
http://twitter.com/MicrosoftPress

CHAPTER 1

Introducing Windows Small Business Server 2011

Simply put, a server is a software application that provides services or furnishes resources to other computers. Although many organizations have computers that are dedicated to server tasks, virtually any computer can function as a server. If you use your Windows workstation to share files or a printer with other users, your computer is acting as a server. Medium-size and large businesses typically have multiple computers running various server applications. Separate computers might function as file servers, mail servers, database servers, and so on. In addition to its Windows Server products, Microsoft has a full line of server applications that can provide virtually any service a business might need.

Purchasing these servers and licensing these server applications can be an expensive proposition, as can learning to install and maintain them. For small businesses, it is often not economically feasible to purchase the hardware, the software, and the expertise needed to implement a full set of business server applications. This is where Windows Small Business Server (SBS) 2011 enters the picture. Windows SBS is a single product that bundles a comprehensive set of server applications with the Windows Server 2008 R2 operating system and also provides a simplified administration interface that enables a reasonably proficient Windows user to manage all the server functions.

What's Included with Windows SBS 2011?

Windows SBS includes a number of Microsoft server applications; some are retail products, and others are available as free downloads. Even in the case of a free product, however, you benefit by obtaining it with Windows SBS in several ways, including ease of installation and automated configuration.

Windows SBS 2011, as shown in Figure 1-1, is designed for use on a network that consists of 1 server and up to 75 workstations. One primary server performs all the infrastructure services required for the operation of the network. The Premium Add-On (available as a separate product) provides the ability to install a second server and run line-of-business (LOB) applications.

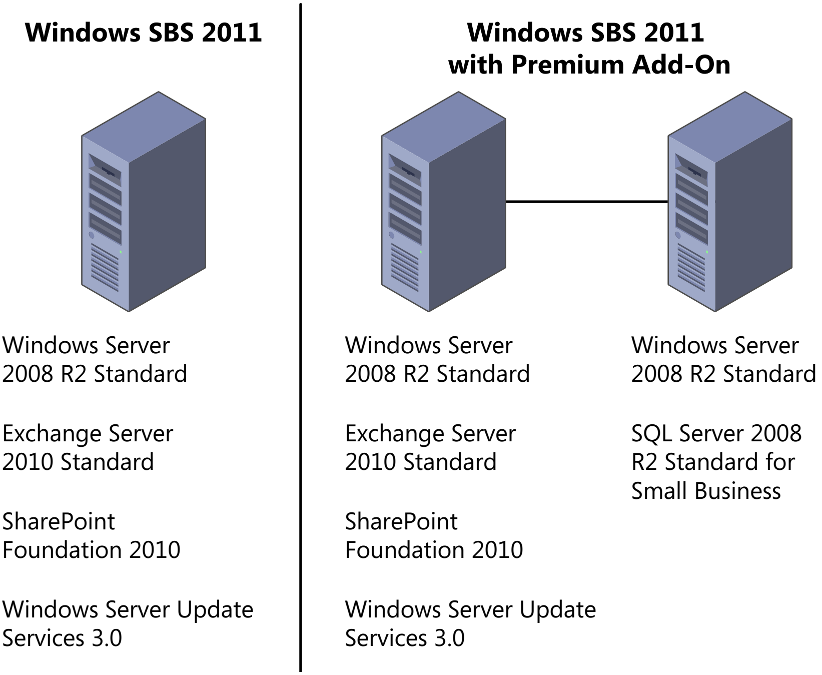

Windows SBS 2011
Windows Server 2008 R2 Standard
Exchange Server 2010 Standard
SharePoint Foundation 2010
Windows Server Update Services 3.0
Windows SBS 2011 with Premium Add-On
Windows Server 2008 R2 Standard
Exchange Server 2010 Standard
SharePoint Foundation 2010
Windows Server Update Services 3.0
Windows Server 2008 R2 Standard
SQL Server 2008 R2 Standard for Small Business

FIGURE 1-1 Windows SBS 2011 server configurations.

The following sections examine each of the components included in the Windows SBS product.

Windows Server 2008 R2

The Windows Server 2008 R2 operating system is a fundamental component of the Windows SBS package; it provides the environment in which all the other components run. Windows SBS 2011 includes Windows Server 2008 R2 Standard, with all the components found in the retail and original equipment manufacturer (OEM) operating system products.

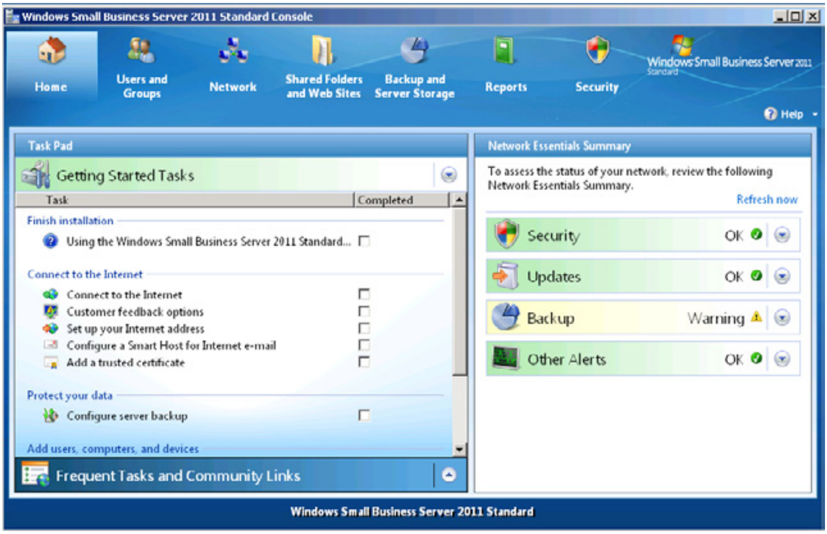
Windows Server 2008 R2 includes a large collection of applications and services, packaged as roles, many of which Windows SBS relies on to provide the infrastructure that your network needs to run. The biggest difference between Windows SBS 2011 and a standalone version of the operating system is that SBS automatically installs and configures many of these roles for you, while with a standalone Windows Server 2008 R2 product you must add the roles that define the functions you want the server to perform.

For example, to configure the server to function as a domain controller, you must install the Active Directory Domain Services (AD DS) role and then run a wizard to promote the server. When you install Windows SBS, the setup program adds the AD DS role for you, along with many of the other available roles, and configures them as needed. In a large business environment, this automatic configuration would not be practical because there are likely to be multiple servers on the network, with each one dedicated to a few specific roles. On a small business network with only one infrastructure server, however, SBS installs all the roles, services, and applications required for a typical network. You can, of course, disable elements that you do not need after the installation, or install additional roles as needed (with some limitations).

MORE INFO **For more information on exactly what components Windows SBS installs and configures during the setup process, see Chapter 3, "Installing Windows Small Business Server (SBS) 2011."**

Another big difference between the Windows SBS version of Windows Server 2008 R2 and the standalone versions is the inclusion of the Windows SBS Console tool, shown in Figure 1-2. This console, not included in the standalone versions of Windows Server 2008 R2, provides a central administration tool for all the applications and services installed with Windows SBS. This console also insulates the relatively inexperienced administrator from many of the more advanced, yet infrequently used configuration settings provided by the standard Windows Server tools. As you gain experience with Windows SBS, or if you are already an experienced Windows administrator, you still have access to all the familiar tools included with Windows Server 2008 R2.

The version of Windows Server 2008 R2 in Windows SBS 2011 includes a five-pack of the SBS 2011 Client Access License (CAL) Suite. This enables up to five users or devices to connect to the server and access its services. To support more than five users, you must purchase additional CALs. Unlike the CALs supplied with and sold for Windows Server 2008 R2, which provide clients with access only to the server, the Windows SBS CALs provide clients with access to all the applications included with the product. With Windows SBS, you do not need to purchase separate licenses for Microsoft Exchange Server clients; the SBS 2011 CAL Suite provides client access to Exchange Server 2010 as well as Windows Server 2008 R2.


Windows Small Business Server 2011 Standard Console
Home
Users and Groups
Network
Shared Folders and Web Sites
Backup and Server Storage
Reports
Security
Windows Small Business Server 2011 Standard
Help
Task Pad
Getting Started Tasks
Network Essentials Summary
Refresh now
Frequent Tasks and Community Links
Windows Small Business Server 2011 Standard

Task	Completed
Finish installation	
Using the Windows Small Business Server 2011 Standard...	□
Connect to the Internet	
Connect to the Internet	□
Customer feedback options	□
Set up your Internet address	□
Configure a Smart Host for Internet e-mail	□
Add a trusted certificate	□
Protect your data	
Configure server backup	□
Add users, computers, and devices	

To assess the status of your network, review the following Network Essentials Summary.

Security	OK
Updates	OK
Backup	Warning
Other Alerts	OK

FIGURE 1-2 Windows SBS Console.

Exchange Server 2010 Standard SP1

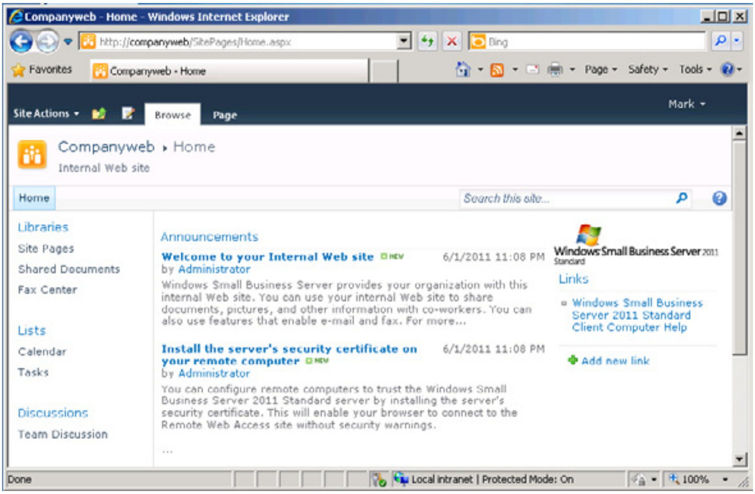
Email has become a staple of business communications, and Exchange Server 2010 is Microsoft's flagship email messaging product. Exchange Server provides an organization with internal email messaging, plus incoming and outgoing Internet email access. The mail is stored on the server so that users can access their messages from different computers and with a variety of client interfaces, including Microsoft Office Outlook on the desktop; Outlook Web Access (OWA), a web-based interface that provides access from any computer, inside or outside the enterprise; and even mobile devices, such as smart phones. In addition to email, Exchange Server also provides storage for calendar data, contacts, journals, and to-do lists, all of which users can share over the network, creating a variety of collaborative business solutions.

Exchange Server is a complex product, with many features and settings. However, in Windows SBS 2011, the main product installation process includes Exchange 2010 along with the Service Pack 1 (SP1) release. In addition, the critical configuration settings for the Exchange Server application and access to parameters for individual users are integrated into the Windows SBS Console, simplifying the administration process considerably. As with Windows Server 2008 R2, though, more experienced administrators can use the standard tools supplied with Exchange Server, such as the Exchange Management Console.

> ***MORE INFO*** **For more information on Exchange Server 2010, see Chapter 15, "Administering Email."**

SharePoint Foundation 2010

As part of its default setup procedure, Windows SBS 2011 installs Internet Information Services (IIS), the web server application included with Windows Server 2008 R2, on the primary server. Windows SBS uses IIS to host a number of websites for various administration purposes, such as client deployment and update distribution. Windows SBS also creates a default company website, as shown in Figure 1-3, using Microsoft SharePoint Foundation 2010 and the Windows Internal Database feature of Windows Server 2008 R2. SharePoint Foundation is a free, web-based collaboration environment that enables users to create, share, and edit files; schedule calendar appointments; create task lists; and participate in forum-style group discussions.



Welcome to your Internal Web site NEW 6/1/2011 11:08 PM
by Administrator
Windows Small Business Server provides your organization with this internal Web site. You can use your internal Web site to share documents, pictures, and other information with co-workers. You can also use features that enable e-mail and fax. For more...

Install the server's security certificate on your remote computer NEW 6/1/2011 11:08 PM
by Administrator
You can configure remote computers to trust the Windows Small Business Server 2011 Standard server by installing the server's security certificate. This will enable your browser to connect to the Remote Web Access site without security warnings.

...

FIGURE 1-3 A default company website created using SharePoint Foundation 2010.

SharePoint Foundation 2010 requires a SQL Server database to store user files, messages, and other information. Windows Server 2008 R2 includes a feature called Windows Internal Database, essentially a special-purpose implementation of SQL Server, which SharePoint Foundation uses by default. Do not confuse the SQL Server implementation in the Windows Internal Database with the full-featured one supplied with Windows SBS Premium Add-On. Windows SBS 2011 includes SharePoint

Foundation 2010 and installs it on the primary server using Windows Internal Database. However, if you are running the Premium Add-On, it is possible to configure SharePoint Foundation to use the full SQL Server 2008 R2 Standard product on your secondary server to host the database.

Windows Server Update Services 3.0

Regular operating system updates are a fact of life for all Windows users and administrators. Microsoft releases security updates, bug fixes, and feature enhancements on a regular basis, and Windows SBS uses Windows Server Update Services (WSUS) 3.0 to automate the process of downloading new updates and distributing them to the computers on the network.

By using a central distribution point, you can conserve bandwidth on your Internet connection by downloading updates once instead of letting each computer download its own copy. WSUS also enables administrators to evaluate and test the updates and then decide whether to deploy them to the rest of the network.

MORE INFO **For more information on WSUS 3.0, see Chapter 11, "Deploying Updates."**

SQL Server 2008 R2 Standard for Small Business

SQL Server 2008 R2 is a relational database manager application that you can use to deploy LOB applications designed to run within the environment that it provides. SQL Server 2008 R2 Standard for Small Business is included only with the Windows SBS 2011 Premium Add-On product, along with a second copy of Windows Server 2008 R2 to install on a second server.

NOTE **Unlike Windows SBS 2008 Premium, the Windows SBS 2011 Premium Add-On includes only 64-bit versions of Windows Server 2008 R2 and SQL Server 2008 R2 Standard because Windows Server 2008 R2 is available only for the 64-bit platform. Therefore, the secondary server on a Windows SBS 2011 network must be 64-bit.**

The primary server in a Windows SBS 2011 deployment performs a large number of functions, including domain controller, Exchange Server, and web server. Adding SQL Server to the mix would likely overtax the server's resources, so the Windows SBS Premium Add-On provides the software for a second computer running Windows Server 2008 R2, which runs SQL Server 2008 R2 and any applications that require its database services.

SQL Server is a database manager, which means it provides the services that applications need to store data and supply it to clients. Structured Query Language (SQL) is a language that applications use to send instructions to the database manager. The instructions enable the database manager to add information to a database stored on the server or retrieve specific information and supply it to another application.

A typical SQL Server implementation in a Windows SBS environment might consist of a web application running on the primary server along with a website that is accessible from the Internet. Users accessing the website supply information via a form, and the web server stores the information in a SQL Server database on the secondary server. Later, internal users access the information in the database using an intranet web interface or a dedicated client, as shown in Figure 1-4.

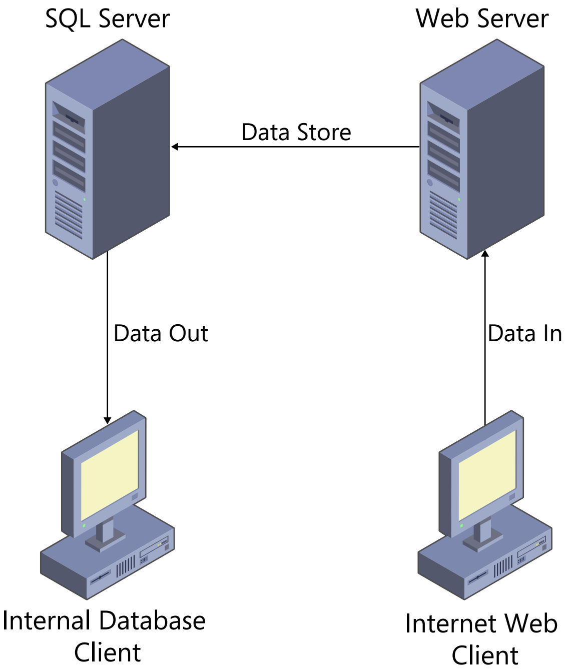


FIGURE 1-4 A typical Windows SBS SQL Server deployment.

For clients on the Windows SBS network to access the SQL Server applications, they must have a special license called the CAL Suite for Premium Users/Devices. This license is more expensive than the standard CAL Suite, but only the clients that access the database require it. If, for example, some users need access to the SQL Server databases and some do not, you can purchase CAL Suite Premium only for those who need it and then use the less expensive, standard CAL Suite for those who do not.

MORE INFO **For more information on SQL Server 2008 R2 Standard, see Chapter 18, "Adding a Second Server."**

Standard or Premium?

The question of whether to purchase the Premium Add-On for Windows SBS 2011 should be based solely on your need for a second server to run LOB applications. The functionality of the primary server remains identical, so if you do not have any applications that require SQL Server, you are better off with just the standard Windows SBS 2011 product.

The price of the Premium Add-On package is less than if you purchased its two products and the appropriate licenses separately. However, it is possible to install additional servers on a Windows SBS 2011 network that you have licensed separately.

Whichever route you choose, it is important to know that purchasing Windows SBS 2011 does not lock you into a single-server network configuration for the rest of the product's lifetime.

Why Use Windows SBS 2011?

When it comes to networking their computers, small businesses can suffer from a variety of shortcomings. The chief problem, not surprisingly, is a limited budget. Business owners accustomed to purchasing workstation software products for a few hundred dollars might be shocked at the four-figure prices of server software plus the additional cost of licensing the client users.

Another big problem for the small business owner is information technology (IT) staffing. Many small businesses cannot justify the expense of full-time IT employees, which leaves them two alternatives: train someone in the organization to manage the network part-time or hire a freelance consultant as needed.

Windows SBS 2011 addresses both of these problems in various ways, as explained in the following sections.

Pricing

One of the biggest benefits of Windows SBS 2011, as compared with the Microsoft standalone server products that it replaces, is its cost. Purchasing server operating systems and server applications can be a complicated business. You must consider the hardware requirements, operating system requirements, software interoperability, and other factors for each component. Without careful evaluation, you can end up purchasing products that do not work together or paying too much for more software than you need.

Windows SBS 2011 eliminates many of these worries by bundling together most, if not all, of the server products that a small business needs into a single package, with one set of hardware requirements and one price. Table 1-1 lists the suggested retail prices for Windows SBS 2011 and its CAL packs, as of May 2011.

TABLE 1-1 Windows Small Business Server 2011 Retail Pricing

PRODUCT	RETAIL PRICE
Windows SBS 2011 (including a 5-pack of SBS 2011 CAL suite)	US $1,096
Windows SBS 2011 Premium Add-On (including a 5-pack of SBS 2011 CAL suite for Premium Users/Devices)	US $1,604
Windows SBS 2011 CAL Suite 5-pack	US $361
Windows SBS 2011 CAL Suite 20-pack	US $1,447
Windows SBS 2011 CAL Suite for Premium Users/Devices 5-pack	US $457
Windows SBS 2011 CAL Suite for Premium Users/Devices 20-pack	US $1,831

Using these prices, the total product cost for a sample network consisting of one Windows SBS 2011 server and 25 client workstations would be US $2,543 (that is, US $1,096 for the Windows SBS 2011 product plus US $1,447 for 20 additional CALs). If you were to purchase the server software products separately, the total cost, based on the current retail prices, would add up as shown in Table 1-2.

TABLE 1-2 Cost of Products Equivalent to Windows SBS Purchased Separately

PRODUCT	RETAIL PRICE
Windows Server 2008 R2 Standard with 5 CALs	US $1029
Windows Server 2008 CAL 20-pack	US $799
Exchange Server 2010 Standard	US $699
(25) Exchange Server 2010 CALs	US $67 x 25 = US $1,675
Total	US $4,202

NOTE **SharePoint Foundation 2010 and Windows Server Update Services 3.0 are free products, and therefore add no cost to the equation. Because this is an example of a one-server network using Windows SBS 2011, SQL Server 2008 R2 is also not part of the calculations.**

Of course, there are additional costs involved in setting up a small-business network, including the client operating systems, the hardware, and various networking expenses. However, a savings of US $1,659 on the server software and client licenses is remarkable, especially when you consider that you are receiving the benefits of the unified installation and administration tools as a bonus.

System Requirements

The literature for every software product on the market includes a list of the system hardware that you need to run the software. Before you purchase a software product, you must make sure that your computer has a processor of the appropriate type and speed; sufficient memory and hard disk space; and the proper peripherals, as specified by the software manufacturer. However, for a single server running a variety of applications and services, determining exactly what hardware you need can be a problem.

In its system requirements for Windows Server 2008 R2, Microsoft specifies minimum and recommended processor speeds, amounts of memory, and hard disk sizes. However, the actual requirements of a server can vary greatly. For example, a computer running Windows Server 2008 R2 that functions only as a file server requires far less memory and disk space than one that is configured to be a domain controller. And when you install additional roles on the server, even more memory is required. Without actual testing, it would be difficult for a small-business purchaser to estimate exactly what hardware is required for a complex Windows Server 2008 R2 configuration such as the one created by Windows SBS 2011.

Complicating the matter even further are the hardware requirements for all the additional applications that you might want to install on a server. Products such as SharePoint Foundation 2010 and Windows Server Update Services 3.0 have their own requirements, which you must consider cumulatively, along with the hardware needed for the operating system. Exchange Server 2010 is even more of a problem because the hardware resources that it requires depend on the role that the individual server plays in an enterprise Exchange Server deployment.

With Windows SBS 2011, the system requirements for the product account for all the components, including Exchange Server 2010, as installed in the default configuration. You don't have to consider the roles that will be installed on the server or the additional components included with the product.

MORE INFO **The system requirements for Windows SBS 2011 are discussed in detail in Chapter 3.**

Installation

The actual process of installing the software for a server is where the question of who will administer the small-business network becomes significant. The process of installing the Microsoft server components individually can be puzzling to an inexperienced administrator.

The Windows Server 2008 R2 setup itself is relatively straightforward. Microsoft has streamlined the operating system installation process so that virtually any user familiar with the Windows interface can do it. However, once the operating system installation is completed, the administrator must add more than a dozen roles and features and, in some cases, configure them as well. Following that is the installation of Exchange Server and the other server components, some of which you must download from Microsoft's website and some of which have software prerequisites that you must install first. Overall, the server installation process is quite complicated when you use the individual software components; it requires a good working knowledge of the Windows Server 2008 R2 tools and components and some background in networking.

With Windows SBS 2011, the installation process for all the server components is performed by a single setup program. The beginning of the process is no different from a standard Windows Server 2008 R2 installation, but once the operating system is installed, the setup program prompts the user for some basic business information and then proceeds to install and configure all the necessary roles and features, as well as the additional server applications included with the product. This integrated setup routine makes it possible for virtually anyone to install Windows SBS 2011.

> ***NOTE*** **The comprehensive, integrated setup routine in Windows SBS 2011 is possible only because the designers of the product have made a great many installation and configuration decisions for the administrator to create a well-integrated, multifunction server platform. One of the big advantages of Windows Server 2008 R2 is the flexibility provided by the roles and features that administrators can install as needed. On a medium-size or large enterprise network, administrators typically use multiple servers to perform different roles. It is therefore not possible to anticipate the roles and features each server needs. Having Windows SBS 2011 is like having a knowledgeable, trustworthy administrator by your side to answer the hard questions for you.**

Administration

Once the installation of Windows SBS 2011 is complete, the server restarts and the user (after logging on) sees the Windows SBS Console. The Home page of this console contains a list of tasks the administrator should perform to get started, and the various other pages contain the most frequently used controls for the product's various components.

By integrating the most important controls into a single interface and eliminating the more advanced, less frequently used ones, Windows SBS 2011 makes it far easier for the beginning administrator to manage a small-business network.

What Can't Windows SBS 2011 Do?

There are limitations to what Windows SBS 2011 can do compared with the standalone products that comprise it. As mentioned previously, one of the main advantages of Windows SBS is its integrated installation and administration tools, and these tools exist only because the product's developers have made many important installation and configuration decisions for you. The Windows SBS server environment is carefully designed to provide most, if not all, of the services that a small business needs.

Because this configuration is so carefully wrought, Windows SBS 2011 has some limitations that Windows Server 2008 R2 does not, such as the following:

- **Only 75 users** Windows SBS 2008 is limited to a maximum of 75 client users, while there is no limit to the number of clients that a computer running Windows Server 2008 R2 can support.
- **Only 64-bit processors** The Windows SBS 2011 primary server can run only on a computer with a 64-bit processor.
- **Only one network interface** A Windows SBS primary server can have only one network interface, which means that you cannot configure the computer to function as a router, as you can with Windows Server 2008 R2, or use other technologies requiring two network adapters, such as DirectAccess.
- **No Remote Desktop Services** The primary server in a Windows SBS 2011 installation cannot function as a Remote Desktop server for any purpose other than administration. Although you can install the Remote Desktop Services role on the computer, attempts to activate the Remote Desktop Licensing server results in errors. You can, however, configure the secondary server in a Windows SBS 2011 Premium Add-On installation to function as a Remote Desktop server.
- **No upgrade from earlier versions** If you are running an earlier version of Windows SBS, you can migrate your data to a new Windows SBS 2011 server, but you cannot perform an in-place upgrade.

What's New in Windows SBS 2011?

The most obvious differences between Windows SBS 2011 and the previous version, Windows SBS 2008, are the latest versions of the software components. Table 1-3 lists the versions of the software components included in the two products.

TABLE 1-3 Software Components Upgraded in Windows SBS 2011

WINDOWS SBS 2008	WINDOWS SBS 2011
Windows Server 2008 Standard	Windows Server 2008 R2 Standard
Exchange Server 2007 Standard	Exchange Server 2010 Standard with SP1
SQL Server 2008 Standard (Premium Add-On only)	SQL Server 2008 R2 Standard (Premium Add-On only)
Windows SharePoint Services 3.0	SharePoint Foundation 2010
Windows Server Update Services 3	Windows Server Update Services 3.0

New System Requirements

As emphasized in this chapter, Windows SBS 2011 requires a computer with a 64-bit, quad-core processor, running at 2 gigahertz (GHz) or faster. Microsoft has also increased the physical memory requirement to 8 gigabytes (GB), up from 4 GB for Windows SBS 2008. Windows SBS 2011 runs reasonably well with 4 GB of memory, but it runs much better with the minimum recommended 8 GB of memory (although, as always, more is better).

Microsoft has also increased the disk space requirement. Windows SBS 2011 does not install on a disk with less than 80 GB of free space, up from 40 GB in Windows SBS 2008.

CHAPTER 2

A Networking Primer

Before you begin installing Windows Small Business Server (SBS) 2011 or even purchasing the hardware you need, you should spend time planning your network and, if necessary, learning more about how a network functions. In the planning phase, you think about what you expect to accomplish with your network and take the time to determine what you must do to achieve those goals.

For Windows SBS 2011 purchasers and administrators who have little or no computer networking experience, this section provides a basic outline of the networking concepts that apply most often when managing a Windows environment. Windows Server 2008 R2 is quite effective at keeping its networking complexities hidden, but understanding what goes on under the surface can often be a good thing.

Keep in mind that computer networking is an extraordinarily complex subject. Many engineers spend their entire careers working with one small aspect of the networking process in great detail. A brief overview such as this cannot begin to provide a comprehensive study, nor do you need one to manage a Windows SBS 2011 network. If you already have network training or experience, you might want to skip this section now and refer to it as needed.

What Is a Computer Network?

Simply stated, a network is a group of computers that are connected so that any one computer can communicate with any other computer. To build a Windows SBS 2011 network, you must purchase computers and connect them using some type of network medium. The network medium—typically composed of cables or radio frequencies—is what carries signals from one computer to another. When you send an email message to a friend, you know that the message somehow leaves your computer and travels to the recipient's computer, as identified by the destination address you used. However, the process by which the message gets from your computer to your friend's computer is far more complicated than you might think.

Clients and Servers

A client is a computer that requests access to a service or resource provided by another computer on the network, which is called a server. Although many people use the terms client and server to refer to entire computers, both of these elements are actually software components running on a computer.

All Windows computers can function as both clients and servers. When connecting to websites using a browser, retrieving email, or accessing a shared folder on another system, a computer is functioning as a client. By sharing its own printers or folders, or hosting a website using Internet Information Services (IIS), a computer is functioning as a server. If you have a few computers in your home or office, you might connect them to a switch or hub to create a network, so that they can share each other's files and printers. This is called a peer-to-peer network because all the computers are performing roughly the same client and server roles.

When you install a Windows SBS 2011 network, you are creating a client/server network because you are installing a computer that is dedicated to server functions. All the other computers, the clients, rely on the server for its resources and services. This does not mean that the clients are incapable of performing server functions, however. The clients can still share their files or attached printers, and they perform server roles by doing so. But your primary Windows SBS 2011 server provides many more server functions and does not have a user sitting at it running productivity applications, such as word processors and spreadsheets.

Protocols and the OSI Model

For teaching purposes, the networking process is often broken down into seven layers, as depicted in the Open Systems Interconnection (OSI) reference model, shown in Figure 2-1. At the bottom of the model is the physical layer, which includes the cables and other components that physically connect the computers. At the top is the application layer, which is represented by the programs that you use to initiate network communications, such as the application in which you compose and send your email. In between are various layers containing protocols that move the data from one location to another.

A protocol is a language that computers use to communicate with one another. When you write a postal code on an envelope and drop it in a mailbox, you know that postal workers all over the country know what area that code represents. Computers prepare data for transmission over a network in the same way, using protocols that they know other computers understand. Collectively, the functions at the layers of the OSI model form what is known as a protocol stack. As long as two computers are running the same protocols at each layer of the stack, they can communicate.

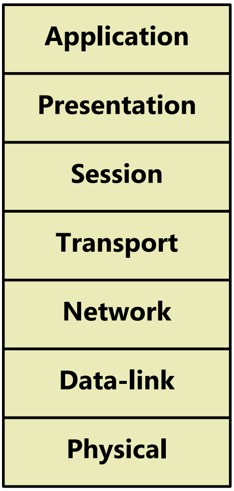


FIGURE 2-1 The OSI reference model.

Every networked computer has a combination of hardware and software components that form a protocol stack, based roughly on the OSI model. When you send an email to your friend, the message originates in the application layer in your computer and travels down through the stack to the physical layer, which transmits it over the network. When the message reaches the destination computer, it arrives at the physical layer and works its way up through the protocol stack to a program at the application layer, which your friend uses to read the message. The process is illustrated in Figure 2-2.

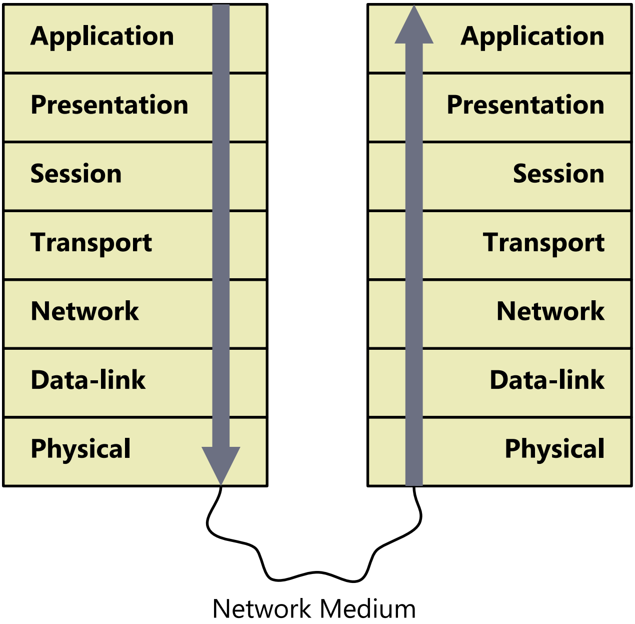


FIGURE 2-2 The network communications process.

What goes on in the various layers of the OSI model is covered in the following sections.

Networking Hardware

The physical layer of the OSI model defines the hardware that connects the computers on the network. Traditionally, the physical layer refers to network cables that carry signals using copper conductors or fiber optic threads, but today, wireless networking is an equally viable medium for the small-business network. The following sections examine the various physical components that you must consider when planning your Windows SBS 2011 deployment.

Network Interface Adapters

Every computer that connects to the network must have a network interface adapter, which is the component that transmits and receives signals, using either a cable or radio frequencies. Virtually all the personal computers sold today have at least one network interface adapter built into them. Desktop computers typically have an IEEE 802.3ab adapter incorporated into the motherboard. IEEE 802.3ab, also known as 1000Base-T or Gigabit Ethernet, is the current industry standard for cabled local area networking.

NOTE **The Institute of Electrical and Electronics Engineers (IEEE) is an international body responsible for the development, publication, and maintenance of industry standards for the electronics field. Industry standards are an essential element of computer networking because they define the protocols that products made by various manufacturers use to communicate with each other.**

Laptop computers usually have the same type of adapter and often include an IEEE 802.11 (or Wi-Fi) wireless network interface as well. If you want to connect computers without network interface adapters (or with the wrong type of adapters) to the network, you must purchase adapters for them, either in the form of network interface cards (NICs), as shown in Figure 2-3, or universal serial bus (USB) devices.

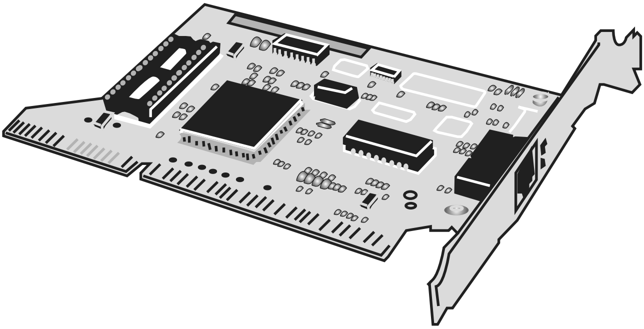


FIGURE 2-3 A network interface card (NIC).

NOTE **Most network interface adapters are compatible with previous standards, which run at slower speeds. For example, IEEE 802.3ab adapters nearly always support IEEE 802.3u (100Base-TX or Fast Ethernet) and IEEE 802.3i (10BaseT or standard Ethernet). In the same way, IEEE 802.11n wireless adapters usually support IEEE 802.1g, IEEE 802.11b, and IEEE 802.11a.**

When you are evaluating the network interface adapters built into computers or purchasing adapters to install into your computers, your primary concern should be that all the adapters on your network support the same standards and the same type of cable. In most cases, this is not a big problem. The majority of the network interface adapters for cabled networks that are manufactured today support IEEE 802.3ab, using copper cable. The exceptions are those that use fiber optic cable, which have different connectors that are easily recognized and are far more expensive.

Network interface adapters can be quite inexpensive. Low-end products are available for less than $10, although as with most things, spending a little more buys better quality. Higher-end adapters typically include support for more advanced features such as network management, which are unsupported and unnecessary on a Windows SBS 2011 network.

Network Cables

Most of the cabled networks used today use a type of cable called unshielded twisted pair (UTP). A UTP cable consists of four pairs of wires, with each pair twisted separately, inside a plastic or Teflon sheath, as shown in Figure 2-4.

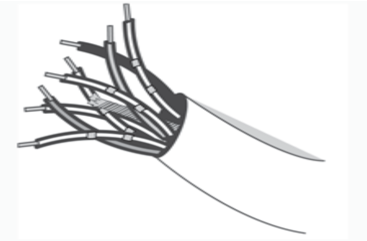


FIGURE 2-4 A UTP cable.

At each end of the cable is a male connector called an 8P8C (often referred to, incorrectly, as an RJ-45). It uses the same modular design as a telephone connector, as shown in Figure 2-5, but it has eight copper connectors instead of four. A network interface adapter has a female 8P8C connector to receive the cable, as do other networking components such as switches and routers.

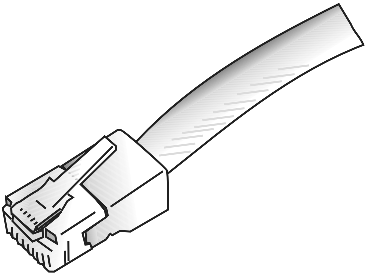


FIGURE 2-5 A UTP cable with an 8P8C connector.

When building a UTP network from scratch, you have two choices: use prefabricated cables or perform a bulk cable installation. Prefabricated cables have the connectors already attached and are available in varying lengths and colors. For a network with computers all in the same general area, prefabricated cables are relatively inexpensive and easy to install yourself. You can also roll them up and take them with you if you move. Depending on how concerned you are with appearance, you can run the cables loose along the floor or secure them to walls or baseboards with staples, as shown in Figure 2-6. If you match the color of the cables to your decor, you can achieve a reasonably professional-looking installation. Your main concern must be that the cables are protected from damage; do not run them under rugs or carpets, and make sure to protect them from foot or wheeled traffic.

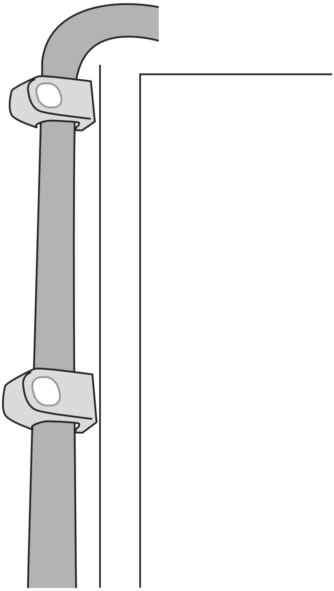


FIGURE 2-6 A UTP cable stapled in place.

A bulk cable installation usually requires a professional contractor because specialized tools and skills are involved. The installers arrive with a large spool of bulk cabling that they pull through hollow walls and ceilings, cut to fit, and attach to connectors mounted in wall plates (like those shown in Figure 2-7) or Patch panels. You then connect the computers to the wall plates using short, prefabricated patch cables. This is the most professional-looking type of installation because most of the cable is hidden inside the walls and ceilings, but it can also be substantially more expensive. If you are having telephone cables installed in a new office, however, the process for installing network cables is essentially the same, and you might be able to save money by having both installed at the same time.

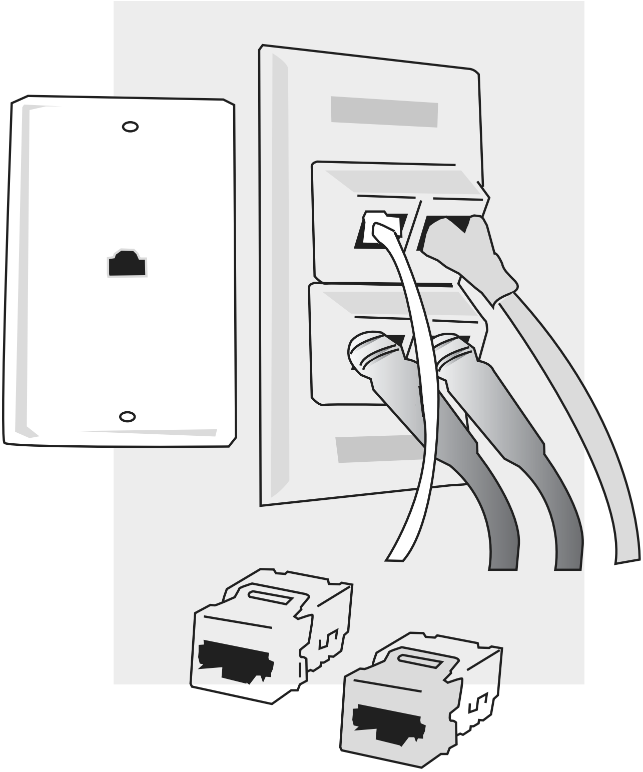


FIGURE 2-7 Wall plates used in a bulk cable installation.

The current industry standard for the installation of a data network using UTP cable is TIA/EIA-568-C, published by the Telecommunications Industry Association (TIA) and the Electronic Industries Alliance (EIA). Among other things, this standard defines several levels of performance characteristics for the UTP cabling, referred to as categories. IEEE 802.3ab networks require at least Category 5 UTP cabling, although there is also an enhanced version called Category 5e, which can provide greater reliability in certain circumstances. When you purchase prefabricated cables or contract for a cable installation, make sure that the cabling is Category 5 or 5e. You should also make sure that your installation complies with the maximum cable length specifications for your network (which is 100 meters for IEEE 802.3ab) and with all building codes in your area.

CAUTION **Installations that run cable through building air shafts, called plenums, are sometimes required to use a special type of cable that does not emit toxic gases when it burns. Whether you are installing cables yourself or contracting the job out, you alone are responsible for the network's compliance with safety codes, and you alone suffer the consequences if you use the wrong type of cable.**

Hubs and Switches

One end of a network cable connects to a computer. The other end connects to a device that joins all the separate cables into a single network. This device, called an Ethernet hub or switch, enables any computer on the network to communicate with any other computer. The hubs and switches for small-business networks are typically stand-alone boxes with a series of female 8P8C ports, as shown in Figure 2-8, and one or more light emitting diodes (LEDs) for each port.

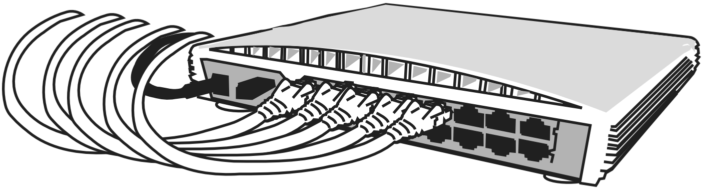


FIGURE 2-8 An Ethernet switch.

Once you connect all your computers to the hub or switch, as shown in Figure 2-9, the effect is the same as if you connected them all with a single cable. The hub or switch can forward signals arriving through any one of its ports out through one or all of the other ports, so that a signal transmitted by one computer can reach any of the other computers on the network.

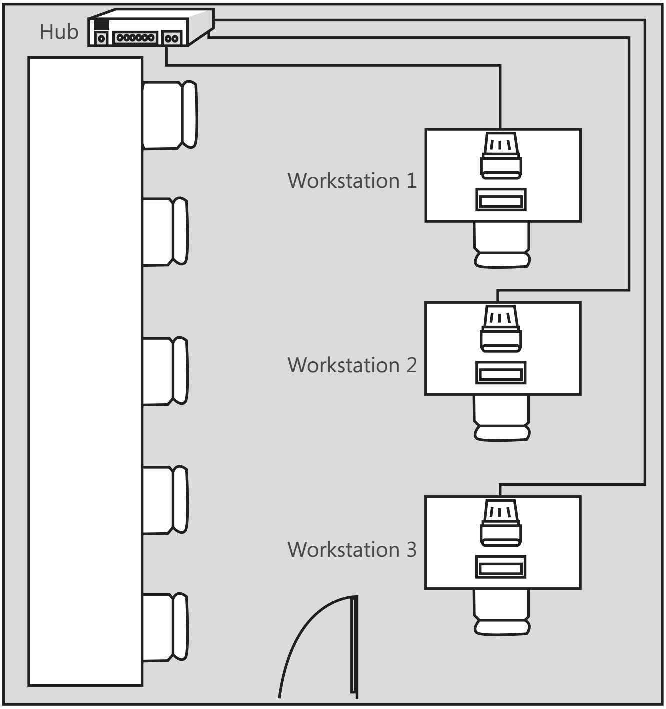


FIGURE 2-9 A network installation using prefabricated cables and a hub.

The difference between a hub and a switch is one of intelligence. A hub is a relatively simple electrical device. When a signal arrives through any one of its ports, the hub forwards that signal out through all its other ports. The hub has no intelligence, in other words. A switch is different in that when a signal arrives through one of its ports, the switch interprets the signal to ascertain its intended destination and forwards it via the port connected to the destination computer only. Because it can read the signals that it receives, a switch is said to be intelligent.

The advantage of using a switch over a hub is that it reduces the amount of traffic passing over the network. When you connect your computers to a hub, the hub always forwards transmissions destined for a single computer to all the computers on the network. This means that all the computers, except one, end up processing the incoming transmissions and discarding them. With a switch, transmissions destined for a single computer go only to that computer, as shown in Figure 2-10.

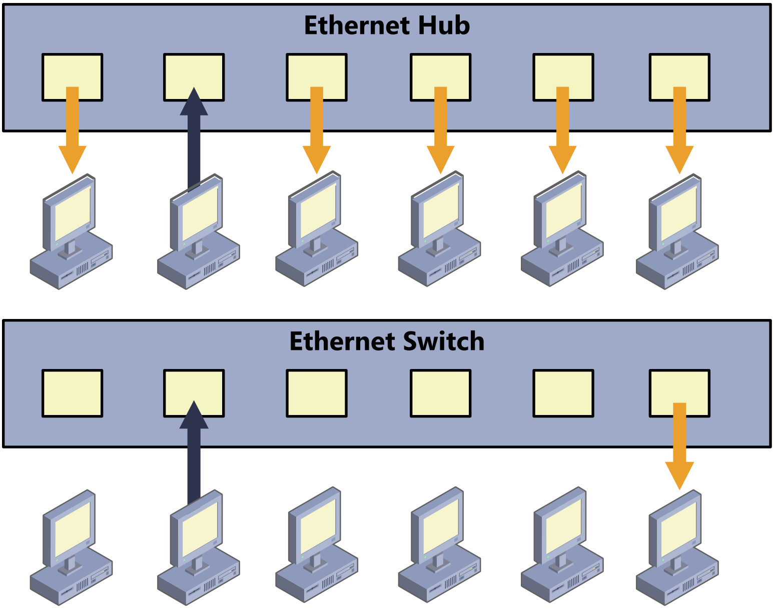


FIGURE 2-10 Network communications using Ethernet hubs and switches.

Because they are more complicated devices, switches were at one time substantially more expensive than hubs, but switches have now all but replaced hubs, particularly in the small-business–networking market. As with cables and network interface adapters, you must make sure that the hubs or switches that you purchase support the same networking standards. IEEE 802.3ab network interface adapters can run at full speed only if they are connected to a hub or switch that also supports IEEE 802.3ab.

If you are building a network using prefabricated cables, you must purchase cables that are long enough to run all the way from each computer to the hub or switch. For a bulk cable installation, the installer typically cables the wall plates at the computer locations to a Patch panel in a central location. A Patch panel is simply a cabling terminus; that is, a box or wall-mounted framework containing a sufficient number of female connectors for all the cable runs, like the panel in Figure 2-11.

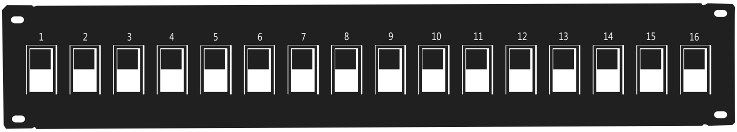


FIGURE 2-11 A Patch panel used in bulk cable installations.

Just as you connect each computer to a wall plate with a patch cord, you use another patch cord to connect each corresponding port in the Patch panel to the hub or switch.

Routers

An internetwork is a network of networks; that is, a number of connected networks. The Internet (note the capital I) is the ultimate example of an internetwork, consisting of thousands of networks all over the globe. When you connect your computers to a hub or switch, you are creating a network. When you connect your network to the Internet, you are adding it to the global internetwork.

The devices that connect networks to form internetworks are called routers. A router is a device with two network interfaces that relays traffic from one network to the other. Large enterprise installations often have multiple internal networks connected by routers. However, for the purposes of your Windows SBS 2011 installation, the only router you need is a small device that enables you to connect your network to the Internet. An Internet access router is a small box with one network interface that connects to your internal network and a second interface that connects to the network of your Internet service provider (ISP).

If you plan to use a dial-up Internet connection, you need a router containing a modem, which connects directly to a telephone line. Most small-business networks use a broadband connection, however, in which case the router has a second Ethernet adapter that you connect to the modem-like device supplied by your ISP.

Many of the routers intended for the home and small-business markets actually combine several different devices into one unit. Internet access routers often have multiple switched ports, enabling you to plug all your computers directly into the router, and might also include a wireless access point, providing connectivity for Wi-Fi devices as well.

Wireless Networking

For many small-business owners, wireless networking is an attractive alternative to cables, which can be unsightly and expensive to install. The IEEE 802.11 standards enable wireless computers to communicate with each other from any location in a typical office.

When deciding whether to build a cabled or a wireless network, you should consider the following factors:

- **Cost** Wireless network interface adapters are more expensive than copper cable adapters, and desktop computers do not have them as standard equipment (although most laptops do). Wireless networking can sometimes be cheaper in the long run, however, because there is no need to purchase and install cables.
- **Security** Wireless networks are inherently less secure than cabled networks because anyone with a wireless-equipped computer can conceivably connect to them, even from outside the premises. Therefore, you must use one of the available security protocols to encrypt your wireless network traffic, such as Wi-Fi Protected Access (WPA). Make sure that all the wireless network interface adapters you use on your network support the security protocol you plan to use.
- **Speed** IEEE 802.11n, a relatively new wireless networking standard, uses multiple antennas to run at a maximum speed of 600 Mb/sec (megabits per second). The previous standard, IEEE 802.11g, runs at a maximum speed of 54 Mb/sec, which is still sufficient for Internet access and general network use, and can usually support high-bandwidth applications such as streaming audio and video. This speed is relatively slow compared with the 1,000 Mb/sec speed of a cabled IEEE 802.3ab network, however.
- **Interference** Wireless network connections are susceptible to interference from a variety of sources, including machinery, electronics, architectural obstructions, and environmental conditions. It is a good idea to perform some tests at your network site with two or three wireless computers, under working conditions, before you make a large investment in wireless technology.
- **Peripherals** To connect printers or other devices to a wireless network, these devices must have wireless network adapters as well. There are wireless printers on the market, as well as network interface adapters made specifically for printers, but the more common solution is to create a hybrid wired/wireless network and connect standard peripheral devices using cables. In the simplest type of wireless network, you install a wireless network adapter into each of your computers, and the systems communicate directly with each other. This is called an ad hoc network, as shown in Figure 2-12.

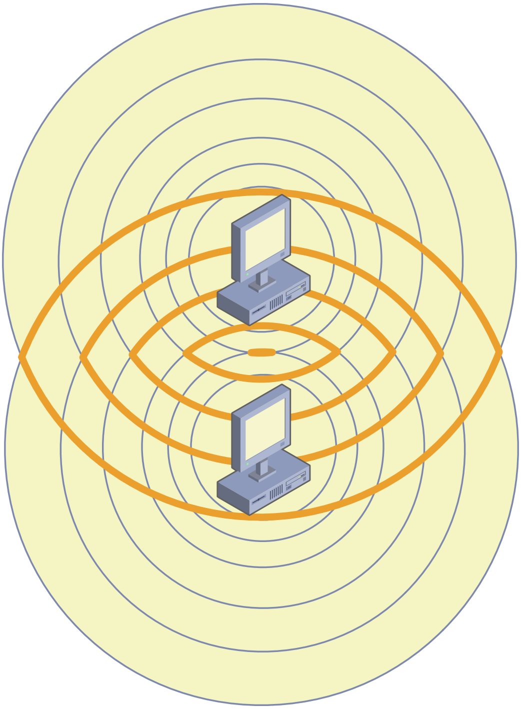


FIGURE 2-12 An IEEE 802.11g wireless network using the ad hoc topology.

The more common arrangement for wireless networks in a business environment is called an infrastructure network, in which all the wireless-equipped computers communicate with a central transceiver unit called a wireless access point (WAP), as shown in Figure 2-13. The access point functions as a hub that enables each computer to communicate with any other computer.

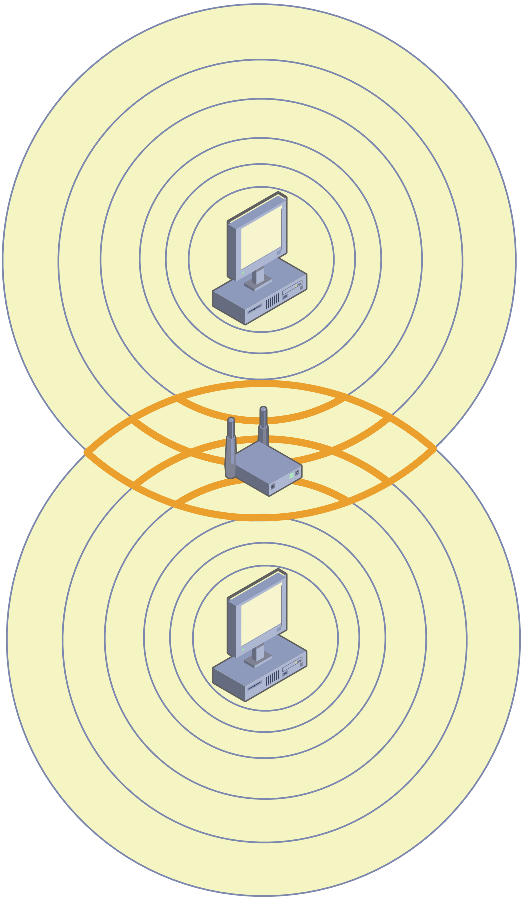


FIGURE 2-13 An IEEE 802.11g wireless network using the infrastructure topology.

The advantage of the infrastructure topology is that the access point provides wireless users with access to cabled network resources such as printers and Internet connections. In its simplest form, an access point is a small box with one or more antennas for its transceivers and a female 8P8C port for a cabled network connection. You connect the access point to a hub or switch, to which you can also connect computers or other devices. This enables any device on the network, wired or wireless, to communicate with any other device.

This type of simple access point is actually relatively rare in today's home and small office market. Most of the wireless access points available today are integrated into combination units that include routing and switching, among other capabilities. These units, which manufacturers typically market as wireless broadband routers, typically contain any of or all of the following:

- **Broadband router** Connects to the modem-like device supplied by your broadband ISP and routes traffic between your internal network and your ISP's network
- **Wireless access point** Enables wireless devices on your network to communicate with each other, with the Internet, and with cabled devices
- **Ethernet switch** Enables cabled devices on your network to communicate with each other, with the Internet, and with wireless devices
- **Web server** Hosts a self-contained web-based interface that you use to configure and manage the device
- **Dynamic Host Configuration Protocol (DHCP) server** Provides computers and other devices on your network with Internet Protocol (IP) address and other configuration settings
- **Firewall** Protects computers on the internal network from potential intruders on the Internet

This sort of device is often ideal for the typical small-business network because it enables you to create a hybrid network that uses both wired and wireless technologies, as shown in Figure 2-14. For example, you might consider installing a wireless broadband router in a closet or other central location where you plan to locate your Windows SBS 2011 server. You can connect the server, and perhaps a printer, to the switched ports using cables; use wireless connections for your clients; and provide Internet access to all by using the broadband connection.

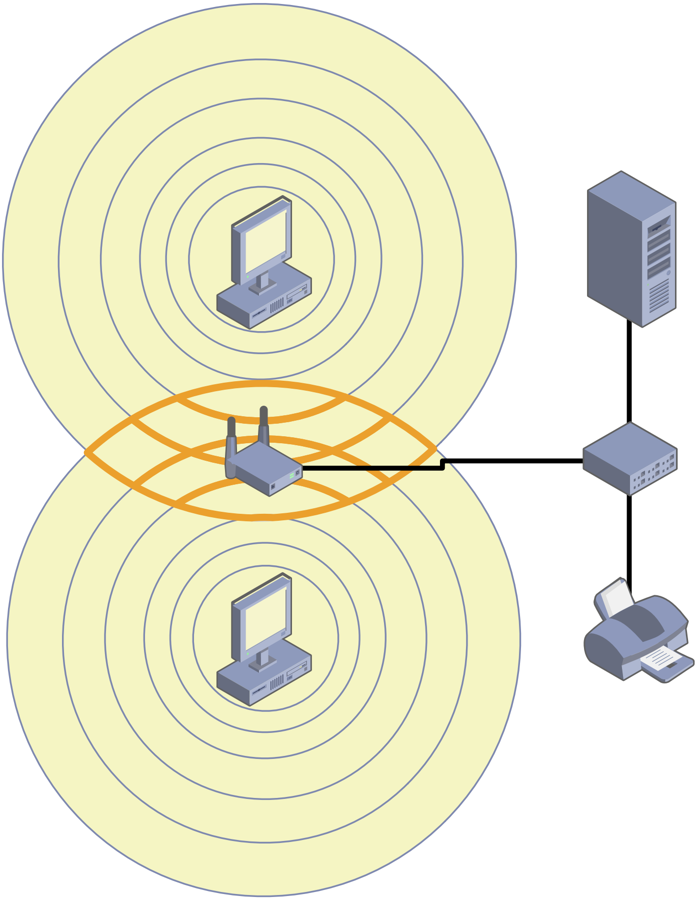


FIGURE 2-14 A hybrid network with a wireless access point cabled to a switch.

Diagramming the Network

As part of the network planning process, you should take special care when documenting everything you plan to do, especially if you will be using contractors for some or all of the installation. Create or obtain a floor plan of your site and use it to diagram the locations of all your equipment and the cable runs that connect them. This is particularly important if you are installing cables or other equipment in relatively inaccessible places, such as closets, walls, and ceilings.

Keep a record of every hardware device on your network, including the manufacturers' names, model numbers, serial numbers, and firmware revisions. This way, if you have to call for support later, you will not need to crawl through closets and under desks to find this information.

If you use contractors for cable installation or network support, make sure that you get detailed documentation of everything they do. Don't count on the contractor to maintain this documentation. The firm might go out of business, or you might decide to use someone else later.

Ethernet/IEEE 802.3

The second layer of the OSI reference model, the data-link layer, is represented by the IEEE 802.3 protocol, commonly known as Ethernet. The Ethernet protocol is responsible for the basic communication between computers on the same network. In a typical local area network (LAN), the Ethernet implementation takes the form of the network interface adapters in the computers and the device drivers that enable the computers to use the adapters.

Ethernet is a packet-switching network, meaning that the computers divide the data they want to transmit into small pieces, called packets, and transmit them individually over the network. When the packets reach their destination, the receiving computer reassembles them back into their original form. The packet-switching concept makes it possible for a computer to run multiple network applications simultaneously and for multiple computers to share a single network cable.

> ***NOTE*** **The alternative to a packet-switching network is a circuit-switching network, in which one device establishes a physical connection through the network to another device. The connection, or circuit, remains open all the time that the two devices are communicating until one or the other device terminates it. The public telephone network is an example of a circuit-switching network.**

The Ethernet protocol prepares packets for transmission by encapsulating them within a frame, which consists of a header and footer, as shown in Figure 2-15. The function of the frame to an Ethernet network is equivalent to that of an envelope in a postal system. The frame contains the address of the computer sending the packet, as well as the address of the destination computer.

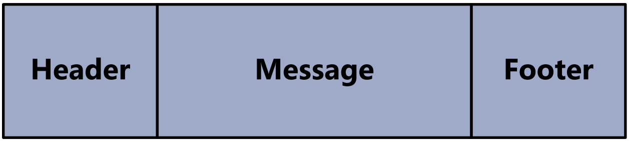
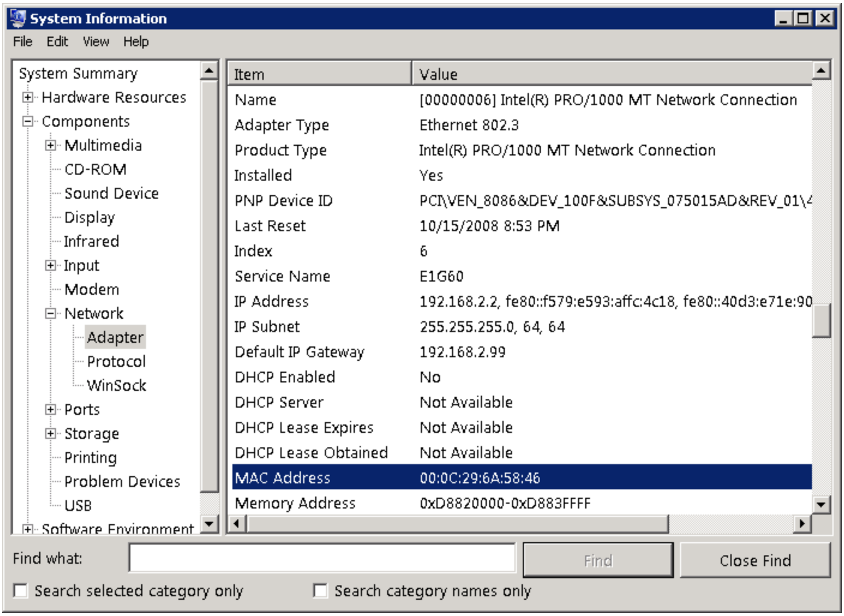


FIGURE 2-15 An Ethernet frame.

The addresses that Ethernet networks use to identify computers and other devices are called Media Access Control (MAC) addresses, or hardware addresses. A MAC address is a 6-byte hexadecimal address that network interface adapter manufacturers code into their hardware devices. The first three bytes identify the manufacturer of the adapter, and the last three bytes are a unique identifier for the individual unit. You can display the MAC address of any Windows computer using the System Information utility, as shown in Figure 2-16.



Item	Value
Name	[00000006] Intel(R) PRO/1000 MT Network Connection
Adapter Type	Ethernet 802.3
Product Type	Intel(R) PRO/1000 MT Network Connection
Installed	Yes
PNP Device ID	PCI\VEN_8086&DEV_100F&SUBSYS_075015AD&REV_01\4
Last Reset	10/15/2008 8:53 PM
Index	6
Service Name	E1G60
IP Address	192.168.2.2, fe80::f579:e593:affc:4c18, fe80::40d3:e71e:90
IP Subnet	255.255.255.0, 64, 64
Default IP Gateway	192.168.2.99
DHCP Enabled	No
DHCP Server	Not Available
DHCP Lease Expires	Not Available
DHCP Lease Obtained	Not Available
MAC Address	00:0C:29:6A:58:46
Memory Address	0xD8820000-0xD883FFFF

FIGURE 2-16 A MAC address displayed in the System Information application.

Ethernet is a complicated protocol that merits further study, but the only other issue pertinent to a Windows SBS 2011 administrator is likely to be the complicated terminology used to refer to Ethernet technologies. DIX Ethernet is the name for a particular type of packet-switching LAN technology, standardized in the 1970s by Digital Equipment Corporation, Intel, and Xerox. To create a nonproprietary standard, the IEEE published its first 802.3 document in 1983. The technology used today is based on the IEEE 802.3 standards, but the term Ethernet, along with variants such as Fast Ethernet and Gigabit Ethernet, are still in common use.

Both the DIX Ethernet and the IEEE 802.3 standards have been modified over the years to support different network media and ever-increasing transmission speeds. Another common shorthand identifier for Ethernet/IEEE 802.3 networks uses the network speed, BASE, to indicate that the network uses baseband transmissions, and a third term that indicates something about the type of network medium. The first of these identifiers was 10BASE5, referring to a 10 Mb/sec baseband network with a maximum segment length of 500 meters.

Table 2-1 lists the designations for the most common types of UTP Ethernet networks in use today.

TABLE 2-1 Ethernet UTP Designations

IEEE STANDARD	COMMON NAME	SHORTHAND IDENTIFIER	TRANSMISSION SPEED
802.3i	Ethernet	10BASE-T	10 Mb/sec
802.3u	Fast Ethernet	100BASE-TX	100 Mb/sec
802.3ab	Gigabit Ethernet	1000BASE-T	1,000 Mb/sec

NOTE **Table 2-1 does not include the many types of Ethernet/IEEE 802.3 technologies designed to run on coaxial, fiber optic, and other cable types, nor does it include standards for networking technologies that have never been successfully introduced to market.**

TCP/IP Basics

The third layer of the OSI reference model, the network layer, is where you first encounter the most commonly known networking protocols: Transmission Control Protocol/Internet Protocol (TCP/IP). Sometimes known as the Internet protocol suite, TCP/IP is a collection of protocols that encompass six of the seven layers of the OSI model. The protocol that runs at the network layer, Internet Protocol (IP), is the most important one in the suite because it carries the messages generated by most of the other protocols.

Ethernet is a LAN protocol, meaning that it is concerned only with transmitting data to other computers on the local network segment. In terms of a Windows SBS 2011 network, the computers connected to your switch, or to your wireless access point, form your LAN. IP, by contrast, is an end-to-end protocol, meaning that it is concerned with the ultimate destination of the message, not just the trip through the first (local) network.

In the same way that Ethernet uses MAC addresses to identify the recipients of its packets, IP uses its own type of address, called an IP address. And in the same way that Ethernet encapsulates information using a frame, IP performs its own encapsulation, creating what is called a datagram. An IP datagram is another envelope, with its own source and destination addresses, that will end up inside the frame envelope created by the Ethernet implementation, as shown in Figure 2-17.

Although the destination address of an Ethernet frame is always the MAC address of another device on the LAN, however, the destination IP address on the datagram in that same packet always identifies the final recipient of the message, whether it is a computer on the LAN or an Internet server thousands of miles away.

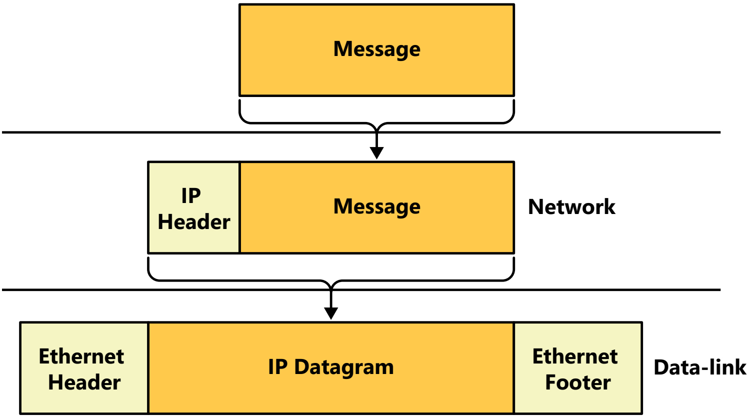


FIGURE 2-17 A message encapsulated in an IP datagram, which is in turn encapsulated in an Ethernet frame.

For example, when one of your clients attempts to access a file on your Windows SBS server, the Ethernet frame specifies the server's MAC address and the IP header contains the server's IP address. In other words, the two are different addresses referring to the same computer. On the other hand, when the client uses a browser to connect to a server on the Internet, the datagram contains the IP address of the Internet server, which is the packet's final destination, but the Ethernet frame contains the MAC address of the router that provides the LAN with access to the Internet. The two addresses point to different devices.

Because it is an end-to-end protocol, the IP address can refer to any computer, on any network, anywhere. The MAC address, however, must point to a device on the local network. Therefore, when the computer recognizes that the destination IP address refers to a computer on another network, it sends the packet to a router that provides access to other networks. The packet is then passed along, from router to router, until it reaches the network hosting the destination computer. Each journey from one router to another is called a hop, and administrators frequently measure the length of a route by the number of hops it contains.

IPv4 Addresses

As currently standardized in Internet Protocol version 4 (IPv4), IP addresses are 32 bits long and are notated as four 8-bit decimal numbers, separated by periods. This is sometimes called dotted decimal notation. Because each of the 4 decimal numbers (sometimes referred to as an octet or a quad) is 8 bits long, it can have 256 (that is 28) possible values, ranging from 0 to 255.

A TCP/IP network consists of devices, called hosts, each of which must have a unique IP address. In a personal computer, the network interface adapter is the host, so a computer can conceivably have two hosts, and therefore two different IP addresses.

An IP address consists of two parts: a network identifier and a host identifier. When IP routers forward datagrams to distant locations, they use the network identifier to locate the correct network and then use the host identifier to locate the correct computer. Unlike MAC addresses, however, IP addresses are not split neatly down the middle. The size of the network and host identifiers can vary. For example, the IP standard originally used a system called classful addressing, which specifies three address classes with different size identifiers, as shown in Table 2-2.

TABLE 2-2 IP Address Classes

CLASS	CLASS A	CLASS B	CLASS C
Subnet mask	255.0.0.0	255.255.0.0	255.255.255.0
Number of network identifier bits	8	16	24
Number of possible networks	256	65,536	16,777,216
Number of host identifier bits	24	16	8
Number of possible hosts per network	16,777,214	65,534	254

NOTE **Classes D and E exist, but are reserved only for multicast and experimental use.**

To determine where the split between the network identifier and the host identifier is located, the classful addressing system uses a value called a subnet mask. The subnet mask is another 32-bit number that in its binary form uses 1s to represent network bits and 0s to represent host bits. For example, the subnet mask for a Class A IP address is 255.0.0.0, which in binary form is 11111111.00000000.00000000.00000000. The eight 1s indicate that the first 8 bits of the accompanying IP address are the network identifier bits, and the 24 zeroes indicate that the last 24 bits of the address are the host identifier bits.

NOTE **An IP network address (that is, an address that includes zeroes for all its host bits) identifies the network itself instead of a specific host on that network.**

Unfortunately, the IP addressing system is further complicated by the fact that the split between the network and host identifier bits need not fall on one of the 8-bit boundaries. To provide greater flexibility in IP address assignments, a system called Classless InterDomain Routing (CIDR) uses a process called variable-length subnet masking (VLSM), which enables an administrator to subdivide an IP network into smaller units, thus allocating additional bytes to the network identifier. For example, an IP network can have 12 network identifier bits, resulting in a subnet mask value of 255.240.0.0 (or 11111111.11110000.00000000.00000000 in binary form).

Fortunately, you don't have to be concerned with these complexities for the purposes of administering a small Windows SBS 2011 network. The only element of CIDR that you might encounter is its alternative form of notation, which consists of a network address, followed by a slash and the length of the network identifier. For example, CIDR notation would use an address such as 10.0.0.0/12 to refer to an address using the same 12 network identifier bits.

Using Private IP Addresses

To be accessible from the Internet, a computer must have a registered IP address: an address that some authority has assigned to that computer. This is necessary because every computer on the Internet must have an IP address that is unique. The ultimate authority for IP address assignments is the Internet Assigned Numbers Authority (IANA), managed by the Internet Corporation for Assigned Names and Numbers (ICANN). However, users do not deal with IANA or ICANN directly; instead, they obtain addresses from their ISPs or web hosting services.

The assignment of registered IP addresses occurs on two levels, which is the primary reason why IP addresses have a network identifier and a host identifier. ICANN, or one of its proxies, assigns a network address to a particular registrant, and then the administrator of the network address assigns the host addresses to the individual computers on the network.

Remember that this discussion of registered addresses refers only to computers that must be accessible to clients on the Internet, such as public web servers. You do not need registered addresses for clients that access servers on the Internet. For most, if not all, of the computers on your Windows SBS 2011 network, you will use private IP addresses, which are addresses reserved for use on unregistered networks. Table 2-3 lists the ranges of IP addresses that are free for use on private networks.

TABLE 2-3 Private IP Addresses

CLASS	CLASS A	CLASS B	CLASS C
IP address range	10.0.0.0 to 10.255.255.255	172.16.0.0 to 172.31.255.255	192.168.0.0 to 192.168.255.255
Subnet mask	255.0.0.0	255.255.0.0	255.255.255.0
Number of addresses	16,777,216	1,048,576	65,536

The primary reason for using private IP addresses is to prevent the depletion of the IPv4 address space. If every client computer accessing the Internet had a registered IP address, the supply of addresses might run out. To enable computers with private IP addresses to access Internet services, routers that connect private networks to the Internet typically use a technique called Network Address Translation (NAT). The NAT router processes all the packets sent to the Internet by computers on the private network and replaces their private IP addresses with a single registered address. For packets arriving from the Internet, the NAT router performs the same process in reverse. As a result, all the computers on the private network can share a single registered address, with the NAT router taking the responsibility for sending the packets to the correct destinations.

> ***NOTE*** **The use of private IP addresses also enhances the security of a network. Computers on the Internet cannot address traffic to private networks directly; they must go through a NAT router. Therefore, the only way for an attacker on the Internet to access a computer on a private network is if the private network computer initiates the communication. Unfortunately, these attackers have developed clever schemes that dupe unsuspecting users into running programs that initiate contact with attack servers on the Internet.**

IPv6

Although IPv4 is still predominant on most private networks and on the Internet, a relatively new version of the protocol, Internet Protocol version 6 (IPv6), is gradually being introduced. The tremendous growth of the Internet during the past decade and the increasing use of TCP/IP for devices other than desktop computers, such as smart phones and handheld computers, have caused experts to fear a depletion of the existing 32-bit IP address space. IPv6 expands the address space to 128 bits, which is more than sufficiently large to provide every device on the planet with a registered address. This eliminates the need for private IP addresses or technologies designed to preserve the current address space, such as NAT.

> ***NOTE*** **To calculate the number of possible addresses provided by a given address space, one raises 2 to the power of n (that is, 2^n), where n equals the number of bits in the address space. Thus, the IPv4 address space consists of 2^{32}, or 4,294,967,296, possible addresses. By contrast, the IPv6 address space consists of 2^{128}, or 340,282,366,92 0,938,463,463,374,607,431,770,000,000 possible addresses. This number is sufficiently large to allocate 52,351,133,372,452,071,302,057,631,913 addresses to each of the approximately 6.5 billion people living today.**

Unlike IPv4 addresses, which use decimal notation, IPv6 addresses use hexadecimals. An IPv6 address consists of eight 16-bit (that is, 2-byte) values, separated by colons, as in the following arrangement:

```
XX:XX:XX:XX:XX:XX:XX:XX
```

In this arrangement, each X is an 8-bit (or 1-byte) hexadecimal value, for a total of 128 bits, or 16 bytes. An example of an IPv6 address would appear as follows:

```
FDC0:0:0:02BD:FF:BECB:FEF4:961D
```

> ***NOTE*** **In hexadecimal notation, also known as Base 16, each digit can have 16 possible values. The traditional means of representing this mathematically is to use the numerals 0 to 9 and the letters A to F to represent those 16 values. Remember, an 8-bit (1-byte) binary number can have 2^8, or 256, possible values. If each hexadecimal digit can have 16 values, 2 characters are needed to express the 256 possible values for each byte of the address (162 = 256). This is why some of the 2-byte XX values in the sample IPv6 address require 4 digits in hexadecimal notation.**

To simplify an IPv6 address, you can omit the zero blocks and replace them with a double colon, as in the following example:

```
FDC0::02BD:FF:BECB:FEF4:961D
```

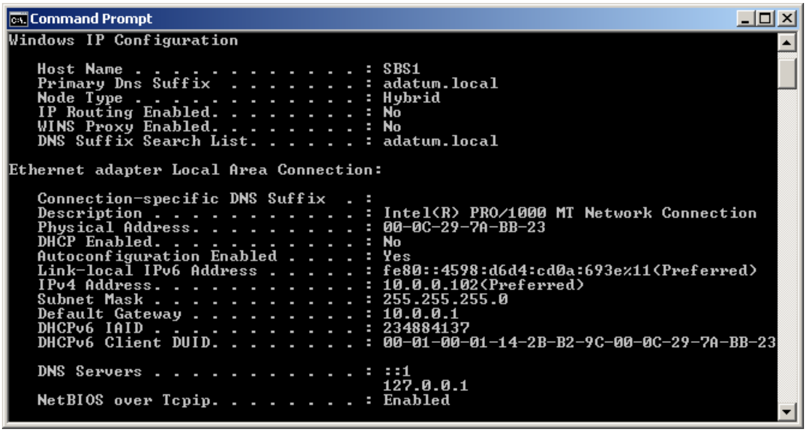
IPv6 addresses include network and host identifiers like IPv4, but they do not use subnet masks; instead, they use the same slash notation as CIDR, as in the following example of a network address:

```
21CD:53::/64
```

Because the full network identifier is 64 bits, the expanded version of this network address is as follows:

```
21CD:0053:0000:0000/64
```

At this time, Windows Server 2008 R2, Windows Server 2008, Windows 7, and Windows Vista all fully support IPv6, and automatically install both the IPv4 and IPv6 clients by default. This is called a dual IP stack. When you open a Command Prompt window and execute the ipconfig /all command, you see both the IPv4 and IPv6 addresses assigned to the computer, as shown in Figure 2-18.



```
Windows IP Configuration

   Host Name . . . . . . . . . . . . : SBS1
   Primary Dns Suffix  . . . . . . . : adatum.local
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : adatum.local

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Network Connection
   Physical Address. . . . . . . . . : 00-0C-29-7A-BB-23
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::4598:d6d4:cd0a:693e%11(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.0.0.102(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.0.1
   DHCPv6 IAID . . . . . . . . . . . : 234884137
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-14-2B-B2-9C-00-0C-29-7A-BB-23

   DNS Servers . . . . . . . . . . . : ::1
                                       127.0.0.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

FIGURE 2-18 Ipconfig.exe output displaying IPv4 and IPv6 addresses.

> ***NOTE*** **Windows Server 2003 and Windows XP include support for IPv6, but they do not install it by default. To configure these operating systems to use IPv6, you must manually install the Microsoft TCP/IP version 6 protocol driver in the Local Area Connection Properties sheet.**

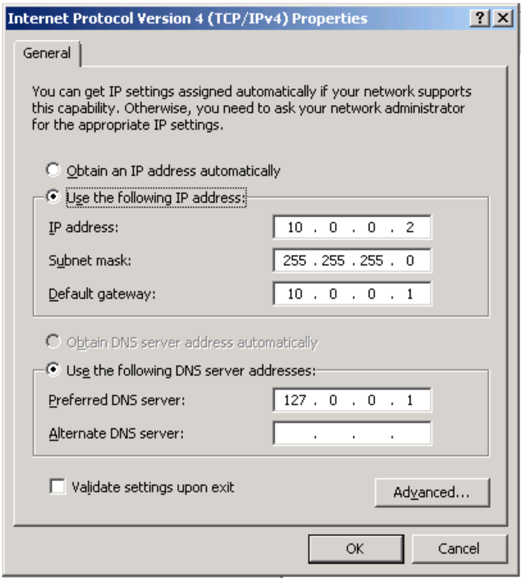
However, Internet communications are still based on IPv4, as are Microsoft Exchange Server email communications and those of most private networks. To accommodate both addressing systems, Windows includes a number of transition mechanisms that enable computers to transmit IPv6 data across IPv4 networks, including 6to4, Intra-Site Automatic Tunnel Addressing Protocol (ISATAP), and Teredo. These mechanisms function automatically, enabling any IPv6 applications you might install to function properly until the transition from IPv4to IPv6 is complete.

TCP/IP Configuration Settings

Windows computers obtain their IP addresses in one of three ways: a network administrator can assign them manually; an automated service, such as DHCP, can assign them; or the computers can self-assign them. Generally speaking, manual address assignment is difficult on a network scale. You must keep track of the addresses you have assigned to ensure that there are no duplicates on the network. Sometimes you might have to configure a Windows computer manually, however, and even if you never do, it is worthwhile knowing the functions of the various configuration parameters for the Windows TCP/IP client.

When you open the Internet Protocol Version 4 (TCP/IPv4) Properties sheet on a Windows Server 2008 computer, as shown in Figure 2-19, you see the following parameters:

- **IP Address** Uniquely identifies the computer on the network
- **Subnet Mask** Specifies which bits of the IP address form the network identifier and which bits form the host identifier
- **Default Gateway** Specifies the IP address of a router that the computer can use to access other networks
- **Preferred DNS Server** Specifies the IP address of a Domain Name System (DNS) server that the computer can use to resolve host and domain names into IP addresses
- **Alternate DNS Server** Specifies the IP address of a second DNS server that the computer can use if the preferred DNS server is unavailable


Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:
IP address: 10 . 0 . 0 . 2
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 10 . 0 . 0 . 1

○ Obtain DNS server address automatically
● Use the following DNS server addresses:
Preferred DNS server: 127 . 0 . 0 . 1
Alternate DNS server: . . .

□ Validate settings upon exit

FIGURE 2-19 The Internet Protocol Version 4 (TCP/IPv4) Properties sheet.

The Internet Protocol Version 6 (TCP/IPv6) Properties sheet contains the same parameters, but with larger fields to accept the longer IPv6 addresses. As with IPv4, Windows computers can obtain IPv6 addresses from a DHCP server or through manual configuration. IPv6 also supports stateless address autoconfiguration, in which the computer uses router discovery messages to obtain network configuration information from routers on the network.

All Windows computers that load the IPv6 client by default start out by performing the stateless address autoconfiguration process, even if they are to receive a different address from router instructions or a DHCPv6 server later.

Static vs. Dynamic Address Configuration

When you manually configure the IP address and other TCP/IP configuration parameters on a Windows computer, the values you assign are permanent; they remain in place until someone manually changes them. This is called a static IP address. When a computer obtains an IP address from a DHCP server, it is possible for the address to change at some future time. This is called a dynamic IP address.

NOTE **A DHCP server has a pool of IP addresses, called a scope, which it leases to clients on the network for a specific length of time, usually a matter of days. Each client must renew its lease periodically to continue using that address. If a client's lease expires because the system has been turned off for an extended period of time, the computer must obtain a new address the next time it starts. If the old address is no longer available, the DHCP server assigns the computer a different one.**

Client computers are better off with dynamic addresses, for several reasons. DHCP eliminates the possibility of address duplication and enables you to add, move, and remove computers without having to configure their TCP/IP parameters manually. However, servers should have static IP addresses in most cases, so that clients can always locate them.

By default, your primary Windows SBS 2011 server configures itself with a static IPv4 address on the same network as your router if it detects a router during installation. The server also configures itself as a DHCP server to provide IPv4 addresses from the same network to your client computers. However, for IPv6, all of the computers—servers and clients—assign themselves link-local unicast addresses using stateless address autoconfiguration.

Transport Layer Protocols

TCP, the other half of TCP/IP, is a protocol that runs at the fourth (transport) layer of the OSI reference model. Two primary protocols actually operate at the transport layer: TCP and User Datagram Protocol (UDP).

TCP is a connection-oriented protocol designed for the transmission of relatively large amounts of data. A connection-oriented protocol is one in which the two computers involved in a transaction exchange messages that establish a connection before they transmit any application data. TCP also provides guaranteed delivery, meaning that the receiving computer sends acknowledgments for all the data packets it receives. The result is a highly reliable transport service, at the cost of some additional network overhead.

When you use a web browser such as Internet Explorer to connect to a web server, the two computers establish a TCP connection before the browser sends its Hypertext Transfer Protocol (HTTP) request, and the server responds with a reply. The connection establishment process confirms that the two computers are ready to send and receive data and also enables them to perform other tasks, such as flow control, which regulates transmission speed. Once they have finished sending their data, the computers exchange messages that terminate the TCP connection.

By contrast, UDP is a connectionless protocol, which means that the computers do not exchange connection establishment messages. UDP is intended primarily for brief transactions that consist of a single request message and a single reply, such as DHCP and DNS transactions. When a computer sends a message to its DNS server to resolve a server name into an IP address, for example, the computer transmits a single packet containing that message by using UDP and then waits for a reply. The sending computer receives no acknowledgment; if a reply is not forthcoming, the computer simply resends the message. From a network traffic standpoint, this is far more efficient than transmitting connection establishment and packet acknowledgment messages that add up to more data than the original message.

NOTE **Network applications also use UDP for the transmission of large data files that are not bit-sensitive, such as streaming audio and video. A video stream can survive the loss of a few packets; there might be a brief interruption in the video display, but the loss is tolerable. For this reason, a nonguaranteed service is acceptable. When a computer is transmitting an application or a document file, however, the loss of a single bit can render the file unusable, so a guaranteed service such as TCP is preferable.**

Both TCP and UDP perform their own data encapsulations, just as IP and Ethernet do at the lower layers of the OSI model. When an application generates a message to be transmitted over the network, it passes it down to the appropriate transport layer protocol, which adds its own header. A message with a TCP header is called a segment, and as in IP, a message with a UDP header is called a datagram. Figure 2-20 illustrates the entire encapsulation process a packet undergoes before transmission.

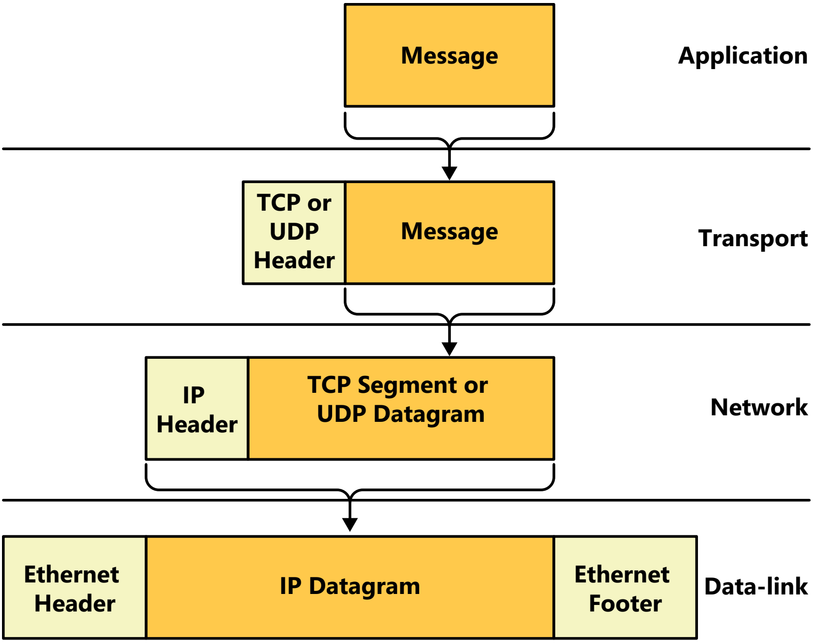


FIGURE 2-20 Transport layer encapsulation.

The transport layer protocol is not involved in getting the message to the correct destination computer; that is the job of IP and Ethernet. Instead, the transport layer protocol header contains values called port numbers, which identify the application that generated the message and the application that will receive it. Therefore, while IP is responsible for getting data packets to the correct destination computers, TCP and UDP are responsible for getting the messages in those packets to the correct applications running on those destination computers.

> ***NOTE*** **Two additional OSI model layers are located between the transport and the application layers: the session and presentation layers. No dedicated protocols operate at these layers; the transport and application layer protocols include the session and presentation layer functions.**

Application Layer Protocols

At the top layer of the OSI model, the application layer, are the protocols that provide network communication services to applications running on a computer. For example, a web browser uses HTTP to generate messages containing requests for a specific document on a web server. The messages travel down through the layers of the protocol stack, out across the network, and into the web server, in which they travel up the server's stack to the HTTP implementation there.

Among the protocols operating at the application layer are the following:

- **Hypertext Transfer Protocol (HTTP)** A protocol that web browsers and web servers use to exchange request and reply messages
- **Dynamic Host Configuration Protocol (DHCP)** A protocol and service that automatically assigns IP addresses and other configuration settings to network clients
- **Domain Name System (DNS)** A protocol and service that computers use to resolve domain and host names into IP addresses
- **Simple Mail Transfer Protocol (SMTP)** A protocol that email clients and servers use to transmit messages
- **Post Office Protocol (POP)** A protocol and service that maintains mailboxes for email clients and enables them to download their messages
- **Internet Message Access Protocol (IMAP)** A protocol and service that maintains mailboxes for email clients and enables them to store their messages on a server
- **File Transfer Protocol (FTP)** A protocol that enables clients to transfer files to and from servers, and to perform basic file management tasks
- **Telnet** A protocol that enables clients to log on to a server and execute programs from the command prompt

Understanding Domains

As noted earlier in this chapter, TCP/IP communication is based on IP addressing. Every packet transmitted over the network must have IP addresses identifying its source and its intended destination. Using numerical addresses, as TCP/IP does, is great for computers, but not as good for humans. How would you like it if whenever you wanted to access your favorite website, you had to remember a Uniform Resource Locator (URL) such as *http://192.168.43.181*?

To make these addresses easier for people to remember, TCP/IP networks use friendly names to refer to specific computers. Therefore, when you type a URL such as *http://www.adatum.com* into your web browser, the computer first converts the name to its equivalent IP address and then sends an HTTP request to the web server using that address.

The names for specific computers on a TCP/IP network, like their equivalent addresses, must be unique, so this presents a problem. How do you assign unique names to the millions of computers on the Internet without having to use long, complex strings that are just as hard to remember as IP addresses? The answer is the same as that for IP addresses: You divide the name into administrative units and let individual network administrators assign names to computers within each unit.

NOTE **The distribution of administrative tasks is one of the key architectural principles of TCP/IP and the Internet that you see again and again. Instead of creating a centralized point of administration that is responsible for all IP addresses or all domain names, the system is designed to distribute the administrative tasks among networks all over the Internet.**

On the Internet, the administrative unit is called a domain. An organization registers a domain name with ICANN or one of its many registrars, and then has the right to create host names within that domain. For example, in the www.adatum.com name mentioned earlier, adatum.com is the name of the domain, and www is the name that the domain administrator assigned to a host in that domain, in this case a web server. Together, the host name and the domain name are called a fully qualified domain name (FQDN).

Domain Namespace

Domain names are hierarchical constructions consisting of two or more words, separated by periods, reading from the bottom to the top of the hierarchy as you go from left to right. The rightmost word, com in this example, is a top-level domain name. The com domain is one of three generic top-level domains created early in the history of the domain namespace. The others are net and org. In addition to these names, there are two-letter, country-code top-level domain names that represent most of the countries in the world, such as fr for France and jp for Japan. Some additional generic top-level domains, such as biz and info, were created later.

NOTE **In addition to the generic top-level domains mentioned, there are a number of sponsored top-level domains, such as edu, gov, mil, and int, for which potential registrants must prove eligibility before they can register a name.**

The generic top-level domain names are administered by ICANN, which is also responsible for designating an appropriate trustee for each of the country-code top-level domains. Network administrators can obtain a name in any of the generic top-level domains and many of the country-code top-level domains by contacting an appropriate registrar and paying a fee. The registrant then receives all rights to a second-level domain beneath that top-level domain, including the right to create hosts and subdomains within that second-level domain.

For example, the organization that owns adatum.com registered that name and owns the rights to the name as long as it continues to pay its fees. It can, therefore, assign the host name www to its web server, creating the FQDN www.adatum.com. If the organization wants to, it can also create additional hosts and additional domain name levels, such as sales.adatum.com.

Domain Name System

In the early days of the Internet, when it was an experimental network consisting of only a few dozen computers, every system had a hosts file, which contained a simple list of all the computers on the Internet, with their host names and equivalent IP addresses. Eventually, the hosts list became too large and changed too often to be manageable, so a new solution of equating host names and IP addresses was needed.

The main reason for the hierarchical design of the domain namespace is to facilitate the creation of that new solution, which is called the Domain Name System (DNS). The fundamental design principle of the DNS is that instead of storing and managing information about the entire domain namespace in one location, the administrators of each domain are responsible for maintaining information about their own computers.

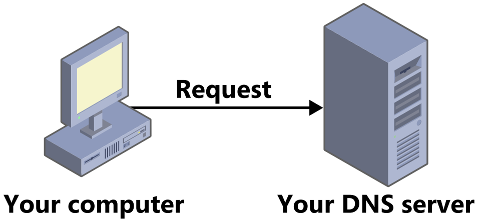
A DNS server is a specialized type of database application, designed to store name and address information about computers in a domain. When you register a second-level domain name for your organization, you must specify the addresses of two DNS servers that will become the authoritative servers for your domain. Then, for each computer on your network, you must create a resource record on your DNS server, which specifies the computer's host name and its equivalent IP address.

NOTE **Administrators can create DNS resource records manually, but computers also can create them automatically. For example, if you use the DHCP Server role on your Windows SBS 2011 server to assign IP addresses to your clients, the system automatically creates a DNS resource record for each DHCP client.**

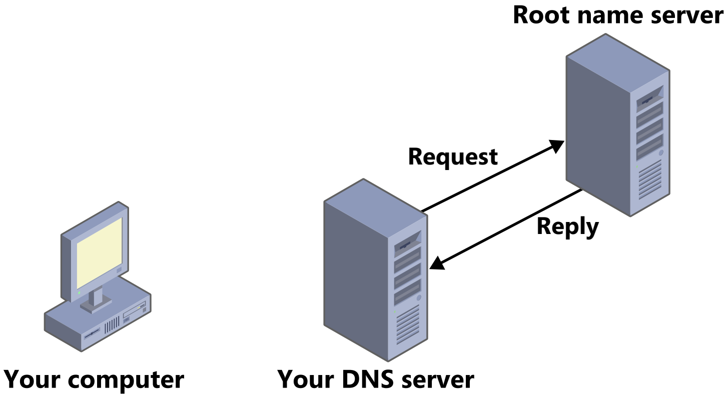
DNS Name Resolution

DNS servers are also responsible for converting host names into IP addresses at the request of clients on the network. This process is known as name resolution. In the name resolution process, DNS servers all over the Internet communicate with each other to locate the authoritative information for specific computers. This process occurs as follows:

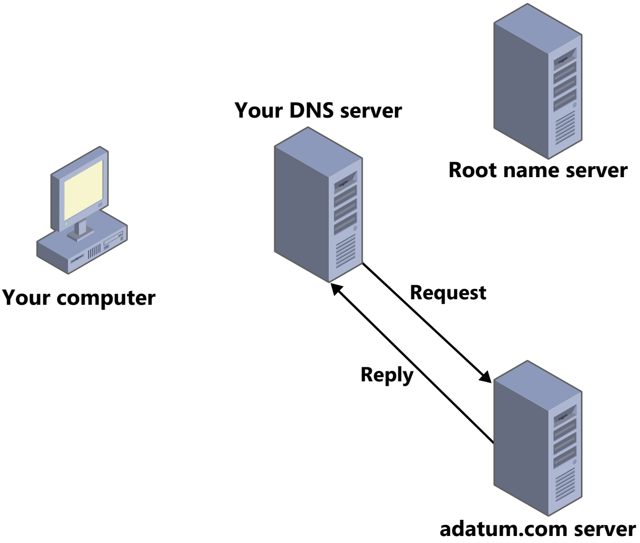
1. When you type the URL *http://www.adatum.com* into your web browser, the first thing your browser does is use your computer's DNS client, called a resolver, to send a name resolution request to your DNS server. The name of the DNS server is specified in the computer's TCP/IP configuration. This request contains the www.adatum.com FQDN, and is asking for its equivalent IP address in return. Unless your computer's DNS server happens to be the authoritative source for the adatum.com domain, it must pass the request on to other servers to get the information it needs.



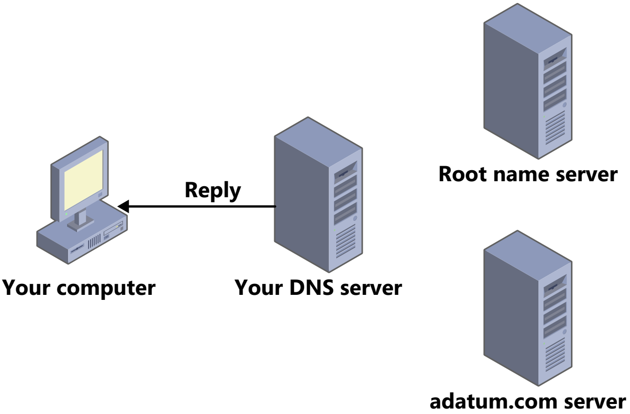
2. The DNS server starts at the top of the domain hierarchy and forwards your request to an authoritative server for the com domain. The com domain is hosted by one of the root name servers whose addresses are coded into every DNS server. Because the root name server is the authoritative source for the com domain, it contains resource records for all the second-level domains beneath com, including adatum.com. Registrars create these resource records using the information supplied by people registering second-level domains. The com server responds to the request by sending the resource record for the adatum.com domain back to your DNS server.



3. Your DNS server now knows where to go to get information about the adatum.com domain, so it forwards the original name resolution request to the adatum.com server it learned about from the com server. The adatum.com server replies by sending the resource record for the www host back to your DNS server. This resource record, which the administrator of the adatum.com domain created, contains the IP address of the www host in that domain.



4. Your DNS server now knows the IP address of the www.adatum.com computer, so it replies to your resolver's original request by forwarding the www.adatum.com resource record to your computer.



5. Your computer now has the IP address for www.adatum.com, so the computer can send its original web page access request, using that address, to the web server on the Internet.

Despite its complexity, the DNS name resolution process occurs very quickly, and it may be more or less complicated, depending on the name being resolved and current conditions on the network. For example, resolving a name beneath one of the country-code top-level domains requires an additional step because the root domain servers do not host these domains. On the other hand, the name resolution process might be abbreviated due to the caching capabilities of DNS servers.

DNS servers are designed to cache the resource records they receive from other DNS servers for a specified length of time. For example, if you use your browser to access the www.adatum.com web server, and someone else on your network tries to connect to the same website a few minutes later, your DNS server still has the www.adatum.com resource record in its cache, so it does not have to perform the entire name resolution process again.

NOTE **The DNS resource records that specify IP address equivalents for host names are called Host (A) records. However, by supporting other types of resource records, DNS servers can perform other functions in addition to name resolution. For example, Mail Exchanger (MX) records enable computers to locate the address of the mail server for a specific domain.**

Active Directory Domains

When you install Windows SBS 2011 on your server, the setup program asks you to supply a name for your domain. It is not an Internet domain name the program is referring to, however; it is an Active Directory Domain Services (AD DS) domain name. As part of the installation process, the setup program installs the AD DS role and creates a domain using the name you specify, plus the top-level domain name local.

AD DS also uses domains to create administrative divisions within a Windows network. In the case of a Windows SBS 2011 installation, you need only one domain, but large enterprise networks can have many domains, grouped into larger divisions called trees and forests. AD DS also uses DNS for name resolution as well as for other internal functions, but the AD DS domain on your server is not accessible from the Internet because local is not an official top-level domain. This protects your internal domain from Internet intrusion.

NOTE **It is theoretically possible to use the same domain name for your organization's Internet presence and for its internal AD DS domain, but this can put your AD DS domain at risk. It is also possible to use a second-level domain name, such as adatum.com, on the Internet; and create a third-level domain, such as int.adatum.com, for internal use. Using a local domain name internally and a completely separate second-level domain name on the Internet is the most secure arrangement, however, which is why Windows SBS 2011 uses this method.**

CHAPTER 3

Installing Windows Small Business Server (SBS) 2011

Although the Windows Small Business Server (SBS) 2011 setup program makes many installation and configuration decisions for you, there is still a good deal of work to do before you actually start the installation process. This chapter discusses the tasks you should perform before you begin installing your server, as well as covering the various types of installations supported by Windows SBS 2011.

Planning a Windows SBS 2011 Deployment

Planning is a crucial part of any network deployment process. The following sections guide you through the predeployment decisions you should make, including what hardware to purchase and what information you must have ready when you begin the installation.

Selecting Server Hardware

Obviously, you must have at least one server before you can install Windows SBS 2011. Table 3-1 lists the official system requirements for a server running Windows SBS 2011.

TABLE 3-1 System Requirements for a Windows SBS 2011 Server

	PRIMARY SERVER
Processor	Quad core x64 processor, 2 gigahertz (GHz) or faster 1 socket (4 sockets maximum)
Memory	8 Gigabytes (GB) minimum, 10 GB recommended, 32 GB maximum
Available disk space	120 GB minimum
Optical drive	DVD-ROM drive
Network interface	One 10/100 Ethernet adapter
Graphic display	Super VGA (1024 x 768) or higher resolution

The main requirement to consider is that the server running Windows SBS 2011 must have a 64-bit processor. In its default configuration, Windows SBS 2011 can run reasonably well on a computer with the minimum recommended hardware.

The actual hardware resources that a server running Windows SBS 2011 needs are based on a multiplicity of factors, including the following:

- **Number of users** The more users who access the server, the more likely it is that you need additional hardware resources to support them.
- **Pattern of use** Resource utilization increases when multiple users are working simultaneously. Therefore, an organization running a single shift of 30 clients will require more server resources than an organization running three shifts of 10 users each. Resource utilization also spikes if many users perform the same task at the same time, such as if 30 users log on to the domain at the same time each morning.
- **Request types** Different types of client requests can require different server resources. For example, file services can benefit from increased storage subsystem performance, while Microsoft Exchange Server can benefit from both storage performance and memory upgrades.
- **Storage requirements** The amount of storage that your applications and users require depends on their number and their activities. Users who work with video files require more storage than users working with still images, and both require much more storage than users who work primarily with text documents.
- **Additional applications** If you plan to install additional applications on your server running Windows SBS, you must account for their hardware requirements in addition to those for the default server functions.

Processors

When selecting a processor for a server running Windows SBS 2011, you certainly do not want to skimp, but you should also be aware that the performance boost you realize from a faster processor might not be worth the expense. This is particularly true at the high end of the market; the latest and fastest processors are often a great deal more expensive than those a few steps down from the top of the line.

Memory

In a server configuration, it is more important to consider the amount of memory in the computer and the maximum amount it can hold instead of comparing memory types or speeds. Memory is usually the most inexpensive way to increase the performance of a server, or indeed any computer. For a server running Windows SBS 2011, 8 GB of memory is adequate, but 10 or 12 GB would be better. You should also make sure that your server supports at least twice as much memory as you have installed initially.

> ***TIP*** **When evaluating servers, you should consider the configuration of the memory modules as well. If the computer has 8 memory slots and you plan to install 8 GB initially, do not purchase a model that comes with eight 1 GB modules, as you will have to replace some of them when you upgrade.**

Storage

Hard disk storage, like memory, is relatively inexpensive, and it is always a good idea to have more disk space than you think you need. However, for a server, you must consider not only the amount of storage space but also the configuration of the storage subsystem. Once you have decided how much storage space you need in your server, you must consider the nature of the data and its value to your organization.

Depending on the sensitivity of the data you plan to store on your server, and how critical the continued availability of that data is to your business, you might want to invest in a disk array that uses *redundant array of independent disks (RAID)* or some other high-availability technology. RAID is a system that uses two or more hard disk drives to store your data, along with duplicate or parity information that enables the server to survive a drive failure without data loss. Many servers are available with drive arrays that include RAID controllers, as well as other fault-tolerance features, such as *hot-pluggable drives* (drives that you can remove from the server and replace without having to shut the server down).

There are many different types of RAID, which are defined in numbered levels. Table 3-2 lists the RAID levels most commonly found in today's servers and storage products. There are many other RAID implementations, some of which have rarely, if ever, appeared in the market, and others that are proprietary technologies of a specific manufacturer.

TABLE 3-2 RAID Levels Commonly Found in Server and Storage Products

RAID LEVEL	RAID FUNCTIONALITY	MINIMUM NUMBER OF DISKS REQUIRED	FAULT-TOLERANT?	DESCRIPTION
RAID 0	Stripe set without parity	2	No	The system writes data one stripe at a time to each successive disk. No fault tolerance, but enhances performance.
RAID 1	Mirror set without parity	2	Yes	Also called *disk mirroring,* the system writes the same data to identical volumes on two different disks. Provides increased read performance, as well as fault tolerance.
RAID 5	Stripe set with distributed parity	3	Yes	The system stripes data and parity blocks across all the disks, without ever storing a block and its parity information on the same disk. Parity calculations add to system overhead, but provide more usable storage space than a mirror set.
RAID 6	Stripe set with dual distributed parity	4	Yes	Same as RAID 5, except that the system stripes two copies of the parity information, along with the data, enabling the array to survive the failure of two drives.

RAID LEVEL	RAID FUNCTIONALITY	MINIMUM NUMBER OF DISKS REQUIRED	FAULT-TOLERANT?	DESCRIPTION
RAID 0+1	Mirrored stripe sets	4	Yes	The system creates a stripe set and then mirrors it. Provides fault tolerance and improved performance. If a drive fails, its entire mirror set goes offline.
RAID 10 (or 1+0)	Striped mirror sets	4	Yes	The system stripes data across two or more mirror sets. Provides fault tolerance and improved performance. If a drive fails, all the remaining drives continue to function.
RAID 50 (or 5+0)	Striped RAID 5 sets	6	Yes	The system stripes data across two or more identical RAID 5 sets.

As long as you have the appropriate number of disk drives in the computer, Windows Server 2008 R2 can create volumes using RAID levels 0, 1, and 5. This is an inexpensive solution, but software-based RAID implementations can impose a penalty in system overhead. When you create a RAID 5 volume, for example, the same processor that performs all the other roles on your server must also calculate parity information for each block the system writes to the RAID array.

NOTE **In Windows Server 2008 R2, RAID level 0 is referred to as a *striped volume* and RAID level 1 as a mirrored volume. Only RAID level-5 volumes use the RAID designation in Windows.**

Hardware-based RAID takes the form of a dedicated host adapter, either integrated into the computer's motherboard or implemented as an expansion card. The host adapter performs all the necessary functions, including parity calculations, so there is no additional burden on the system processor.

High-availability hardware products, such as RAID arrays, can add significantly to the cost of a server, and it is important to understand that this technology does not eliminate the need for regular system backups. Manufacturers design high-availability products for organizations that cannot tolerate server downtime. For example, if you run an order-entry application on your server, a hard disk failure can mean lost business and lost income, so the additional expense of a RAID array might be worthwhile. However, if a server outage due to a disk failure would be no more than a minor inconvenience to your organization, then standard hard disk drives might be a more reasonable and economical solution.

Other Server Components

In their basic components, servers are different from workstations only in matters of degree; they tend to have faster processors, more memory, and larger amounts of storage space, for example. They also have no more than rudimentary graphics and sound systems, as servers have no need for high performance in these areas.

However, as you can see in the case of the RAID storage solutions, server technologies are available that greatly enhance the performance and fault-tolerance capabilities of the computer. You can also purchase servers with redundant power supplies and fans, multiple processors, and many other elaborate and expensive components. In the case of a small-business server, however, most of these components are usually not necessary, and avoiding them can save you some money.

OEM or DVD?

You have two ways to purchase Windows SBS 2011: as a retail product, in which case you receive the product on DVDs, or as part of an original equipment manufacturer (OEM) package, in which case the product comes preinstalled on a computer. The OEM option is one solution to the problem of purchasing a suitable server to run Windows SBS 2011, but it does not save you a great deal of work. The Windows SBS installation process is quite simple, so if you can conceivably save money by purchasing the computer hardware and the Windows SBS 2011 product separately, you should do so.

Selecting Clients

The clients on a Windows SBS 2011 network must be running one of the following operating systems:

- Windows 7 Professional
- Windows 7 Enterprise
- Windows 7 Ultimate
- Windows Vista Business
- Windows Vista Enterprise

- Windows Vista Ultimate
- Windows XP Professional with SP2 or later
- Windows Mobile 5.0 or later

Table 3-3 lists the published system requirements for the Windows 7, Windows Vista, and Windows XP operating systems.

TABLE 3-3 System Requirements for Windows SBS 2011 Clients

	WINDOWS 7 PROFESSIONAL, ENTERPRISE, AND ULTIMATE	WINDOWS VISTA BUSINESS, ENTERPRISE, AND ULTIMATE	WINDOWS XP PROFESSIONAL SP2
Processor	x86 or x64 processor, 1 GHz or faster	x86 or x64 processor, 1 GHz or faster	x86 processor, 300 megahertz (MHz) or faster
Memory	1 GB minimum (32-bit) or 2 GB (64-bit)	1 GB minimum	128 megabytes (MB) recommended
Hard disk space	40 GB, with 15 GB available	40 GB, with 15 GB available	1.5 GB available
Optical drive	DVD-ROM drive	DVD-ROM drive	CD-ROM or DVD-ROM drive
Network interface	Ethernet or IEEE 802.11a/b/g/n wireless	Ethernet or IEEE 802.11a/b/g/n wireless	Ethernet or IEEE 802.11a/b/g/n wireless

Selecting Network Components

The first decision to make before purchasing the networking hardware needed for your Windows SBS 2011 installation is whether you intend to build a cabled network, a wireless network, or a hybrid network that supports both. For a cabled network, you need Ethernet network interface adapters for all your computers, the cables, and an Ethernet switch to connect the computers together. For a wireless network, you need wireless network interface adapters for your computers and a wireless access point. Finally, if you plan to connect your network to the Internet, you need a router.

> ***MORE INFO*** **For the purposes of this chapter, and throughout the rest of this book, network discussions will mainly use the term *Ethernet* to refer to the packet-switching network defined in the 802.3 standards published by the Institute of Electrical and Electronics Engineers (IEEE). For a discussion of Ethernet terminology, see the section "Ethernet/IEEE 802.3" in Chapter 2, "A Networking Primer."**

Selecting an Internet Service Provider

Virtually all businesses want to connect their networks to the Internet, even if it is only for email access. Your network planning process should include a consideration of how much bandwidth your network needs and what Internet service provider (ISP) you will use to supply it. The ISP is the only networking component you need that takes the form of a service rather than a hardware product. The service provided by the ISP is also one of the regular network expenses that you must add to your budget.

The Internet bandwidth you need for your network is primarily for client connections. The server running Windows SBS 2011 is not designed to function as an Internet router or Internet web server, although the underlying Windows Server 2008 R2 operating system is capable of doing so. This is because the server is performing critical functions for your internal network, such as being an Active Directory Domain Services (AD DS) domain controller, and making it accessible from the Internet is a serious breach of accepted security practices.

> ***NOTE*** **To protect their internal networks from intrusion, small businesses that want to run websites on the Internet typically use commercial web hosting services instead of running the site from one of their internal servers.**

The typical uses for the Internet connection on a small-business network are email transfers and web browsing, neither of which requires massive amounts of bandwidth. Therefore, you can roughly calculate the bandwidth you need by allocating 50 Kbps (kilobits per second) of downstream bandwidth for each simultaneous web/email user. If you plan to support remote network access using virtual private network (VPN) connections, you should allocate another 50 Kbps of upstream bandwidth per user.

> ***BEST PRACTICES*** **Many types of Internet connections are asymmetrical, meaning that they have different upload and download speeds. Most broadband connections, for example, provide much more downstream bandwidth than upstream. When evaluating Internet connection services, be sure to consider your upstream as well as downstream bandwidth needs.**

Using these calculations, you can assume that a Windows SBS 2011 network with 25 internal users needs approximately 1,250 Kbps (1.25 megabits per second, or Mbps). A standard broadband connection from a cable or digital subscriber line (DSL) provider can usually meet these needs. Networks with more users might require a higher-speed connection.

> ***TIP*** **Do not confuse network bandwidth speeds, which are measured in kilobits (Kb), megabits (Mb), or gigabits (Gb) per second, with the download speeds displayed by your computers, which are measured in kilobytes (KB) or megabytes (MB) per second. One byte equals 8 bits, so one kilobyte equals 8 kilobits.**

While calculations such as these can give you a rough idea of how much bandwidth your network needs, the most practical method of approaching the problem is to begin by determining what types of Internet connections are available at your location. Small businesses typically use standard consumer ISPs; they generally do not have the bandwidth needs or the budget for elaborate connection technologies such as T-1 lines. In most areas, you should be able to select from the following types of providers:

- **Dial-up** Available anywhere there is a telephone line, dial-up connections are inexpensive but slow, with a maximum bandwidth of 56 Kbps that line quality can reduce even further.
- **DSL** A digital subscriber line (DSL) connection is supplied by a telephone provider using the available bandwidth on a standard telephone line. Consumer DSL connections are asymmetrical and are often available in multiple speeds that can range from 256 Kbps to 20 Mbps, for varying prices. DSL availability and reliability depends on the distance from your location to the provider's nearest central office.
- **Cable** Delivered over the same private fiber optic network used for cable television services, cable-based Internet connections are asymmetrical and can often exceed DSL in their bandwidth capabilities. Typically available in two or more tiers of service, cable download speeds can reach as high as 50 Mbps.
- **Satellite** Similar in speed, but generally more expensive than cable or DSL, satellite Internet providers target customers in remote locations that have no access to other high-speed Internet services.

When contacting the ISPs that service your area, you should find out what connection speeds they provide and, of course, the prices. When discussing the price of a connection, be sure to consider the following points:

- **Contracts** Some ISPs discount the monthly connection fee if you sign a contract for a year of service or more. You might want to evaluate the service for a month or two before you commit, but the savings can be significant. Bear in mind, however, that there are penalties for early termination of the contract.
- **Hardware leasing** Broadband connections require a modem. In many cases, you must choose between leasing a modem from the ISP, for an additional monthly fee, and purchasing one outright. The modems are usually not expensive, and purchasing the device can often begin saving you money within one or two years.
- **Networking** Some ISPs have different tiers of service, and different prices, for business customers or customers who connect the service to a network rather than a single computer.

In most cases, small-business administrators decide on one of the broadband solutions available in their area. Depending on the ISP and the conditions of your site, you might have to schedule an installation, but in some cases, you can obtain a self-installation kit and connect the modem to the ISP's network yourself.

Selecting a Router

In many ways, the key component for your network is the router because you will probably purchase a unit that combines the broadband routing function with other important networking components. The components in the router that you select often dictate what features you have to look for in your other networking equipment.

For a small-business network, a consumer-grade router that also includes firewall and network connectivity functions is usually sufficient. Business-grade products are more expensive and usually separate the routing capabilities from the other functions, forcing you to purchase individual router, switch, and wireless access point products. If you choose to purchase separate components, you must be sure that all the products you select are compatible in the networking standards and protocols that they support.

> ***TIP*** **A consumer-grade broadband router typically includes an Ethernet switch, a wireless access point, or both. In most cases, the difference in price between a unit with wireless capabilities and one without is minimal, so you might consider purchasing a broadband router with both wireless and cabled Ethernet switching capabilities, even if you do not plan to use one or the other right away.**

The consumer-grade router that you choose for your network should have all or most of the following capabilities:

- **Broadband connectivity** The device has an Ethernet wide area network (WAN) port, which connects to your broadband modem using a standard Ethernet patch cable. A broadband client built into the unit enables you to specify the user name and password for your ISP account, as well as configure account parameters.
- **Switched Ethernet ports** Virtually all broadband routers have at least one switched Ethernet port, but few have more than four or five. If you intend to have more than a few cabled devices on your network, you need a separate Ethernet switch that provides a larger number of ports. The switched ports on most routers support standard 10 Mbps Ethernet (10Base-T) and 100 Mbps Fast Ethernet (100Base-TX). If you have 1,000 Mbps Gigabit Ethernet devices on your network, they automatically negotiate down to Fast Ethernet when you connect them to the switch.

TIP **If you are running a Gigabit Ethernet network with a separate switch, plugging the router into the switch establishes a connection at 100 Mbps. There is no need to search for a broadband router with Gigabit Ethernet ports because the connection between the switch and the router only carries traffic to and from the Internet, and Internet connections run at far slower speeds than local area network (LAN) connections.**

- **Wireless access point** Routers with wireless networking capabilities have antennas, a transceiver, and an access point that enables wireless devices to connect to the network. Virtually all of the wireless routers on the market today support the 54 Mbps IEEE 802.11g standard, but they can also support devices using the slower IEEE 802.11b and IEEE 802.11a standards. Many devices also now support the newer IEEE 802.11n standard, which can provide speeds up to 600 Mbps.
- **Wireless security protocols** While older wireless devices can usually connect to an IEEE 802.11g transceiver, they might not support the latest wireless security protocols. Most of the current wireless router products support the Wi-Fi Protected Access (WPA and WPA2) security protocols, while older devices might support only *Wired Equivalent Privacy (WEP)*, which has critical weaknesses. Routers can typically use only one wireless security protocol at a time, so all your wireless devices must support the protocol that you elect to use.
- **Web-based administration** Broadband routers typically have an internal web server that you access to configure the device's properties. You therefore must connect a computer to the router before you can use it to connect to your ISP's network.
- **Dynamic Host Configuration Protocol (DHCP) server** Most routers include DHCP server capability, which enables them to assign Internet Protocol (IP) addresses and other Transmission Control Protocol/Internet Protocol (TCP/IP) configuration settings to clients on the network. Windows SBS 2011 also includes a DHCP server. You must decide whether you want to use DHCP to configure your client workstations, and if so, which DHCP server implementation you want to use.
- **Universal Plug and Play (UPnP)** UPnP is a set of protocols that enable devices on the same network to communicate and automatically configure their networking settings. Windows SBS 2011 can communicate with a UPnP router to determine what IP address it should use and open the appropriate firewall ports for the services running on the computer.

- **Network Address Translation (NAT)** NAT is the router technology that enables the computers on your internal network to use private IP addresses and still access the Internet. NAT also protects your network from Internet intrusion.

  MORE INFO **For more information on NAT, see the section "Using Private IP Addresses," in Chapter 2.**

- **Virtual private networking (VPN)** A VPN connection is when an authenticated user at a remote location connects to the Internet and accesses your private network through your router. This enables users who are traveling or working at home to access their files, Exchange Server email, and other network resources. To enable VPN connections, the router must be able to open the appropriate port for the VPN protocol the client uses to connect to the network server.
- **Access restrictions** Many broadband routers enable you to specify which of the computers on your network are allowed to access the Internet, or restrict Internet access to certain days and times. These features can prevent casual intruders from accessing the Internet through your router, but they are relatively ineffective against determined and knowledgeable attackers.
- **Content filtering** Many broadband routers enable you to block client access to specific network services on the Internet, specific website addresses, or websites containing specific keywords. Knowledgeable users can often find ways to bypass these features, but they are reasonably effective on casual users.
- **Firewall** Broadband routers usually have a variety of firewall features that are designed to protect your network from various types of attacks. Features such as packet filtering and *stateful packet inspection (SPI)* analyze incoming traffic to limit the network's susceptibility to specific types of attacks from the Internet.

Selecting Cables, Adapters, and Switches

If you decide to install a cabled network, you must have an Ethernet network interface adapter in each of your computers; a switch that functions as the central connection point; and, of course, the cables themselves. As mentioned in Chapter 2, the main concern when selecting Ethernet equipment is that all the components support the same standards.

CABLES

Choosing cables is a relatively simple matter. If you plan to use prefabricated cables throughout the network, purchase Category 5 or 5e cables of appropriate lengths. The maximum length for the cable connecting an Ethernet device to the switch is

100 meters. Category 5e cable is more expensive than Category 5, and the standards do not require it, but if you are planning to run Gigabit Ethernet throughout your network, Category 5e cable is usually worth the additional expense.

If you are having bulk cable installed at your site, make sure that the contract calls for all cables and connectors to be Category 5 or 5e. You also must purchase prefabricated patch cables to connect your computers to the wall plates and your Patch panel ports to the switch. These too must be Category 5 or 5e. As with a chain, it's important to remember that a network connection is only as strong as its weakest link.

MORE INFO **For more information about purchasing and installing cables, see the section "Network Cables," in Chapter 2.**

NETWORK ADAPTERS

Nearly all the desktop computers sold today have an Ethernet adapter integrated into the motherboard. Higher-end workstations and virtually all servers have 1,000 Mbps Gigabit Ethernet adapters, while some budget workstations have 100 Mbps Fast Ethernet. No matter what the maximum speed, however, most Ethernet adapters and switches can negotiate down to accommodate slower speeds. For example, if you plug a computer with a Gigabit Ethernet adapter into a Fast Ethernet switch, the two devices negotiate the fastest speed they have in common, which is 100 Mbps. Switches perform separate negotiations on each port, so it is possible to mix Ethernet devices running at different speeds on the same network.

NOTE **For most network applications, 100 Mbps Fast Ethernet is more than sufficient. However, if many of the computers that you intend to purchase have integrated Gigabit Ethernet adapters, a Gigabit Ethernet switch is not that much more expensive than a Fast Ethernet one.**

If you have computers with no Ethernet adapter or if you want to upgrade a computer to a faster Ethernet standard, you can purchase network interface cards (NICs) that plug into an expansion slot. Before you select NICs, be sure that each computer has a free slot and check what type of slot it is. For computers without free slots, there are external network interface adapters available, which plug into a universal serial bus (USB) port.

Higher-end adapter cards frequently have integrated network management functionality, which provides the device with the ability to report its status to a centralized Network Management console. For a small business network, this capability is not needed, so when evaluating adapters, don't reach for the cheapest adapters in the market, but don't buy the most expensive ones, either.

SWITCHES

Apart from the Ethernet standards they support, the other main issue when purchasing a switch is the number of ports. Switches are available in a variety of sizes, with as many as 48 ports, often clustered in multiples of 8. As with computer memory or hard disk space, buying more switch ports than you think you need is usually a good idea. Having a switch with extra ports enables you to expand your network later simply by plugging additional computers or other devices into the switch.

When evaluating switches, you will notice that prices range from under US $100 to well up in the tens of thousands of dollars. For a small business, you are again more likely to be looking at lower-end, consumer-grade switches rather than high-end, enterprise network products. Some of the other features that you might encounter when shopping for a switch are as follows:

- **Form factor** Most small-business networks want external switches and routers; that is, freestanding devices with their own cases and power supplies. Networking devices are also available in rack-mounted form factors, which are efficient and convenient if you have a formal data center but are beyond the means of most small businesses.
- **Uplink negotiation** A twisted pair cable contains some wires that are dedicated to transmitting data and some that are dedicated to receiving it. For communication between two devices to occur, the transmit pins on one have to be crossed over to the receive pins on the other. Ordinarily, the switch performs this crossover. However, when you expand a network by connecting a second switch to your first one, the two crossovers cancel each other out. Older Ethernet hubs and switches have a designated *uplink* port, which lacks the crossover circuit, for a connection to another hub or switch. Modern switches have an *uplink negotiation* feature that enables all the ports to detect automatically whether they are connected to a computer or another switch and adjust the crossover circuit accordingly. This is a feature worth having, which adds little cost to the device.
- **Management** A managed switch, like a managed router or other network component, is a device with one or more interfaces that administrators can use to control its operation. This is a high-end, enterprise networking feature that most small-business networks do not need and cannot afford. Unmanaged switches are preferable for virtually all Windows SBS 2011 networks.

Diagramming the Network

As you decide what computers and components to purchase, you should create a diagram showing the layout of the network. Figure 3-1 shows a typical hybrid network for a small business with one server running Windows SBS 2011, eight workstations, and a broadband router that also contains a wireless access point. All the computers and the router are connected to an Ethernet switch.

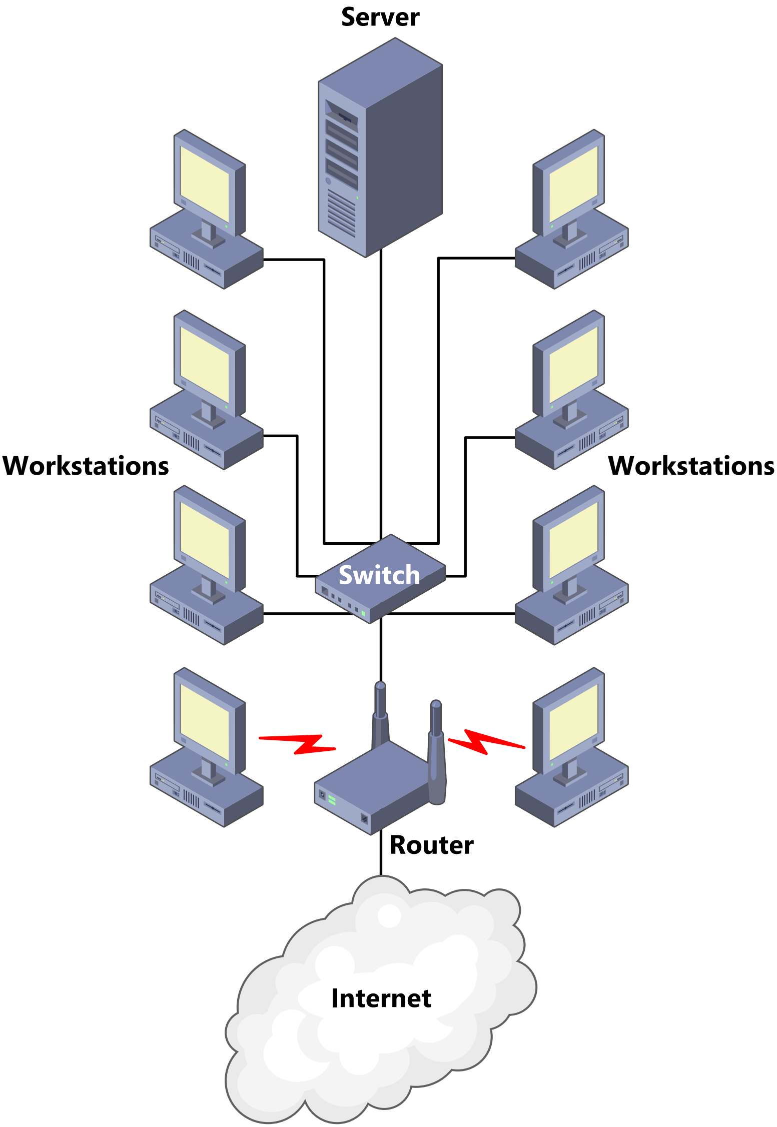


FIGURE 3-1 Diagram of a typical hybrid network.

This type of diagram is useful as a guide for building your network and as a reference, especially if you must familiarize employees or consultants with the network layout. However, this type of diagram shows only the relationships between the components; it is not a true map of your site showing the actual equipment locations. If you are opening a new office or renovating an existing one, and you have a floor plan available, you might want to create a second diagram that shows not only the exact placement of each component but also the cable runs connecting them.

REAL WORLD **If you are having a bulk cable installation performed by a contractor, you should insist on a diagram showing the locations of all the cable runs. This way, if you ever need to service or upgrade the cabling, you do not have to search for them inside walls or ceilings.**

Preparing for the Installation

Once you have selected and purchased all the hardware and software that you need to build your network, you can begin assembling the pieces and collecting the information you need to perform the Windows SBS 2011 installation.

Physical Security

Selecting a secure location for your network components is an important first step in the deployment process. You must choose a location that protects your servers, routers, and switches from theft, damage (accidental or otherwise), excessive heat and moisture, electromagnetic interference, airborne dust and fumes, and other extreme environmental conditions. You should also have a clean source of power for your equipment, which, in the case of your server, means an *uninterruptible power supply (UPS)* that both conditions the power and provides battery backup in case of a power outage.

BEST PRACTICES **UPS devices are available in three types: offline, line interactive, and online. Both offline and line interactive devices perform a brief transition when a power failure occurs, while online UPSs do not because they always supply the computer with power from the continuously replenishing battery. Therefore, even though it is more expensive, an online UPS is preferable for your servers.**

When it comes to physical security, wireless access points are a special case for several reasons. First, while the wireless radio signals can penetrate walls and other barriers, they are susceptible to *attenuation*, meaning that the signals weaken when they have to pass through too many barriers or barriers that are too dense. If the signal between a computer and the access point becomes sufficiently weak, the system might have to drop down to a slower transmission speed or even lose the connection entirely. Second, there is the danger of outside intrusion occurring when you place the access point too close to an outside wall. Choosing a central location within your building can help prevent unauthorized users in the parking lot from connecting to your network.

Connecting Your Router

If you are using a shared broadband Internet connection for your network, you should consider setting up the connection and your router before you install your server running Windows SBS 2011. It is not absolutely necessary, but there are multiple benefits to doing so. During the installation, the Windows SBS 2011 setup program attempts to detect a UPnP router on the network by transmitting a variety of discovery messages and listening for replies. If the server locates a router and can access the Internet through that router, it proceeds as follows:

- The server configures its own TCP/IP client with a static IP address on the same subnet as the router and with the router's IP address as its Default Gateway address.
- With the installer's permission, the server downloads the latest operating system updates from Microsoft's website and installs them during the installation process.

After the Windows SBS 2011 installation, when you run the Connect To The Internet Wizard, if the server detects an operational DHCP server on the router, the server configures its own DHCP server to distribute IP addresses on the same subnet as the router and then disables the router's DHCP server.

If the server fails to detect a router on the network during the Windows SBS 2011 installation, it configures its own TCP/IP client with the static IP address 192.168.0.2 and no default gateway address. The server still installs the DHCP Server role during the installation, but it does not configure or activate the DHCP Server service. After the installation is completed, you must configure the DHCP Server on the router or the server manually if you want to dynamically allocate IP addresses to your network clients.

MORE INFO **For more information on configuring DHCP, see Chapter 13, "Managing Windows SBS 2011."**

The procedures for installing your broadband Internet connection and your router vary depending on your ISP and router manufacturer. However, in most cases, you must perform the following basic steps:

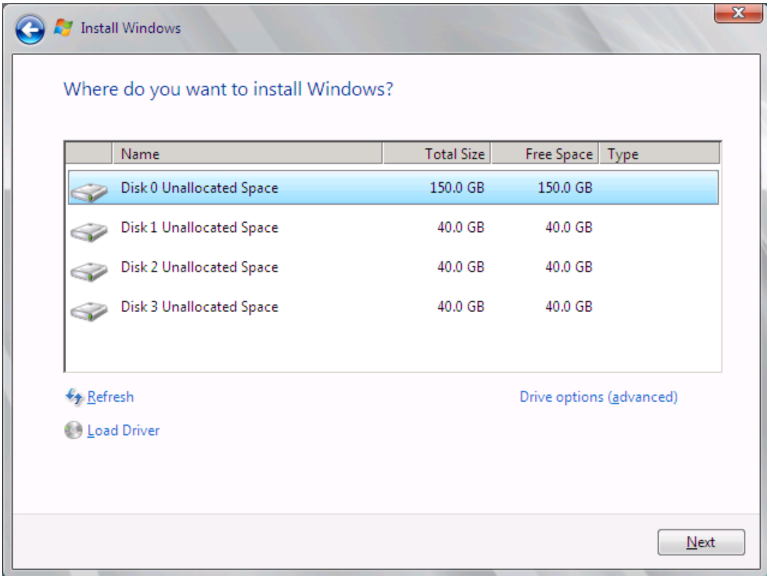
1. Connect the broadband modem to a power source and to the jack providing access to the ISP's network, using the appropriate cable.
2. Connect the router to a power source and then to the modem using an Ethernet cable. In most cases, the router automatically obtains an IP address and other settings from a DHCP server on the ISP's network.
3. If you are using a separate switch, connect it to a power source and then connect both the router and a computer running Windows to the switch using Ethernet cables. If your router has switched ports or an integrated wireless access point, you can also connect the computer directly to the router.

4. On the computer, start a web browser and connect to the router's administrative interface using the default IP address supplied by the router manufacturer.
5. Configure the router to access the Internet by applying the settings supplied by your ISP. These settings typically consist of a user name and password and might include other parameters as well.

Once the computer can access the Internet through the router, you can connect your server to a power source and to your new network. At this point, the hardware is ready for the Windows SBS 2011 installation.

Provisioning Disk Space

Early in the Windows SBS 2011 installation process, you must specify the hard disk on which you want to install the Windows Server 2008 R2 operating system and other software products. Using the interface from the Windows SBS 2011 setup program shown in Figure 3-2, you can select an entire unallocated disk on the computer or create a new volume using part of the unallocated space on a disk. Before you actually perform this task, you should consider how you are going to use the disk space on your server so that you can create the appropriate volumes.



Where do you want to install Windows?

Name	Total Size	Free Space	Type
Disk 0 Unallocated Space	150.0 GB	150.0 GB	
Disk 1 Unallocated Space	40.0 GB	40.0 GB	
Disk 2 Unallocated Space	40.0 GB	40.0 GB	
Disk 3 Unallocated Space	40.0 GB	40.0 GB	

FIGURE 3-2 The volume creation interface in the Windows SBS 2011 setup program.

During the Windows SBS 2011 installation, you can create only simple volumes on your server disks; you cannot create striped, spanned, or RAID-5 volumes. Therefore, if you are planning to use these volume types for your user data or other purposes, you must create them using the Disk Management snap-in for the Microsoft Management Console (MMC), after the installation is completed.

For the purposes of the installation, you must decide which hard disk you want to use for the *system volume* (that is, the volume on which the operating system is installed) and how much disk space you want to use to create that volume. As noted earlier in this chapter, the Windows SBS 2011 system requirements call for a minimum of 120 GB, but you might want to allocate more disk space. As a general rule, you should avoid storing documents and other user data on the system volume. You can create a separate volume for data either during or after the installation.

In addition to the Windows Server 2008 R2 operating system itself, Windows SBS 2011 creates the Exchange Server email stores on the system volume and stores its library of Windows Server Update Services (WSUS) updates there. Depending on how many users you have on your network and how they use email, the Exchange Server stores might grow to consume a great deal of disk space, especially if the users do not delete their old emails. The WSUS library also gets larger over time. Fortunately, however, Windows SBS 2011 includes tools that enable you to move the Exchange Server store and WSUS library to another volume easily. Therefore, you do not have to account for these in the size you select for your system volume as long as you have another volume in which you can store them.

NOTE **For information on how to move Windows SBS data stores to other volumes, see Chapter 9, "Managing Storage."**

Selecting Names

During the installation process, the Windows SBS 2011 setup program prompts you to supply names for your server, for your internal domain, and for an administrative user. The program suggests server and domain names based on the company name you supplied earlier, but you might want to change them. Computer names and domain names cannot be more than 15 characters long and can consist only of letters, numbers, and the underscore and hyphen characters. These names are not case-sensitive.

CAUTION **Consider the server and domain names that you choose carefully because you cannot change them once the installation is complete.**

COMPUTER NAMING

The best practice, when selecting a name for your server and for all your network computers, is to choose consistent, logical names that make sense to all the network's users. Remember, there will be many times in the future when people need to know the names of specific computers, and unless you want to receive a phone call every time that happens, you want to avoid using whimsical or nonsensical names. You should avoid using people's names for computers as well because it only causes confusion when employees change jobs or leave the organization.

On a small-business network that has only a few servers, simple names such as SERVERA or SERVER1 are appropriate, as are names reflecting each server's primary role, such as SVR-DC for your domain controller and SVR-FILE for your file server. For workstations, generic names such as WKSTN-01 and WKSTN-02 are suitable, but you might also consider names that reflect the locations of the computers, such as WK-RECEP for the system on the receptionist's desk and WK-BKPG1 and WK-BKPG2 for the computers in the bookkeepers' office. Whatever conventions you elect to use, create a set of naming rules and use them consistently for all your computers.

DOMAIN NAMING

The domain name that you supply is the name that the setup program assigns to your AD DS domain, appended with the suffix *local*. You do not have to register the name that you choose for use on the Internet. Indeed, this domain cannot be Internet-accessible because *local* is not an official top-level domain. However, if you have a registered Internet domain name, such as *adatum.com*, you can elect to use the same second-level name on your internal domain, as in *adatum.local*, if you want to.

> ***MORE INFO*** **For more information on domains, both on the Internet and in AD DS, see the section "Understanding Domains," in Chapter 2.**

It is possible to use a suffix other than *local* for your internal domain name, but to do so you must install Windows SBS 2011 using an answer file. In fact, if you are connecting Apple Macintosh computers running OS X version 10.3 or higher to your network, you must use a different suffix because OS X uses the *local* suffix for its Rendezvous service. An *answer file* is an Extensible Markup Language (XML) file you create that automates the installation process by supplying responses to the setup program's user prompts. The file also enables you to configure additional installation parameters that do not appear during an interactive installation or trigger a server migration.

> ***MORE INFO*** **For more information on using answer files, see "Creating an Answer File," in Chapter 5, "Migrating to Windows SBS 2011."**

If you intend to use an internal domain name with a suffix other than *local*, you should be careful not to use a domain name that someone else has already registered for Internet use. Your internal use of the domain name does not affect the legal registrant's rights, but it does prevent users on your internal network from accessing that name on the Internet.

Internal domain names typically use some permutation of the organization's name. For example, the A. Datum Corporation might use *adatum.local* for its internal domain. Once you decide on a name for your internal domain, you might want to consider registering that name on the Internet, in the .com, .net, or .org top-level domain. Even if you do not need an Internet domain name right now, registering it prevents anyone else from taking it.

USER NAMING

After you supply your server and internal domain names, the setup program prompts you to create a network administrator account. For security reasons, the setup program disables the operating system's built-in Administrator account at the end of the installation, so you must create an account to use in its place. Before you do this, you might want to consider a user naming convention for your network as well. A common convention for smaller networks is to create account names from the user's first name and last initial, as in MarkL. For larger networks, where there is more likely to be a name conflict, you might want to use the first initial and surname, as in MLee.

Instituting a user-naming convention for your network is not essential. It is certainly less necessary than a computer-naming convention, but letting users select their own account names only increases the burden on the network administrator. When an administrator knows what a user's account name should be without having to ask, the account maintenance process runs more smoothly for everyone involved.

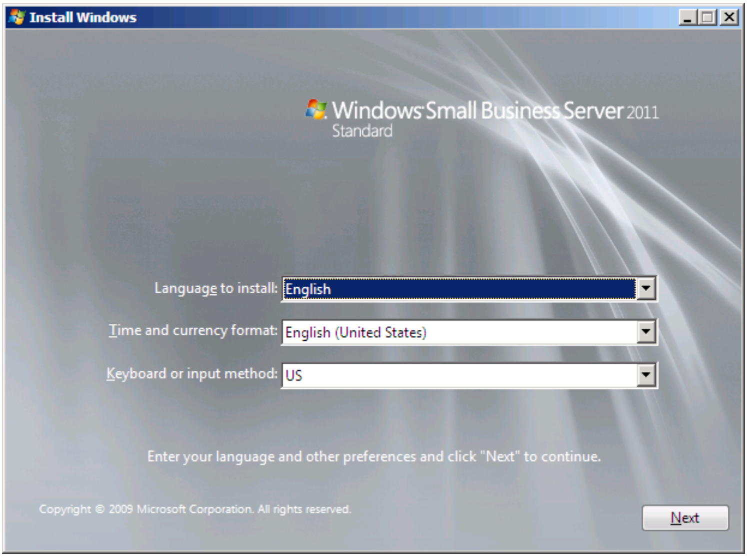
Installing Windows SBS 2011

Once your hardware is in place and you have made all the necessary decisions, you are ready to perform the Windows SBS 2011 installation. Considering all that the setup process accomplishes, the installation process for Windows SBS 2011 is remarkably easy. A clean installation (that is, an installation performed on a blank hard disk) requires only a small amount of interaction; the setup program does nearly everything itself. Migrations from earlier versions of Windows SBS are a bit more problematic, however.

Performing a Clean Windows SBS 2011 Installation

To perform a clean installation of Windows SBS 2011 on a new computer or on a computer with a hard disk that you can wipe clean, use the following procedure:

1. Turn on the computer and insert Disk 1 from the Windows SBS 2011 package into the DVD-ROM drive.
2. Press a key to boot from the DVD if the system prompts you to do so. The computer reads from the DVD and displays the first page of the Install Windows Wizard.



Language to install: English

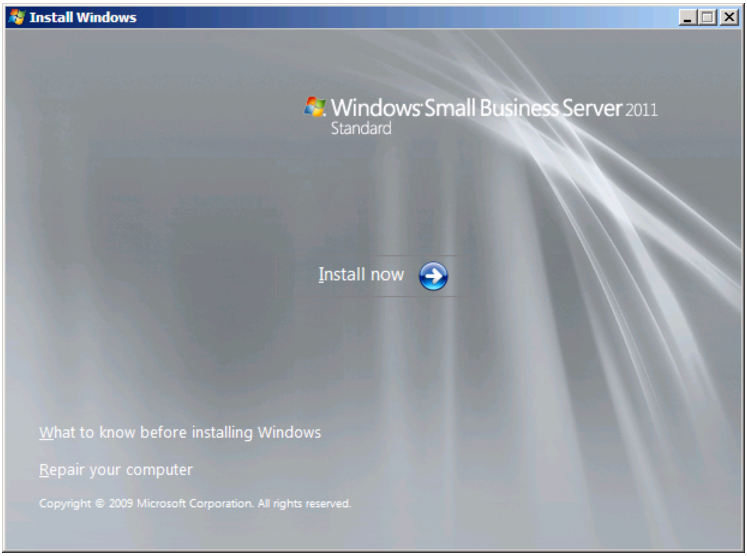
Time and currency format: English (United States)

Keyboard or input method: US

Enter your language and other preferences and click "Next" to continue.

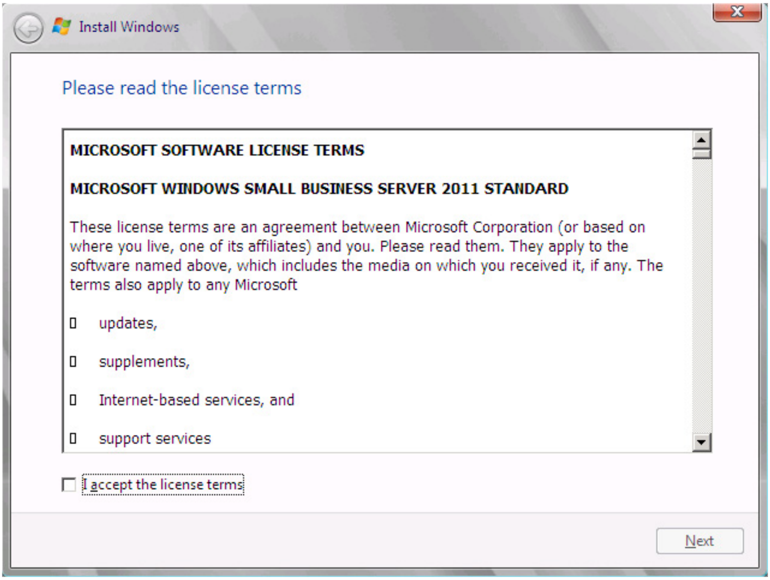
Copyright © 2009 Microsoft Corporation. All rights reserved.

3. If you plan to use language, time, and currency format, or keyboard settings other than the defaults, select your preferences from the three drop-down lists. Then click *Next*. The Install Now page appears.


Install Windows
Windows Small Business Server 2011
Standard
Install now
What to know before installing Windows
Repair your computer

Copyright © 2009 Microsoft Corporation. All rights reserved.

4. Click *Install now*. The Please Read The License Terms page appears.



Please read the license terms

MICROSOFT SOFTWARE LICENSE TERMS

MICROSOFT WINDOWS SMALL BUSINESS SERVER 2011 STANDARD

These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to the software named above, which includes the media on which you received it, if any. The terms also apply to any Microsoft

▯ updates,

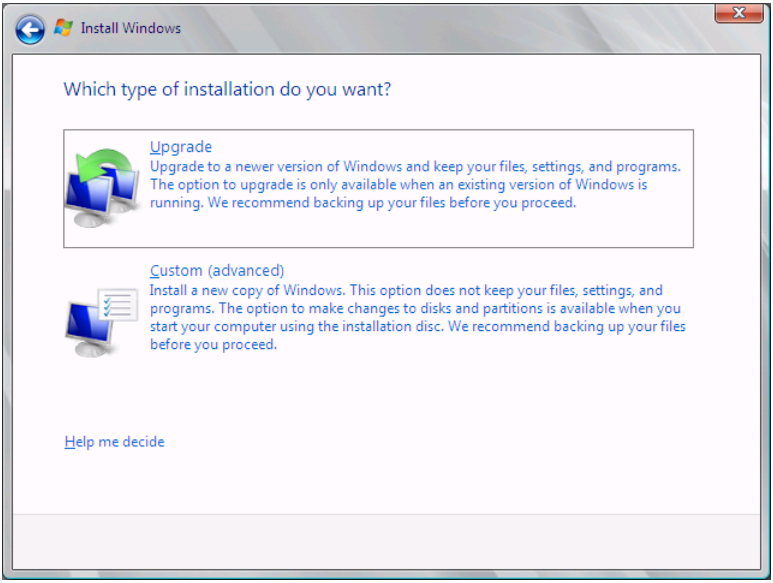
▯ supplements,

▯ Internet-based services, and

▯ support services

□ I accept the license terms

5. Select the *I accept the license terms* check box and click *Next*. The Which Type Of Installation Do You Want? page appears.



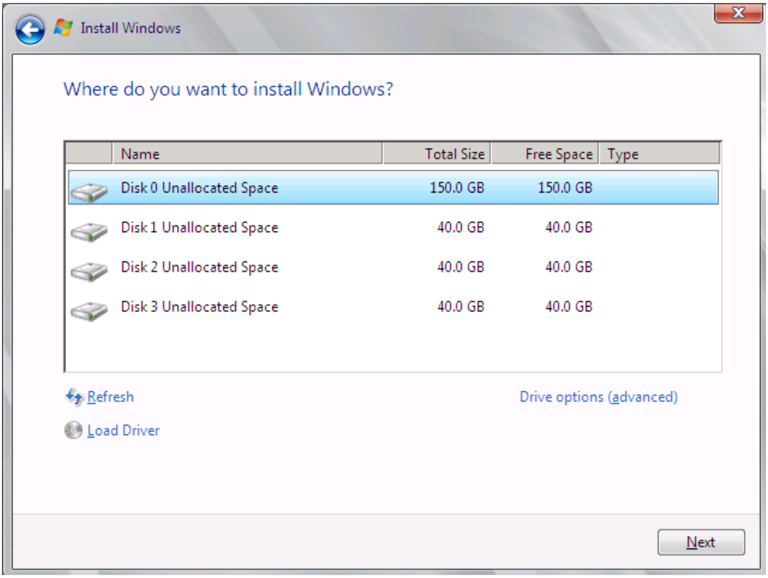
Which type of installation do you want?

Upgrade
Upgrade to a newer version of Windows and keep your files, settings, and programs. The option to upgrade is only available when an existing version of Windows is running. We recommend backing up your files before you proceed.

Custom (advanced)
Install a new copy of Windows. This option does not keep your files, settings, and programs. The option to make changes to disks and partitions is available when you start your computer using the installation disc. We recommend backing up your files before you proceed.

NOTE There is no upgrade path for the Windows SBS 2011 product. If you have an existing Windows SBS installation, you can migrate it to another server, but you cannot upgrade it. For more information, see Chapter 5.

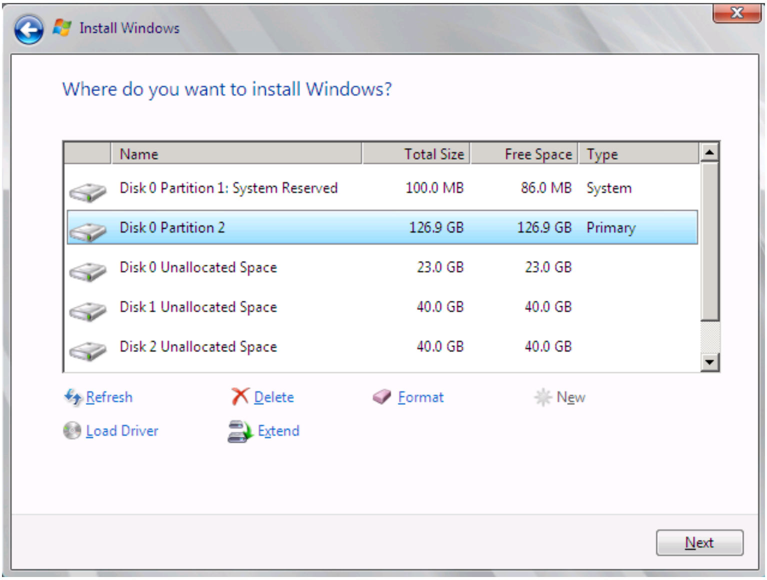
6. Click *Custom (advanced)*. The Where Do You Want To Install Windows? page appears.



Where do you want to install Windows?

Name	Total Size	Free Space	Type
Disk 0 Unallocated Space	150.0 GB	150.0 GB	
Disk 1 Unallocated Space	40.0 GB	40.0 GB	
Disk 2 Unallocated Space	40.0 GB	40.0 GB	
Disk 3 Unallocated Space	40.0 GB	40.0 GB	

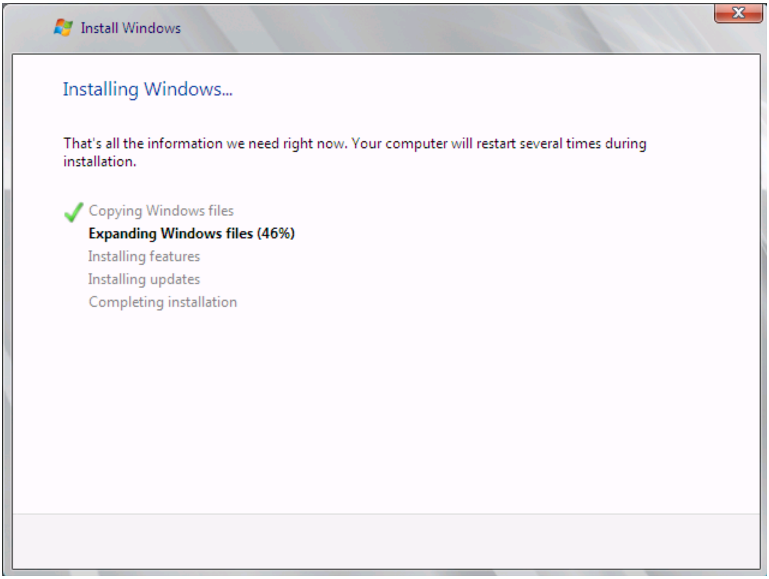
7. To create a partition on a disk, click *Drive options (advanced)* to display additional controls.
8. Select the disk on which you want to create the partition and click *New*. In the *Size* box that appears, specify a size greater than 120,000 MB (120 GB) for the partition and click *Apply*. An Install Windows message box appears, informing you that Windows will create additional partitions for system files.
9. Click *OK*. The new partition you created appears in the list.



Where do you want to install Windows?

Name	Total Size	Free Space	Type
Disk 0 Partition 1: System Reserved	100.0 MB	86.0 MB	System
Disk 0 Partition 2	126.9 GB	126.9 GB	Primary
Disk 0 Unallocated Space	23.0 GB	23.0 GB	
Disk 1 Unallocated Space	40.0 GB	40.0 GB	
Disk 2 Unallocated Space	40.0 GB	40.0 GB	

10. Select the partition on which you want to install Windows SBS 2011 and click *Next*. The Installing Windows page appears, and the setup program proceeds through the various stages of the Windows Server 2008 R2 operating system installation.



Installing Windows...

That's all the information we need right now. Your computer will restart several times during installation.

✓ Copying Windows files

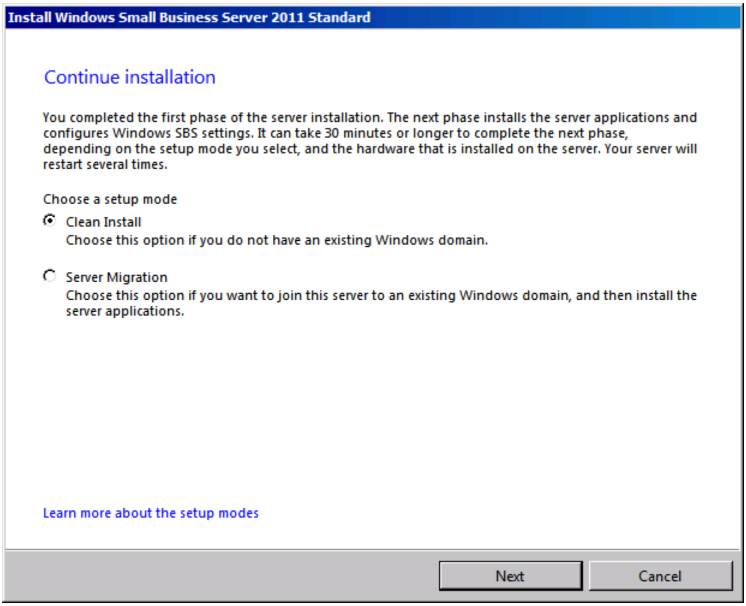
Expanding Windows files (46%)

Installing features

Installing updates

Completing installation

11. When this phase of the installation process is completed, the computer restarts twice, and the Continue Installation page appears.



Install Windows Small Business Server 2011 Standard

Continue installation

You completed the first phase of the server installation. The next phase installs the server applications and configures Windows SBS settings. It can take 30 minutes or longer to complete the next phase, depending on the setup mode you select, and the hardware that is installed on the server. Your server will restart several times.

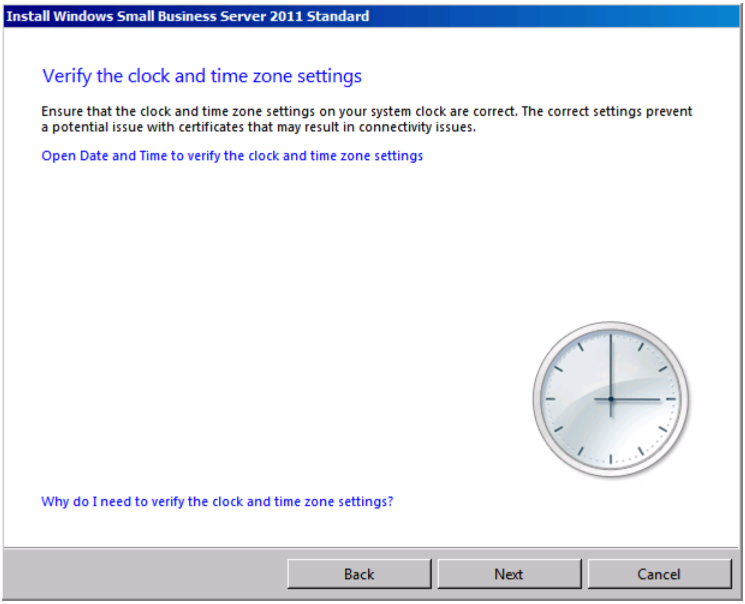
Choose a setup mode

● Clean Install
Choose this option if you do not have an existing Windows domain.

○ Server Migration
Choose this option if you want to join this server to an existing Windows domain, and then install the server applications.

Learn more about the setup modes

12. Select the *Clean install* option and click *Next*. The Verify The Clock And Time Zone Settings page appears.



Install Windows Small Business Server 2011 Standard

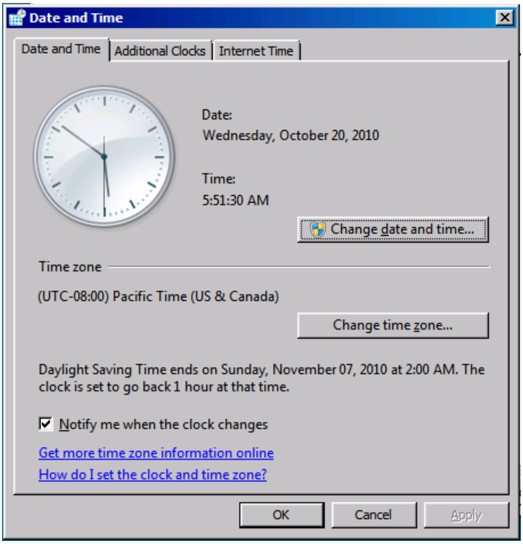
Verify the clock and time zone settings

Ensure that the clock and time zone settings on your system clock are correct. The correct settings prevent a potential issue with certificates that may result in connectivity issues.

Open Date and Time to verify the clock and time zone settings

Why do I need to verify the clock and time zone settings?

13. Click *Open date and time to verify the clock and time zone settings*. The Date And Time dialog box appears.



Date and Time

Date and Time | Additional Clocks | Internet Time

Date:
Wednesday, October 20, 2010

Time:
5:51:30 AM

Time zone

(UTC-08:00) Pacific Time (US & Canada)

Daylight Saving Time ends on Sunday, November 07, 2010 at 2:00 AM. The clock is set to go back 1 hour at that time.

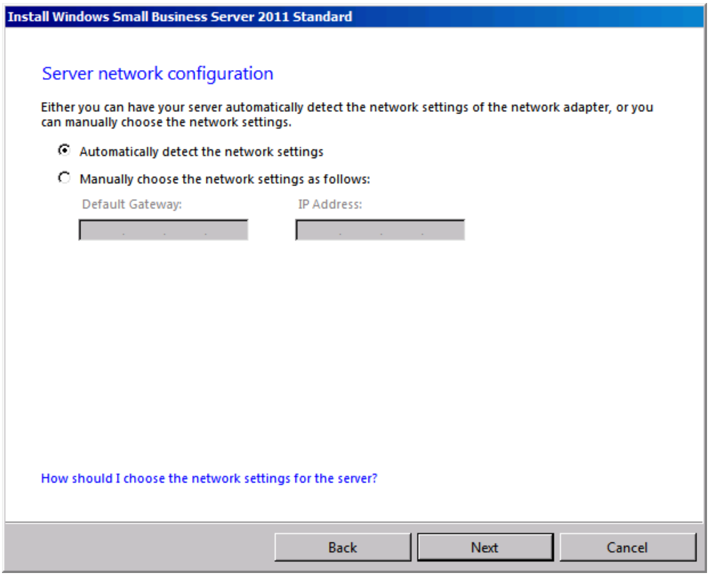
☑ Notify me when the clock changes

Get more time zone information online

How do I set the clock and time zone?

14. Verify that the *Date, time, and time zone* settings are correct. If they are not, click *Change date and time* or *Change time zone* to correct them. Then click *OK* to close the Date And Time dialog box.

15. Click *Next*. The Server Network Configuration page appears.



Install Windows Small Business Server 2011 Standard

Server network configuration

Either you can have your server automatically detect the network settings of the network adapter, or you can manually choose the network settings.

● Automatically detect the network settings

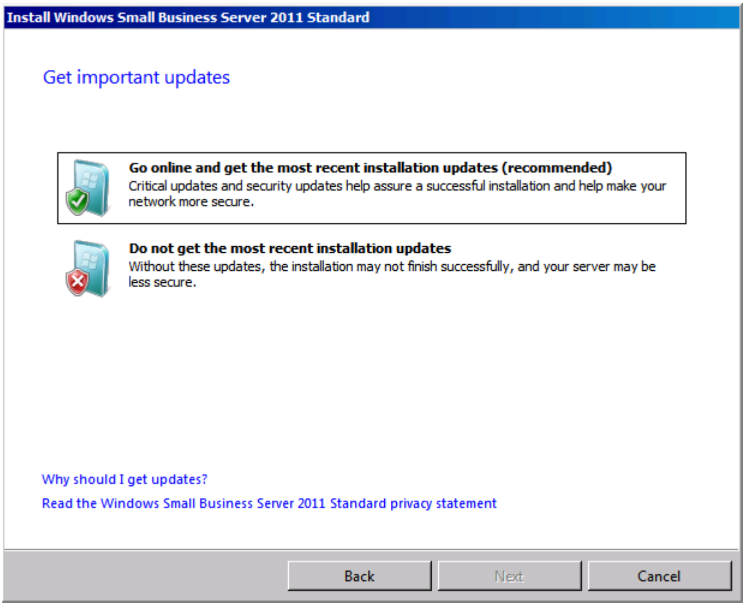
○ Manually choose the network settings as follows:

Default Gateway:

IP Address:

How should I choose the network settings for the server?

16. If you have a router already connected to the network, leave the *Automatically detect the network settings* option selected and click *Next*. The Get Important Updates page appears.



Install Windows Small Business Server 2011 Standard

Get important updates

Go online and get the most recent installation updates (recommended)
Critical updates and security updates help assure a successful installation and help make your network more secure.

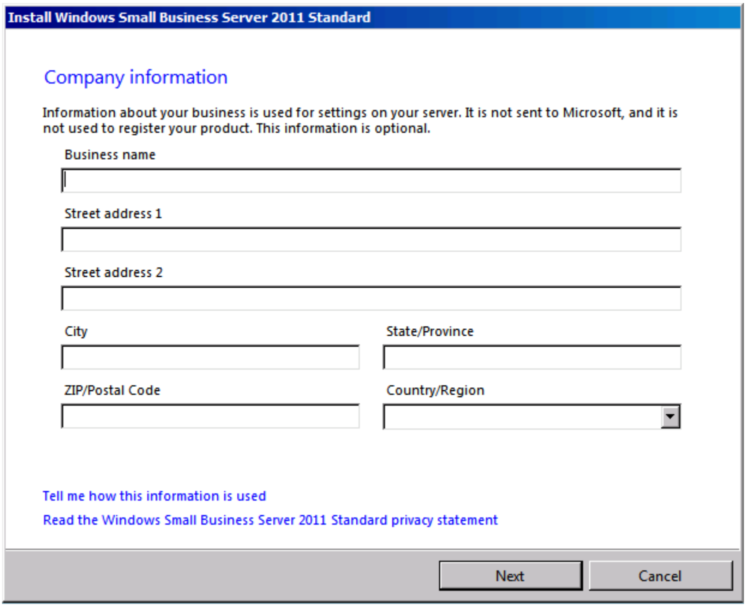
Do not get the most recent installation updates
Without these updates, the installation may not finish successfully, and your server may be less secure.

Why should I get updates?

Read the Windows Small Business Server 2011 Standard privacy statement

17. If you have already installed a router and an Internet connection on your network, click *Go online and get the most recent installation updates*. The Connecting Your Server page appears, displaying the progress of the setup program as it searches for the router, configures the server's TCP/IP client, and downloads updates from the Microsoft website.

18. When the process is complete, the Company Information page appears.



Install Windows Small Business Server 2011 Standard

Company information

Information about your business is used for settings on your server. It is not sent to Microsoft, and it is not used to register your product. This information is optional.

Business name

Street address 1

Street address 2

City

State/Province

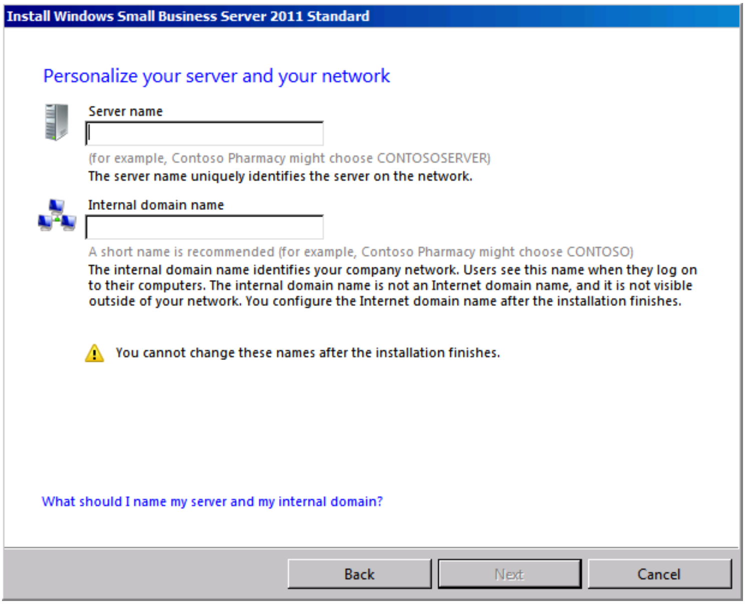
ZIP/Postal Code

Country/Region

Tell me how this information is used

Read the Windows Small Business Server 2011 Standard privacy statement

19. Fill out the text boxes with the name and address of your organization and click *Next*. The Personalize Your Server And Your Network page appears.



Install Windows Small Business Server 2011 Standard

Personalize your server and your network

Server name

(for example, Contoso Pharmacy might choose CONTOSOSERVER)

The server name uniquely identifies the server on the network.

Internal domain name

A short name is recommended (for example, Contoso Pharmacy might choose CONTOSO)

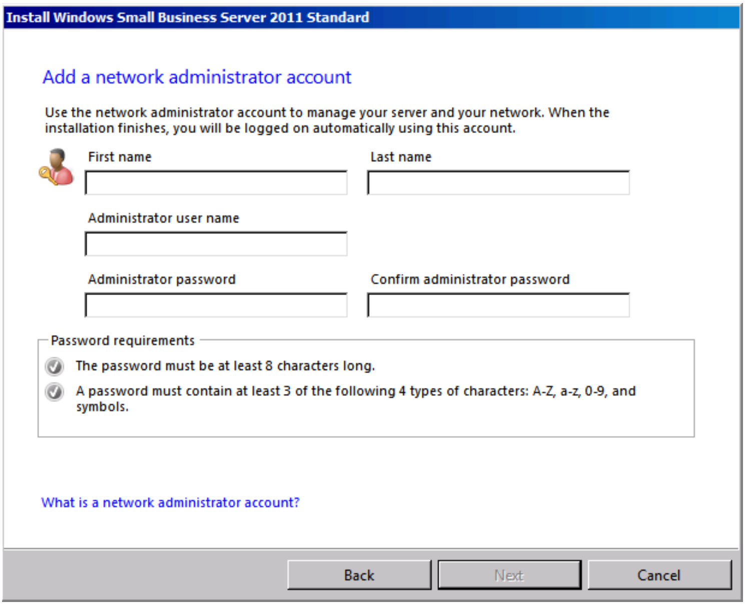
The internal domain name identifies your company network. Users see this name when they log on to their computers. The internal domain name is not an Internet domain name, and it is not visible outside of your network. You configure the Internet domain name after the installation finishes.

⚠ You cannot change these names after the installation finishes.

What should I name my server and my internal domain?

20. In the *Server name* text box, type the name you selected for your server running Windows SBS 2011.

21. In the *Internal domain name* text box, type the name you selected for your AD DS domain, without the *local* suffix. Then click *Next*. The Add A Network Administrator Account page appears.



Install Windows Small Business Server 2011 Standard

Add a network administrator account

Use the network administrator account to manage your server and your network. When the installation finishes, you will be logged on automatically using this account.

First name

Last name

Administrator user name

Administrator password

Confirm administrator password

Password requirements

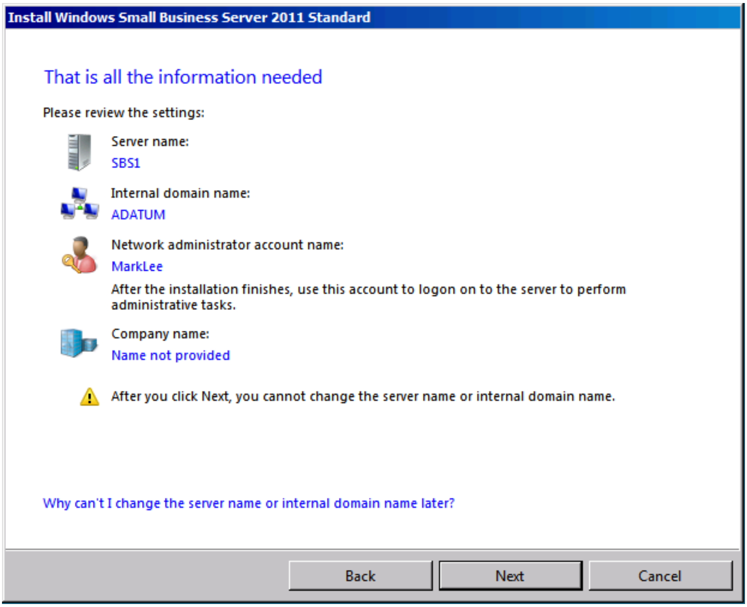
✓ The password must be at least 8 characters long.

✓ A password must contain at least 3 of the following 4 types of characters: A-Z, a-z, 0-9, and symbols.

What is a network administrator account?

22. Fill out the first and last names of the network administrator and, in the *Administrator user name* field, type an account name that conforms to your naming convention. Then type an appropriate password in the *Administrator password* and *confirm administrator password* text boxes and click *Next*. The That Is All The Information Needed page appears, containing the values that you supplied on the previous pages.

> ***NOTE*** **The name that you specify in the *Administrator user name* field can contain uppercase or lowercase letters, numbers, or the _#$%&'-^{}~! symbols. The password you specify must be at least eight characters long and contain three of the following character types: uppercase letters, lowercase letters, numbers, and symbols.**



Install Windows Small Business Server 2011 Standard

That is all the information needed

Please review the settings:

Server name:
SBS1

Internal domain name:
ADATUM

Network administrator account name:
MarkLee

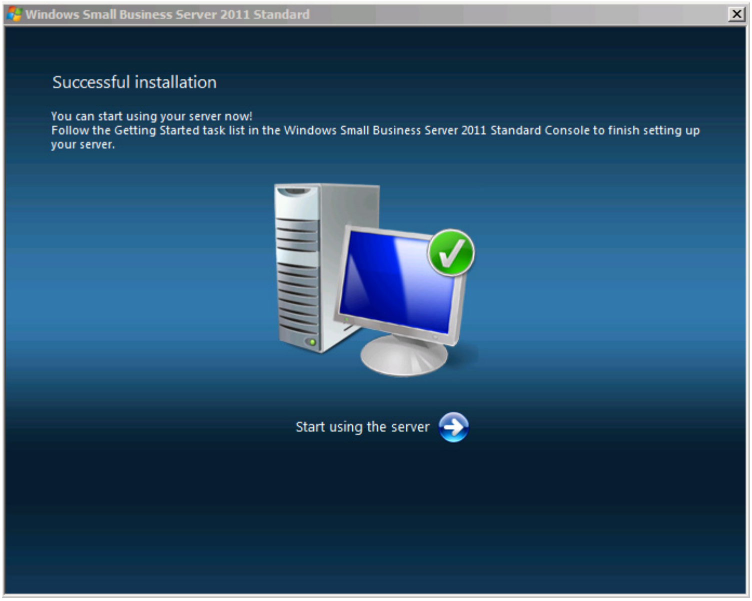
After the installation finishes, use this account to logon on to the server to perform administrative tasks.

Company name:
Name not provided

⚠ After you click Next, you cannot change the server name or internal domain name.

Why can't I change the server name or internal domain name later?

23. Click *Next*. The Expanding And Installing Files page appears, tracking the program's progress as it completes the installation.
24. The system restarts twice during this phase of the installation process, returning to the Expanding And Installing Files page each time. When the process is complete, the computer restarts one final time and the Successful Installation page appears.


Windows Small Business Server 2011 Standard

Successful installation

You can start using your server now!
Follow the Getting Started task list in the Windows Small Business Server 2011 Standard Console to finish setting up your server.

Performing an OEM Windows SBS 2011 Installation

If you purchase a server with the OEM version of Windows SBS 2011 preinstalled, the software is already on the computer's hard disk, but you must perform an abbreviated version of the setup procedure. The OEM setup procedure omits the generic operating system installation tasks, which the computer manufacturer has already performed at the factory, leaving only the tasks that require company-specific input to proceed.

When you turn on the computer for the first time, the Install Windows Wizard displays the same first three pages as a DVD installation (shown in steps 1 to 5 of the procedure in the previous section). These pages enable you to change the language, time, and currency format, and keyboard settings (if necessary); start the installation; and accept the license terms. In an OEM package, the manufacturer usually supplies the Windows SBS 2011 product keys on a Certificate of Authenticity sticker attached to the computer. You might also find that you do not have to enter the product key yourself because the manufacturer has entered it as part of the factory setup.

NOTE **If you purchase an OEM version of Windows SBS 2011, the Certificate of Authenticity sticker on your server should contain both the physical and virtual product keys.**

After you have completed the initial pages, the setup procedure skips to the Continue Installation page and resumes from there (starting at step 12). The installation is identical to the DVD-based procedure from this point.

REAL WORLD **One additional thing to remember is that when you purchase Windows SBS 2011 in a bundle with a computer, you might not receive installation DVDs. If this is the case, the media are on the computer's hard disk. One of the first things you should do after completing the setup procedure is to create a set of installation DVDs in case you ever have to reinstall the computer.**

Understanding the Installation Process

When you install the standalone Windows Server 2008 R2 product, you are left with what is essentially a clean slate. The operating system includes a large collection of services, packaged in groups called *roles,* but the setup program does not install any of them by default. You must add and configure them yourself. With Windows SBS 2011, the situation is extremely different. The setup program not only installs the operating system; it also adds and configures many of the supplied roles to create a default server environment that requires relatively little additional configuration.

Most of the configuration tasks that the setup program performs are invisible to the user during the installation process. However, it is a good idea for administrators to know what the setup program has done so that they can work with the various server components later. The following sections list the various roles the setup program installs and describe how the program configures them.

Active Directory Certificate Services

A *digital certificate* is an electronic document, issued by a trusted source called a *certification authority (CA)*, that verifies the identity of a user or computer. When you connect to a secured website on the Internet, for example, your browser downloads a certificate from a third-party CA that verifies that you really are connecting to the correct site. The setup program for Windows SBS 2011 installs the Active Directory Certificate Services role, which enables your server to function as a CA for your internal network.

In addition to installing the role, the setup program uses the new CA to issue two certificates to your server: a Domain Controller certificate and a Web Server certificate. These two certificates, self-signed by your server, enable clients on the network to establish secured connections to the websites hosted by your server and to the authentication services provided by the AD DS role.

Active Directory Domain Services

One of the most important roles of your server running Windows SBS 2011 is that of an AD DS domain controller. Among many other functions, the domain controller maintains a central database of your user and computer accounts, which is accessible to all the computers on the network. Without an AD DS domain, you would have to create and maintain separate user accounts on each of the network's computers. With AD DS, your users log on to the domain, not individual computers. The domain controller is responsible for authenticating the users and granting them access to network resources.

During the Windows SBS 2011 installation process, the setup program adds the Active Directory Domain Services role on your server and, using the internal domain name you specified on the Personalize Your Server And Your Network page, promotes the server into a domain controller. On a standalone computer running Windows Server 2008 R2, these are both tasks that you must perform manually. When the installation is finished, you can begin creating AD DS user and computer accounts immediately.

MORE INFO **For more information on AD DS, see "An Active Directory Primer" in Chapter 6, "Working with Users, Computers, and Groups."**

Application Server

The Application Server role provides an integrated environment for deploying and running server-based business applications developed by or for the organization, including those requiring the services provided by Internet Information Services (IIS), Microsoft .NET Framework 3.5.1, TCP Port Sharing, and Windows Process Activation Service.

DHCP Server

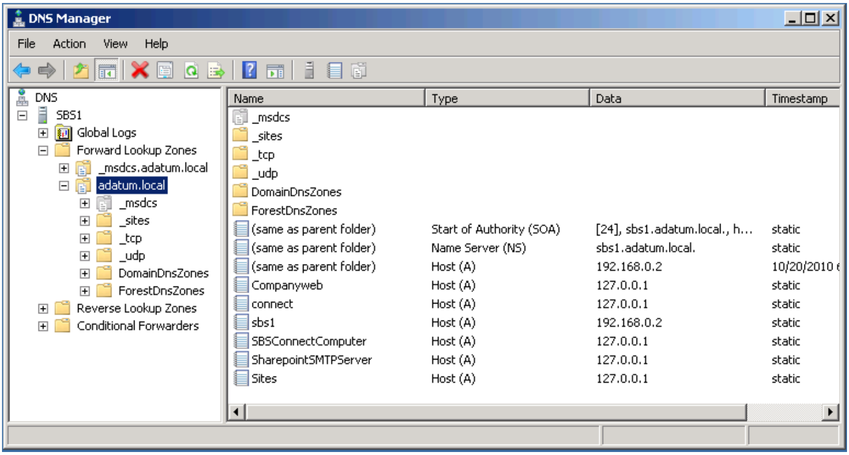
As mentioned earlier in this chapter and in Chapter 2, the DHCP Server role enables your server to issue IP addresses and other TCP/IP configuration settings to other computers on your network automatically. The Windows SBS 2011 setup program always installs the DHCP Server role, but it configures and activates the DHCP server only if it can obtain the information that it needs from a router on the network.

If the server does not detect a router during the installation, it leaves the DHCP server unconfigured and does not start the DHCP Server service. You must then start the service manually and configure it using the DHCP Console.

DNS Server

As discussed in Chapter 2, the Domain Name System (DNS) stores information about domains and computers, most particularly their names and IP addresses. The computers on your network use the DNS server to resolve domain and host names into the IP addresses they need to initiate TCP/IP communications with other computers, locally and on the Internet.

In addition to this basic connectivity function, DNS also plays a vital role in AD DS. As the setup program promotes the server into a domain controller, it installs the DNS Server role and creates a zone representing your internal domain. In this zone, the program creates a variety of resource records that enable clients on the network to locate not only the server but also specific websites and AD DS services on that computer, as shown in Figure 3-3.



DNS
SBS1
Global Logs
Forward Lookup Zones
_msdcs.adatum.local
adatum.local
_msdcs
_sites
_tcp
_udp
DomainDnsZones
ForestDnsZones
Reverse Lookup Zones
Conditional Forwarders

Name	Type	Data	Timestamp
_msdcs			
_sites			
_tcp			
_udp			
DomainDnsZones			
ForestDnsZones			
(same as parent folder)	Start of Authority (SOA)	[24], sbs1.adatum.local., h...	static
(same as parent folder)	Name Server (NS)	sbs1.adatum.local.	static
(same as parent folder)	Host (A)	192.168.0.2	10/20/2010 6
Companyweb	Host (A)	127.0.0.1	static
connect	Host (A)	127.0.0.1	static
sbs1	Host (A)	192.168.0.2	static
SBSConnectComputer	Host (A)	127.0.0.1	static
SharepointSMTPServer	Host (A)	127.0.0.1	static
Sites	Host (A)	127.0.0.1	static

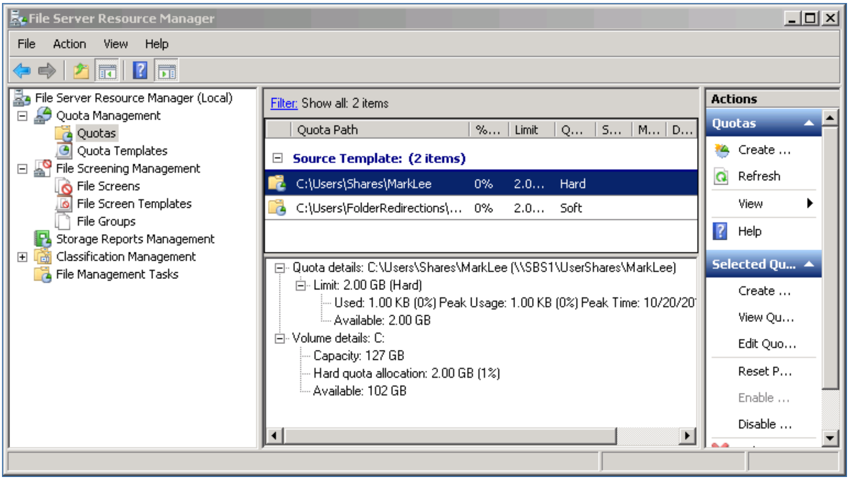
FIGURE 3-3 Resource records in a DNS zone.

For example, the zone for your domain contains a Host (A) resource record for the server name you specified during the installation, with the IP address that the program configured the server to use. The program also created an Alias (CNAME) record for the name Companyweb, which points to the server's Host (A) record. When a client uses a Web browser to connect to the *http://companyweb*.yourdomain .local address, the client uses the DNS server to resolve the Companyweb alias and receives the server name in return. The client then resolves the server name and receives the server's IP address in return. The client can now send a message to the specific website on the server.

> ***NOTE*** **In this example, using your Windows SBS 2011 server configuration, the need for two-name resolution processes to establish a connection to a web server that is running on the same computer as the DNS service might seem strange, but the web server could just as easily be running on another computer.**

File Services

The Windows SBS 2011 setup program installs the File Services role, but does not add all the available role services. In addition to the File Services role, which enables the computer to share its files, and which all computers running Windows Server 2008 R2 run by default, the program installs the File Server Resource Manager role service. This role service, using the File Server Resource Manager Console shown in Figure 3-4, enables you to establish storage quotas for your users, which limit how much server disk space they can consume; define file-screening policies, which limit the types of files that users can store on the server; and generate reports on storage consumption.



Quota Path	%...	Limit	Q...	S...	M...	D...
Source Template: (2 items)						
C:\Users\Shares\MarkLee	0%	2.0...	Hard			
C:\Users\FolderRedirections\...	0%	2.0...	Soft			

```
Quota details: C:\Users\Shares\MarkLee (\\SBS1\UserShares\MarkLee)
    Limit: 2.00 GB (Hard)
        Used: 1.00 KB (0%) Peak Usage: 1.00 KB (0%) Peak Time: 10/20/20
        Available: 2.00 GB
Volume details: C:
    Capacity: 127 GB
    Hard quota allocation: 2.00 GB (1%)
    Available: 102 GB
```

FIGURE 3-4 The File Server Resource Manager Console.

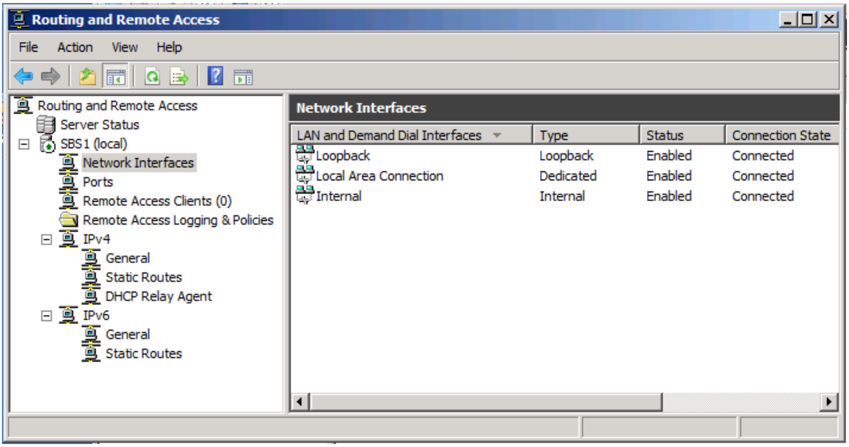
Network Policy and Access Services

When the setup program installs the Network Policy and Access Services role, it selects only the Network Policy Server and Routing and Remote Access Services (RRAS) role services. Network Policy Server enables you to specify conditions that clients must satisfy before the server allows them to establish a connection.

Windows SBS 2011 uses network policies to control server access through VPN connections and the Remote Desktop Gateway. For the server to grant them access, users must be members of the correct security groups and connect with a specific authentication protocol.

The setup program installs the Routing and Remote Access role service, but only with its Remote Access Service capabilities. The Routing option, which the program does not install, is intended to enable a computer running Windows Server 2008 R2 to function as a router, connecting two networks and forwarding traffic between them. Windows SBS 2011 is designed to support only one network interface on its primary server, so the server configuration omits the Router module.

The Remote Access Service option enables you to configure your server to host incoming VPN connections, which enables users at remote locations to connect to the server through the Internet. Although the setup program installs the role service required for this function, it does not configure it. You must do this manually using the Routing and Remote Access Console, shown in Figure 3-5.



- Routing and Remote Access
  - Server Status
  - SBS1 (local)
    - Network Interfaces
    - Ports
    - Remote Access Clients (0)
    - Remote Access Logging & Policies
    - IPv4
      - General
      - Static Routes
      - DHCP Relay Agent
    - IPv6
      - General
      - Static Routes

Network Interfaces

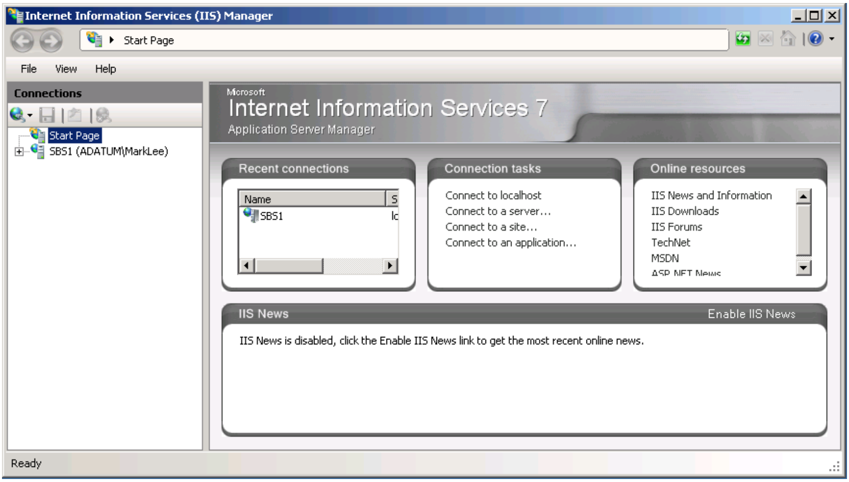
LAN and Demand Dial Interfaces	Type	Status	Connection State
Loopback	Loopback	Enabled	Connected
Local Area Connection	Dedicated	Enabled	Connected
Internal	Internal	Enabled	Connected

FIGURE 3-5 The Routing and Remote Access Console.

> ***MORE INFO*** **For more information on configuring Routing and Remote Access, see Chapter 13.**

Web Server (IIS)

Windows SBS 2011 uses web interfaces for a variety of its applications and services, so the Web Server (IIS) role is a critical part of the product installation. The setup program installs the role with many of its dozens of role services, and also creates a large number of websites and applications, as shown in Figure 3-6. These websites include the default SharePoint Foundation site, the SharePoint Central Administration site, the WSUS administration site, and the Outlook Web Access site for Exchange Server.

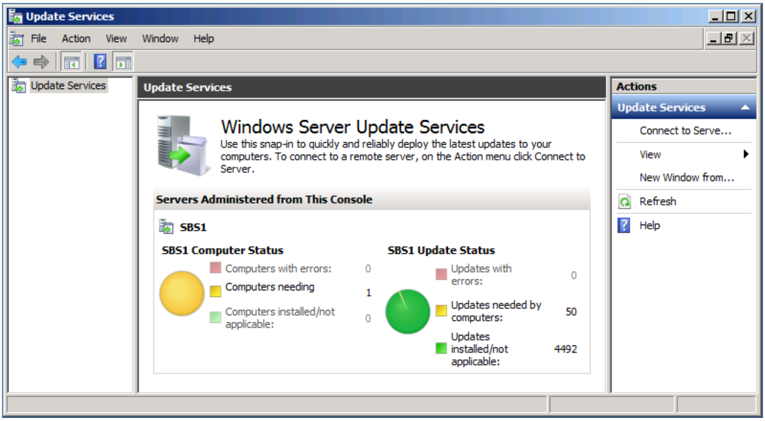


IIS News is disabled, click the Enable IIS News link to get the most recent online news.

FIGURE 3-6 The Internet Information Services (IIS) Manager Console.

Windows Server Update Services

The Windows Server Update Services role enables the Windows SBS server to store operating system and Microsoft application updates for approval by administrators and deployment to client computers on the network. Using Group Policy settings that the Windows SBS setup program creates, Windows SBS configures all the computers on the network to obtain their updates from WSUS, rather than from the Microsoft Update servers on the Internet. Using the Update Services Console, shown in Figure 3-7, administrators can review the latest updates received from Microsoft, evaluate them, and approve them for release to clients.



Use this snap-in to quickly and reliably deploy the latest updates to your computers. To connect to a remote server, on the Action menu click Connect to Server.

SBS1 Computer Status

- Computers with errors: 0
- Computers needing 1
- Computers installed/not applicable: 0

SBS1 Update Status

- Updates with errors: 0
- Updates needed by computers: 50
- Updates installed/not applicable: 4492

FIGURE 3-7 The Update Services Console.

CHAPTER 4

Getting Started

The Windows Small Business Server (SBS) 2011 installation process performs a large number of configuration tasks that administrators have to perform manually in the case of a standalone Windows Server 2008 R2 installation. However, this is not to say that a server running Windows SBS is ready for users when the installation is finished. You still must perform a variety of tasks to prepare the server for use, not the least of which is familiarizing yourself with the Windows SBS Console.

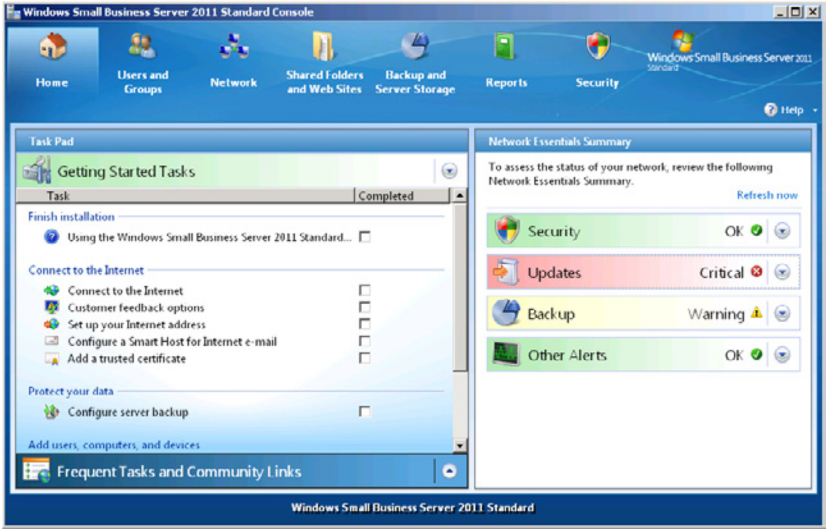
Using the Windows SBS Console

The Windows SBS Console is an administrative tool, first introduced in Windows SBS 2008, which replaces the Server Management Console from Windows SBS 2003. Unlike Server Management, Windows SBS Console is not a Microsoft Management Console (MMC) snap-in; it is a standalone application that groups together many of the basic server management and monitoring functions that require separate applications in Windows Server 2008 R2.

> ***NOTE*** **Windows SBS Console does not replace the standard Windows Server 2008 R2 tools; it merely supplements them. While Windows SBS Console includes many of the tools that administrators use most often, the various Windows Server 2008 R2 utilities offer many more advanced functions.**

Starting Windows SBS Console

When you log on to Windows SBS 2011 for the first time after the installation, the Windows SBS Console window opens by default and displays the interface shown in Figure 4-1. You can also start the program at any time by selecting *Start > Administrative Tools > Windows SBS Console*, and then clicking *Yes* in the User Account Control dialog box.


Windows Small Business Server 2011 Standard Console
Home
Users and Groups
Network
Shared Folders and Web Sites
Backup and Server Storage
Reports
Security
Windows Small Business Server 2011 Standard
Help
Task Pad
Getting Started Tasks
Network Essentials Summary
Refresh now
Frequent Tasks and Community Links
Windows Small Business Server 2011 Standard

Task	Completed
Finish installation	
Using the Windows Small Business Server 2011 Standard...	□
Connect to the Internet	
Connect to the Internet	□
Customer feedback options	□
Set up your Internet address	□
Configure a Smart Host for Internet e-mail	□
Add a trusted certificate	□
Protect your data	
Configure server backup	□
Add users, computers, and devices	

To assess the status of your network, review the following Network Essentials Summary.

Security	OK
Updates	Critical
Backup	Warning
Other Alerts	OK

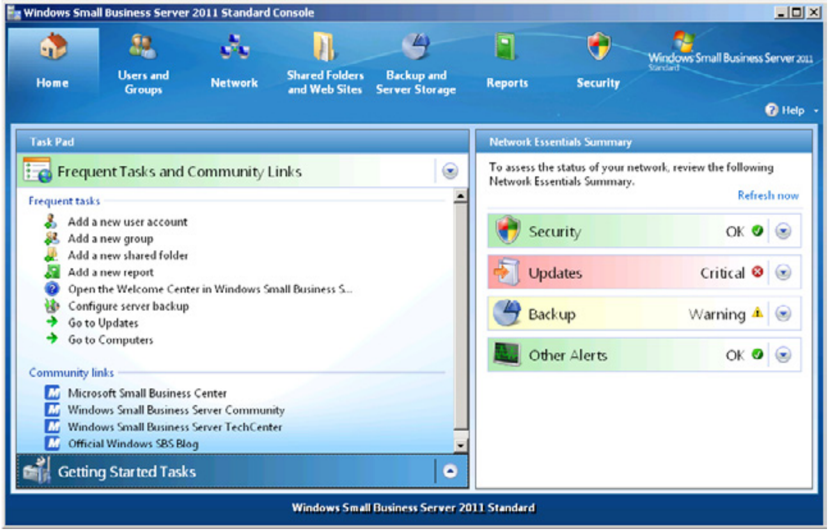
FIGURE 4-1 The Windows SBS Console.

You might notice that the Administrative Tools group also contains a Windows SBS Console (Advanced Mode) shortcut. Selecting this shortcut opens a version of the Windows SBS Console that includes links to other Windows Server 2008 R2 tools, such as the Active Directory Users And Computers, DHCP, and DNS Manager Consoles.

> ***TIP*** **In addition to running the Windows SBS Console application on the server, you can access it from remote locations. From another computer on the local network, you can use the Remote Desktop Connection client to access the server and start Windows SBS Console. You can also use the Remote Web Workplace (RWW) site to access the server from anywhere on the Internet. The address for your RWW site is *http://remote.domain_name.com*, where *domain_name.com* is the name of your Internet domain.**

Using the Windows SBS Console Interface

The Windows SBS Console has seven main pages represented by seven buttons at the top of the window. Clicking *Home* displays a page, different in appearance from the other six, which consists of two task panes and a status area. Each of these two panes has an arrow button on the right. Clicking the down arrow on the open pane minimizes it and moves it to the bottom, so that the other pane can open and take its place, as shown in Figure 4-2.

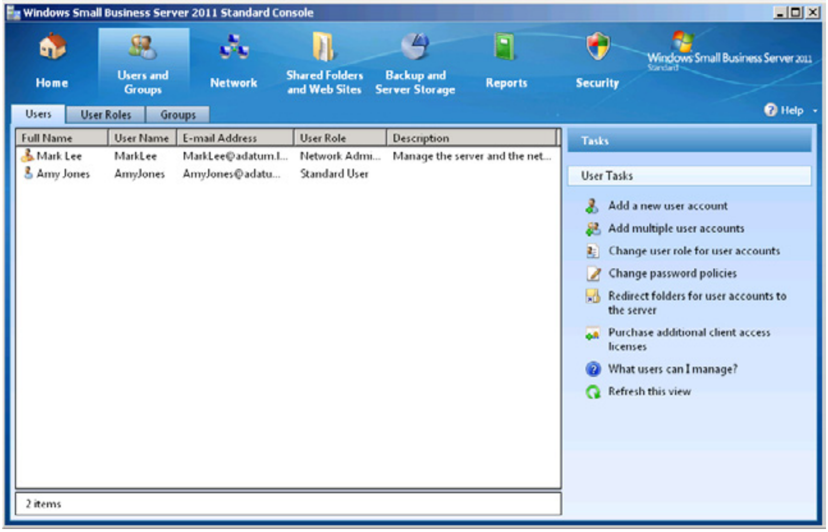

Windows Small Business Server 2011 Standard Console
Home
Users and Groups
Network
Shared Folders and Web Sites
Backup and Server Storage
Reports
Security
Windows Small Business Server 2011 Standard
Help
Task Pad
Frequent Tasks and Community Links
Frequent tasks
Add a new user account
Add a new group
Add a new shared folder
Add a new report
Open the Welcome Center in Windows Small Business S...
Configure server backup
Go to Updates
Go to Computers
Community links
Microsoft Small Business Center
Windows Small Business Server Community
Windows Small Business Server TechCenter
Official Windows SBS Blog
Getting Started Tasks
Network Essentials Summary
Refresh now
Windows Small Business Server 2011 Standard

To assess the status of your network, review the following Network Essentials Summary.

Security OK
Updates Critical
Backup Warning
Other Alerts OK

FIGURE 4-2 Swapping the Task pane in the Home page of the Windows SBS Console.

The other six pages in the console consist of tabbed lists of operating system elements on the left, as shown in Figure 4-3, and a context-sensitive task list on the right, which you can use to perform specific actions.


Windows Small Business Server 2011 Standard Console
Home
Users and Groups
Network
Shared Folders and Web Sites
Backup and Server Storage
Reports
Security
Windows Small Business Server 2011 Standard
Help
Users
User Roles
Groups
Tasks
User Tasks
Add a new user account
Add multiple user accounts
Change user role for user accounts
Change password policies
Redirect folders for user accounts to the server
Purchase additional client access licenses
What users can I manage?
Refresh this view

Full Name	User Name	E-mail Address	User Role	Description
Mark Lee	MarkLee	MarkLee@adatum.l...	Network Admi...	Manage the server and the net...
Amy Jones	AmyJones	AmyJones@adatu...	Standard User	

2 items

FIGURE 4-3 The tabbed interface of the Windows SBS Console.

The functions found in the main pages of the Windows SBS Console are as follows:

- Home
  - *Getting started tasks* Contains a list of post-installation tasks to perform on your server
  - *Frequent tasks and community links* Contains links to the console's most frequently used functions and to Windows SBS resources on the Internet
  - *Network essentials summary* Contains status displays for the servers on your network, along with links to appropriate pages with more information
- Users and groups
  - *Users* Contains a list of the user accounts you have created in your domain and enables you to create new user accounts and manage existing ones
  - *User roles* Enables you to create and manage templates that simplify the process of creating user accounts
  - *Groups* Contains a list of the Windows SBS security and distribution groups in your domain and enables you to create new groups and manage group memberships
- Network
  - *Computers* Contains a list of the computers on your network and enables you to add new computers and monitor existing ones

    - *Devices* Contains a list of shared print and fax devices on the network, and enables you to manage existing devices and share additional ones
    - *Connectivity* Contains a list of Windows SBS network and Internet resources and enables you to manage their properties
- Shared folders and web sites
    - *Shared folders* Contains a list of the shared folders on the network and enables you to create new shares and manage existing ones
    - *Web sites* Contains a list of the intranet and Internet websites for the organization and enables you to manage their properties and permissions
- Backup and server storage
    - *Backup* Contains a list of the scheduled backup jobs for the server and enables you to configure the jobs, check their status, and restore files from backups
    - *Server storage* Contains a list of the server's storage volumes and enables you to move specific data stores to other locations
- Reports Contains a list of the Windows SBS reports that the system is configured to generate and enables you to view the reports and create new ones
- Security
    - *Security* Contains a list of the security mechanisms on the server, and enables you to check their status and view their properties
    - *Updates* Contains a list of the updates downloaded by Windows Server Update Services (WSUS), tracks their status, and enables you to deploy or decline them

Performing Post-Installation Tasks

As soon as possible after you install Windows SBS 2011 on your server, you should begin addressing the items in the *Getting started tasks* list on the Home page of the Windows SBS Console. Some of these tasks link to wizards that help you to configure various server functions, while others display help files that provide useful information about administering your server and your network.

The following sections describe the functions of the various tasks in the list. As you finish each task, select its *Completed* check box to keep track of your progress.

Using the Windows SBS Console

For administrators working with Windows SBS for the first time, it is a good idea to become familiar with the management tools supplied with Windows SBS 2011, especially the Windows SBS Console. Clicking the *Using the Windows SBS console* link on the Home page opens a Help window that describes the basic capabilities of the Windows SBS and provides links to more detailed help pages on specific subjects.

Some of the other entries in the *Getting started tasks* list link to help files as well, including *How can users access computers on the network?* and *How can I add a shared printer to the network*? For more information on these subjects, see Chapter 6, "Working with Users, Computers, and Groups" and Chapter 10, "Sharing Printers."

MORE INFO **If you migrated your server running Windows SBS 2011 from an earlier version of Windows SBS, an additional *Migrate to Windows SBS* task appears in the *Getting started tasks* list. For more information on completing the migration process, see the section entitled "Performing Post-Migration Tasks," in Chapter 5, "Migrating to Windows SBS 2011."**

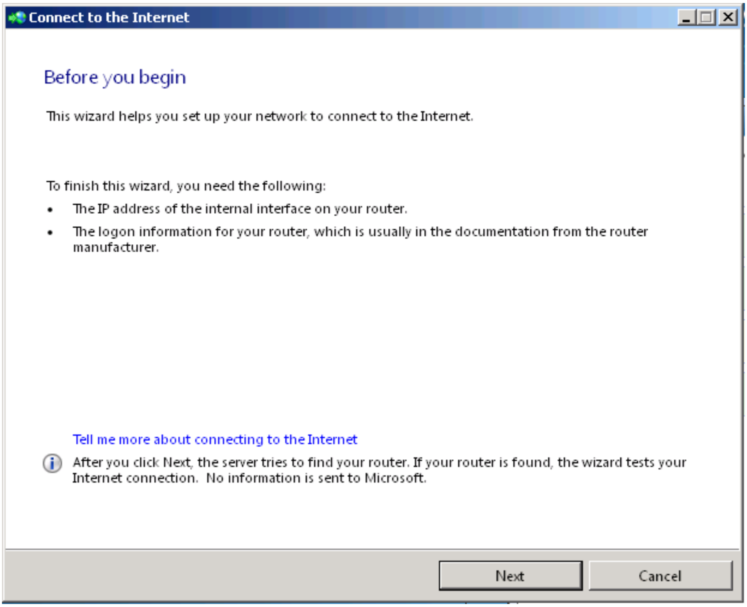
Connecting to the Internet

The Connect To The Internet Wizard is an important part of the Windows SBS 2011 setup process; many of the other wizards in the *Getting started tasks* list cannot run until you complete it. If you installed your server running Windows SBS 2011 before setting up an Internet access router on your network, this wizard detects the router and configures the server to use it for Internet access. The wizard also configures the DHCP Server service on the computer to supply Internet Protocol (IP) addresses and other Transmission Control Protocol/Internet Protocol (TCP/IP) configuration settings to the client workstations that you will be connecting to the network.

TIP **You should run the Connect To The Internet Wizard again if you ever install a new router on your network or reconfigure your router to use a different IP address. You can access the wizard from the Home page of the Windows SBS Console or by switching to the Network page, selecting the *Connectivity* tab, and, in the Tasks pane, clicking *Connect to the Internet*.**

To complete the Connect To The Internet Wizard, set up your router on the network according to the manufacturer's instructions and then use the following procedure:

1. Log on to your server running Windows SBS 2011 using an account with network Administrator privileges. The Windows SBS Console appears.
2. On the Home page of the Windows SBS Console, click *Connect to the Internet*. The Connect To The Internet Wizard appears, displaying the Before You Begin page.



Connect to the Internet

Before you begin

This wizard helps you set up your network to connect to the Internet.

To finish this wizard, you need the following:

- The IP address of the internal interface on your router.
- The logon information for your router, which is usually in the documentation from the router manufacturer.

Tell me more about connecting to the Internet

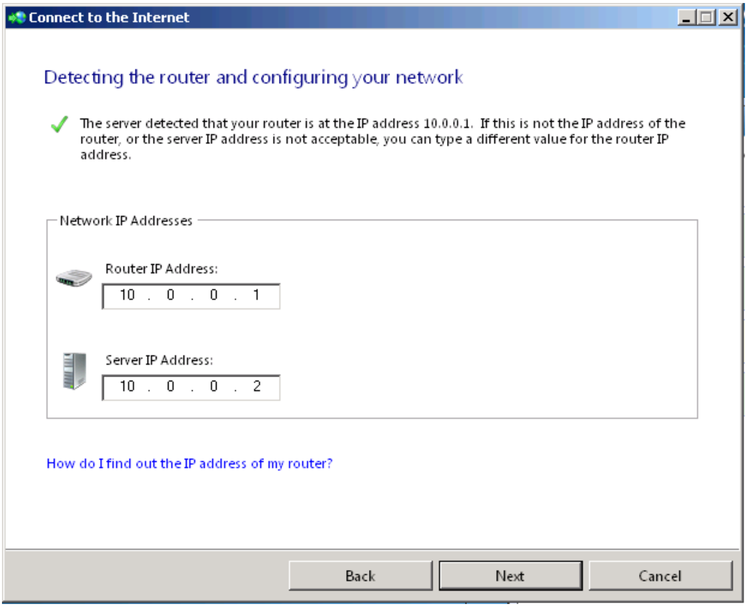
After you click Next, the server tries to find your router. If your router is found, the wizard tests your Internet connection. No information is sent to Microsoft.

As noted on the Before You Begin page, you should locate the IP address of your router's internal interface before you proceed with the wizard. Standalone router devices usually have a web-based administration interface and a factory-configured IP address that is specified in the product documentation. To access the administration interface, you type that IP address in a web browser and log in using the access password, also specified in the product documentation.

MORE INFO **TCP/IP routers, by definition, have two IP addresses because their function is to connect two networks. The internal interface is the one connected to your private network, for which the router uses an address in the designated private IP address ranges. The external network interface is the one connected to your Internet service provider's (ISP's) network, which typically has a Dynamic Host Configuration Protocol (DHCP) server that assigns an IP address to the router.**

3. Click *Next*. The Detecting The Existing Network page appears.

The wizard attempts to detect a router on the network and access its settings. If the attempt is successful, the Detecting The Router And Configuring Your Network page appears. This page specifies the IP address of the router's internal interface, which becomes the Default Gateway address for all your network computers, and the IP address that the wizard configures your server to use.



Detecting the router and configuring your network

✓ The server detected that your router is at the IP address 10.0.0.1. If this is not the IP address of the router, or the server IP address is not acceptable, you can type a different value for the router IP address.

Network IP Addresses

Router IP Address: 10 . 0 . 0 . 1

Server IP Address: 10 . 0 . 0 . 2

How do I find out the IP address of my router?

If there is a router on your network, and the wizard fails to detect it, the wizard leaves the *Router IP address* and *server IP address* text boxes blank. Click *Cancel* to exit the wizard, troubleshoot your router, and restart the wizard.

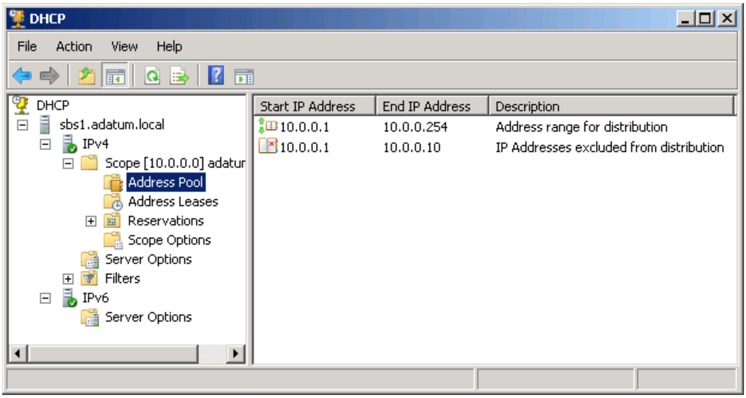
4. If the *Router IP address* and *Server IP address* values that appear on the page are correct, click *Next*. If the *Router IP address* and *Server IP address* fields are incorrect or blank, then troubleshoot your router (if necessary), supply the correct values, and click *Next*. The wizard configures your server, and the Your Network Is Now Connected To The Internet! page appears.
5. Click *Finish*. The wizard closes.

MORE INFO **The previous procedure assumes that you have a properly functioning router connected to your network and configured to access the Internet. For more information on choosing and setting up an Internet access router, see the sections entitled "Selecting a Router" and "Connecting Your Router," in Chapter 3, "Installing Windows Small Business Server (SBS) 2011."**

The basic function of the Connect To The Internet Wizard is to configure your server with an IP address on the same network as your router, and a Default Gateway address that is the same as the router's IP address. This enables the server to access the Internet through the router. In addition, the wizard configures the DHCP Server service on the computer running Windows SBS.

The Windows SBS 2011 setup program installs the DHCP Server role during the server installation whether a router is present on the network or not, leaving the DHCP Server unconfigured and the service stopped. The wizard configures the DHCP Server by starting the service and creating a scope. In DHCP parlance, a *scope* is a range of IP addresses that the server can allocate dynamically to clients on the network as needed.

As you can see in the DHCP Console, shown in Figure 4-4, the wizard has created a scope consisting of the IP addresses from *x.x.x.*1 to *x.x.x.*254 on the network it detected from the router. The wizard has also created an address exclusion for the scope, which prevents the service from allocating the IP addresses from *x.x.x.1* to *x.x.x.10*. This exclusion range includes the address of the router, the Windows SBS server address, and additional addresses for any other servers that you might want to install on the network at a later time.

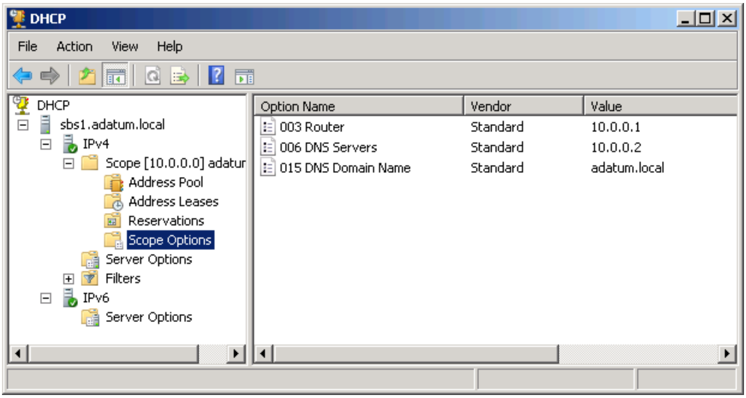


Start IP Address	End IP Address	Description
10.0.0.1	10.0.0.254	Address range for distribution
10.0.0.1	10.0.0.10	IP Addresses excluded from distribution

FIGURE 4-4 The DHCP Console, showing the scope that the Connect To The Internet Wizard created.

NOTE **In Figure 4-4, the DHCP scope is using the 192.168.2.0 network address because this happens to be the private network address that the router uses. Your router might use a different address, and the wizard configures the DHCP scope accordingly.**

In addition to the range of IP addresses and the exclusion range, the wizard also configures the DHCP scope with scope options, as shown in Figure 4-5. *Scope options* are additional TCP/IP configuration settings that the DHCP server delivers to clients along with an IP address.



Option Name	Vendor	Value
003 Router	Standard	10.0.0.1
006 DNS Servers	Standard	10.0.0.2
015 DNS Domain Name	Standard	adatum.local

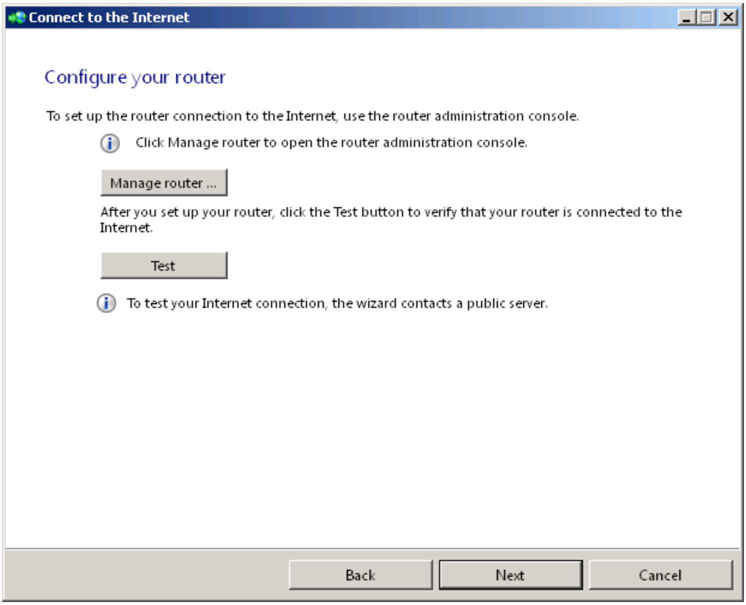
FIGURE 4-5 The DHCP Console, showing the scope options that the Connect To The Internet Wizard created.

The scope options that the wizard configures are as follows:

- **003 Router** Specifies the IP address of the router, which the client should use for its Default Gateway address
- **006 DNS servers** Specifies the IP address of the server running Windows SBS 2011, which functions as a DNS server and which the client should use for its Preferred DNS Server address
- **015 DNS Domain name** Specifies the name of the internal domain that you created during the Windows SBS 2011 installation

If the wizard fails to detect a router on the network, you can still specify values for the *Router IP address* and *Server IP address* fields. After you confirm that you want the server configuration process to continue, the wizard configures the TCP/IP and DHCP Server settings just as if a router were present and then displays pages that help you to configure your router for Internet access.

The Configure Your Router page, shown in Figure 4-6, enables you to connect to your router's administration console so that you can manually configure it and then test its Internet connectivity. This function assumes that the router uses web-based configuration and the standard port number (80) for its interface. If the router is configured to use a nonstandard port number for the administrative interface, you can connect to it with a web browser using a uniform resource locator (URL) that specifies both an IP address and a port number, as in the following example: *http://10.0.0.1:4096*. If the router uses a different type of administrative interface, consult the router manufacturer's documentation to determine how to access it.



Connect to the Internet

Configure your router

To set up the router connection to the Internet, use the router administration console.

ⓘ Click Manage router to open the router administration console.

After you set up your router, click the Test button to verify that your router is connected to the Internet.

ⓘ To test your Internet connection, the wizard contacts a public server.

FIGURE 4-6 The Configure Your Router page of the Connect To The Internet Wizard.

Before you proceed with the other wizards in the *Getting started tasks* list, you must complete this wizard successfully by connecting to the Internet through a router on your network. The Windows SBS Console does not permit the other wizards requiring Internet access to launch until the Connect To The Internet Wizard succeeds.

Customer Feedback Options

Selecting the *Customer feedback options* link causes a Customer Experience Improvement Program dialog box to appear, which asks if you want to allow Windows SBS to send information about your system hardware and usage trends anonymously to Microsoft for analysis.

Set Up Your Internet Address

For your users to send and receive Internet email or access your network services from a remote location, you must establish a presence on the Internet. This is different from simply accessing the Internet, which you configured the server to do when you ran the Connect To The Internet Wizard. Establishing a presence on the Internet enables users on the Internet to access your network's resources. To receive email from users outside your organization, for example, their messages must be able to reach the Microsoft Exchange Server application running on your server.

By default, Windows SBS 2011 configures your server to use a private IP address and a domain name with a *local* suffix (both of which are inaccessible from the Internet by design). To establish an Internet presence, you must register a domain name with an Internet domain registrar and configure your router to admit Internet traffic addressed to your server. The domain name enables Internet users to locate your network, and the router configuration lets the packets coming from those users pass through your firewall. Both of these tasks can be relatively complicated, but fortunately, Windows SBS 2011 includes an Internet Address Management Wizard that helps you to complete them.

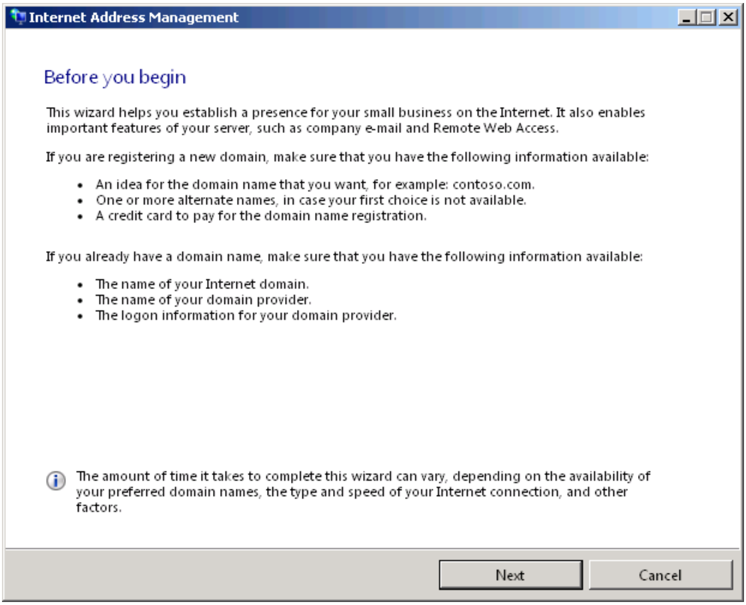
The Internet Address Management Wizard prompts you to select a domain name that is accessible from the Internet, as opposed to the local name you specified for your Active Directory Domain Services (AD DS) domain during the Windows SBS 2011 installation. The most common practice is to use the same second-level domain name, but with a different top-level domain. For example, if you use *adatum.local* for your internal domain, you might choose *adatum.com* for your Internet domain. You don't have to use the same second-level domain, however; you can use any domain name that is available for registration.

If the Internet domain name you select is available, the wizard enables you to register it with one of several commercial domain registrars. If you already have a registered domain name, the wizard lets you use that instead. Once you have a registered domain name, the wizard then configures your server, your router, and the Domain Name System records for the new domain.

Registering a New Domain

The Internet Address Management Wizard requires access to the Internet, so you must complete the Connect To The Internet Wizard first. Then, to run the wizard and register a new domain name, use the following procedure:

1. Log on to your Windows SBS 2011 primary server using an account with network Administrator privileges. The Windows SBS Console appears.
2. On the Home page of the Windows SBS Console, click *Set up your Internet address*. The Internet Address Management Wizard appears, displaying the Before You Begin page.



Before you begin

This wizard helps you establish a presence for your small business on the Internet. It also enables important features of your server, such as company e-mail and Remote Web Access.

If you are registering a new domain, make sure that you have the following information available:

- An idea for the domain name that you want, for example: contoso.com.
- One or more alternate names, in case your first choice is not available.
- A credit card to pay for the domain name registration.

If you already have a domain name, make sure that you have the following information available:

- The name of your Internet domain.
- The name of your domain provider.
- The logon information for your domain provider.

The amount of time it takes to complete this wizard can vary, depending on the availability of your preferred domain names, the type and speed of your Internet connection, and other factors.

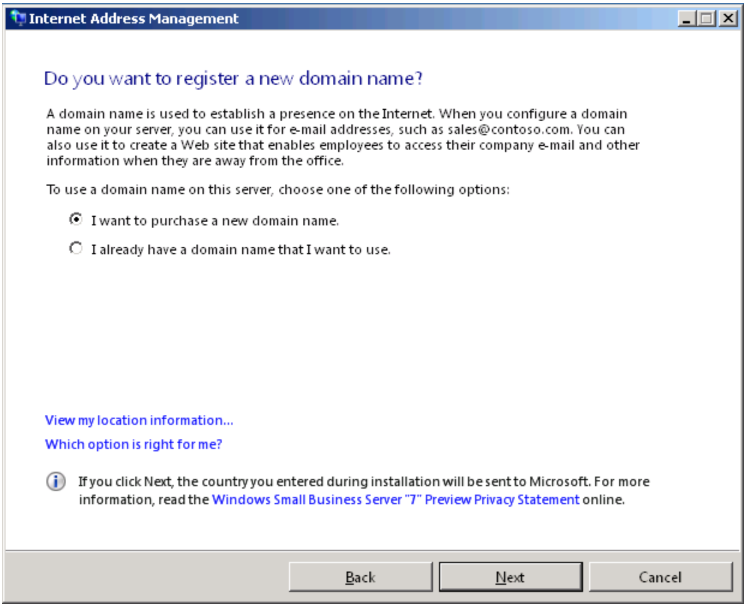
The Before You Begin page lists the resources that you need to complete the wizard, which vary, depending on whether you are registering a new domain name or using an existing one. To register a new name, you must have some idea what name you want to use and a credit card to pay the registration fee.

TIP **Determining what domain name to use for your organization can often be the hardest part of this entire process. In fact, you might want to begin your search for a domain name before you install Windows SBS 2011 and create your internal domain. The most popular generic top-level domains (gTLDs) on the Internet: *com*, *net*, and *org*, have millions of names already registered, and you might find it difficult to find a satisfactory name that is available for use.**

If your company name is already taken in the *com*, *net*, and *org* domains, you must either choose a variation on the company name, or select a different gTLD. For example, if you are the owner of an eponymously named company that manufactures kilts, and your surname is the same as that of a well-known fast food restaurant chain, you will probably not be able to register your company name in the *com* domain. Your alternatives are to either vary the name, such as by adding the word "kilts" to your surname, or register your surname in a less popular gTLD, such as *biz*.

To check on the availability of specific domain names before you run the Internet Address Management Wizard, you can use the WHOIS service provided by the Internet Corporation for Assigned Names and Numbers (ICANN), available at *http://www.internic.net/whois.html*.

3. Click *Next*. The Do You Want To Register A New Domain Name? page appears.



Do you want to register a new domain name?

A domain name is used to establish a presence on the Internet. When you configure a domain name on your server, you can use it for e-mail addresses, such as sales@contoso.com. You can also use it to create a Web site that enables employees to access their company e-mail and other information when they are away from the office.

To use a domain name on this server, choose one of the following options:

● I want to purchase a new domain name.

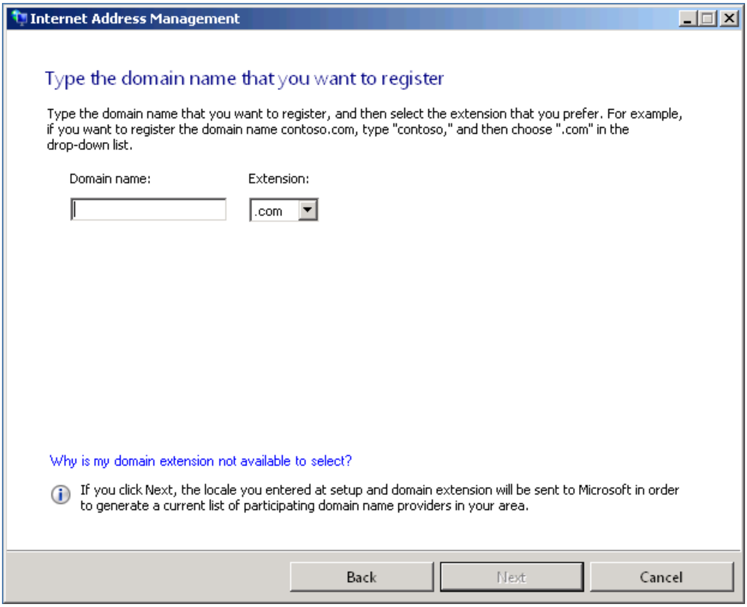
○ I already have a domain name that I want to use.

View my location information...

Which option is right for me?

If you click Next, the country you entered during installation will be sent to Microsoft. For more information, read the Windows Small Business Server "7" Preview Privacy Statement online.

4. Select the *I want to purchase a new domain name* option and click *Next*. The Type The Domain Name That You Want To Register page appears.



Type the domain name that you want to register

Type the domain name that you want to register, and then select the extension that you prefer. For example, if you want to register the domain name contoso.com, type "contoso," and then choose ".com" in the drop-down list.

Domain name:

Extension: .com

Why is my domain extension not available to select?

If you click Next, the locale you entered at setup and domain extension will be sent to Microsoft in order to generate a current list of participating domain name providers in your area.

5. In the *Domain name* text box, type the second-level domain name that you want to register. Then, from the *Extension* drop-down list, select the top-level domain that you want to use and click *Next*. The Choose A Domain Name Provider page appears.

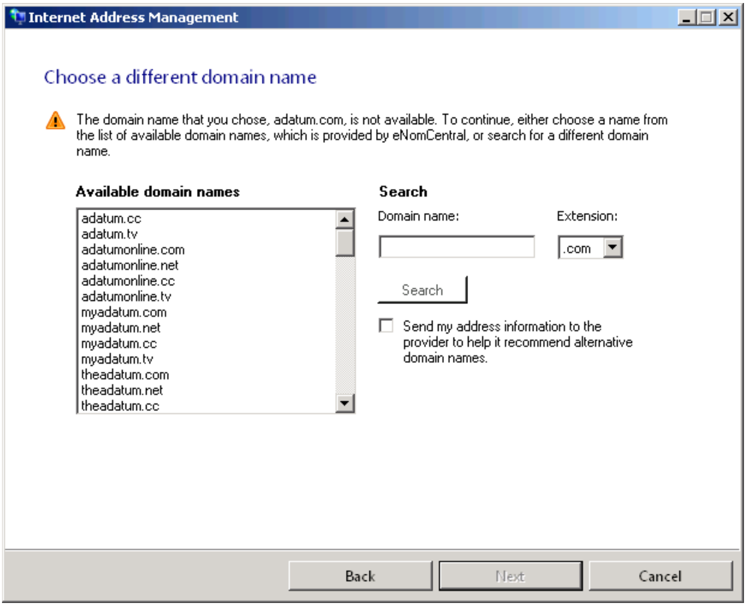
   The wizard displays a list of domain name registrars, based on the domain name that you entered and the location that you specified during the Windows SBS 2011 installation.

   NOTE **Although you can use any registrar to register your domain name, you must select one of the registrars suggested by the wizard for Windows SBS 2011 to manage your domain fully.**

6. Select the domain registrar that you want to use and click *Next*. The wizard sends the name you specified to the selected registrar.

   TIP **You might want to examine each of the registrars' websites before you commit to one of them. Domain registration has become a highly competitive business in recent years, and prices can vary widely.**

7. If the name you specified is not available for registration, the Choose A Different Domain Name page appears, offering variations on the name that are available. Type an alternative name in the fields provided and click *Search*.



Internet Address Management

Choose a different domain name

The domain name that you chose, adatum.com, is not available. To continue, either choose a name from the list of available domain names, which is provided by eNomCentral, or search for a different domain name.

Available domain names

adatum.cc
adatum.tv
adatumonline.com
adatumonline.net
adatumonline.cc
adatumonline.tv
myadatum.com
myadatum.net
myadatum.cc
myadatum.tv
theadatum.com
theadatum.net
theadatum.cc

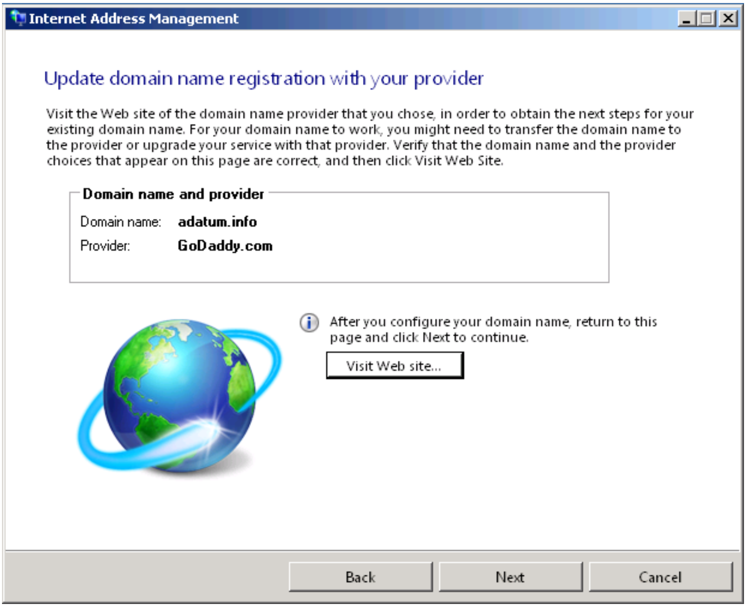
Search

Domain name:

Extension: .com

□ Send my address information to the provider to help it recommend alternative domain names.

8. If the name you specified is available for registration, the Register And Purchase The Domain Name page appears. Click *Register now* to open Internet Explorer and connect to the registrar's website.



Update domain name registration with your provider

Visit the Web site of the domain name provider that you chose, in order to obtain the next steps for your existing domain name. For your domain name to work, you might need to transfer the domain name to the provider or upgrade your service with that provider. Verify that the domain name and the provider choices that appear on this page are correct, and then click Visit Web Site.

Domain name and provider

Domain name: **adatum.info**

Provider: **GoDaddy.com**

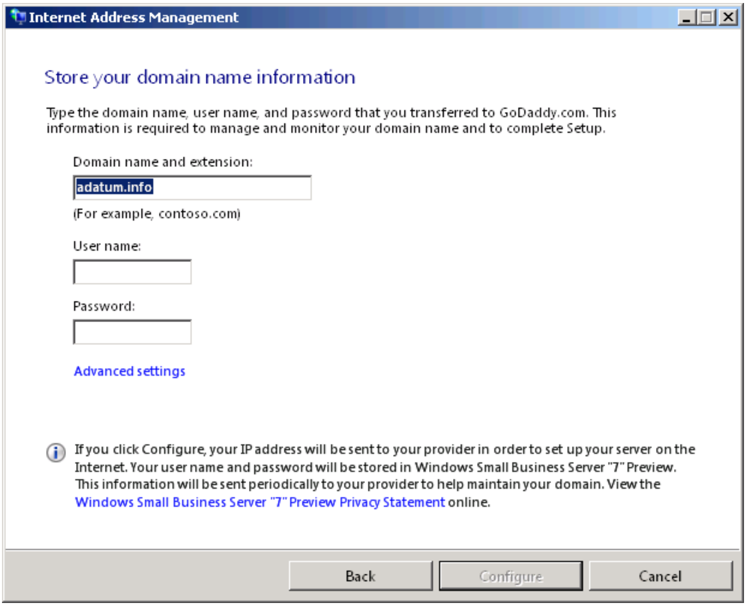
After you configure your domain name, return to this page and click Next to continue.

BEST PRACTICES **Domain name registrars are commercial enterprises, and they may very likely try to sell you a variety of additional products and services before you complete the registration process. While you might want to consider some of their offers, you don't need anything other than a standard domain name registration to complete the wizard and finish configuring your server.**

9. Use the form on the registrar's website to register your selected domain name. You have to supply, at minimum, your name, mailing address, telephone number, and credit card information to complete the registration process.

NOTE **The registrar adds the contact information that you supply to the WHOIS database, in which it is available to anyone who searches for your domain name. Domain name registration listings must have an administration, a billing, and a technical contact. These can all be the same person, or you can specify a different individual for each one. Because this is public information, many organizations use a post office box or pay an additional fee for a private registration to prevent their contact information from being harvested by spammers.**

10. Once you have completed the registration process on the website, return to the wizard and click *Next*. The Store Your Domain Name Information page appears.



Store your domain name information

Type the domain name, user name, and password that you transferred to GoDaddy.com. This information is required to manage and monitor your domain name and to complete Setup.

Domain name and extension:

adatum.info

(For example, contoso.com)

User name:

Password:

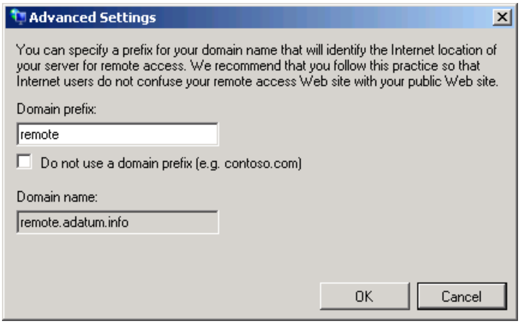
Advanced settings

If you click Configure, your IP address will be sent to your provider in order to set up your server on the Internet. Your user name and password will be stored in Windows Small Business Server "7" Preview. This information will be sent periodically to your provider to help maintain your domain. View the Windows Small Business Server "7" Preview Privacy Statement online.

11. In the *Domain name and extension* text box, type your full domain name, with the suffix.
12. In the *User name* and *password* text boxes, type the credentials that provide access to your account on the registrar's website.

NOTE **Some registrars have you supply the user name and password that you want to use during the registration process, while others assign credentials to you.**

By default, the wizard uses the name *remote* for the Windows SBS 2011 Remote Web Workplace site, so that the Internet URL for the domain *adatum.info* would be *http://remote.adatum.info*. If you want to use a different name, click *Advanced settings* to display the Advanced Settings dialog box, shown in the following illustration, in which you can specify an alternative.



You can specify a prefix for your domain name that will identify the Internet location of your server for remote access. We recommend that you follow this practice so that Internet users do not confuse your remote access Web site with your public Web site.

Domain prefix:

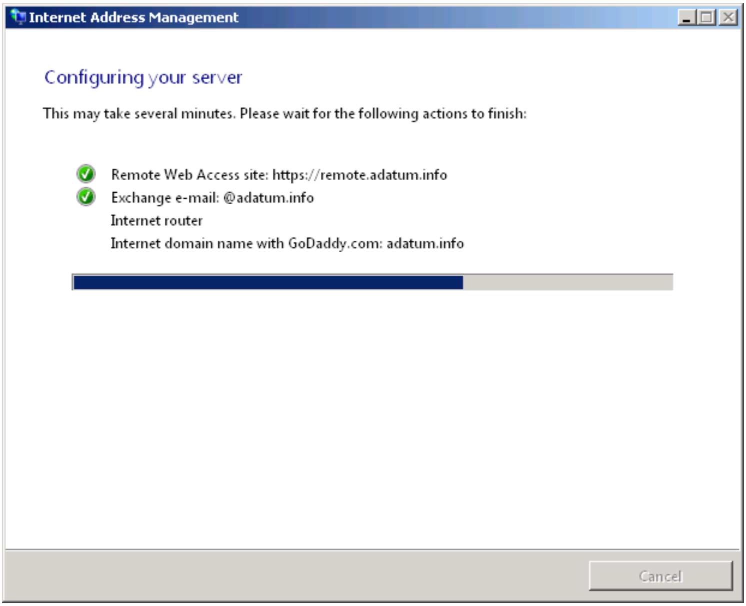
remote

□ Do not use a domain prefix (e.g. contoso.com)

Domain name:

remote.adatum.info

13. Click *Configure*. The Configuring Your Server page appears, displaying the wizard's progress as it configures the server, the router, and the DNS resource records for the domain.



Configuring your server

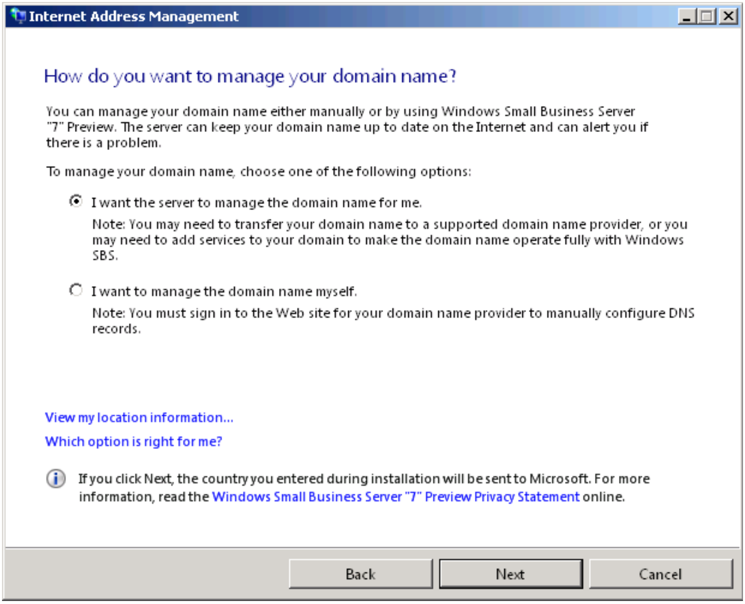
This may take several minutes. Please wait for the following actions to finish:

✓ Remote Web Access site: https://remote.adatum.info
✓ Exchange e-mail: @adatum.info
Internet router
Internet domain name with GoDaddy.com: adatum.info

14. When the configuration process finishes, the Congratulations! page appears, summarizing the wizard's results and displaying any warnings that might have occurred.
15. Click *Finish*. The wizard closes.

Using an Existing Domain

If you already have a registered domain on the Internet, you can still use the Internet Address Management Wizard to configure your network to use it. When you select the *I already have a domain name that I want to use* option on the Do You Want To Register A New Domain Name? page and click *Next*, a How Do You Want To Manage Your Domain Name? page appears, as shown in Figure 4-7.



Internet Address Management

How do you want to manage your domain name?

You can manage your domain name either manually or by using Windows Small Business Server "7" Preview. The server can keep your domain name up to date on the Internet and can alert you if there is a problem.

To manage your domain name, choose one of the following options:

● I want the server to manage the domain name for me.

Note: You may need to transfer your domain name to a supported domain name provider, or you may need to add services to your domain to make the domain name operate fully with Windows SBS.

○ I want to manage the domain name myself.

Note: You must sign in to the Web site for your domain name provider to manually configure DNS records.

View my location information...

Which option is right for me?

If you click Next, the country you entered during installation will be sent to Microsoft. For more information, read the Windows Small Business Server "7" Preview Privacy Statement online.

FIGURE 4-7 The How Do You Want To Manage Your Domain Name? page in the Internet Address Management Wizard.

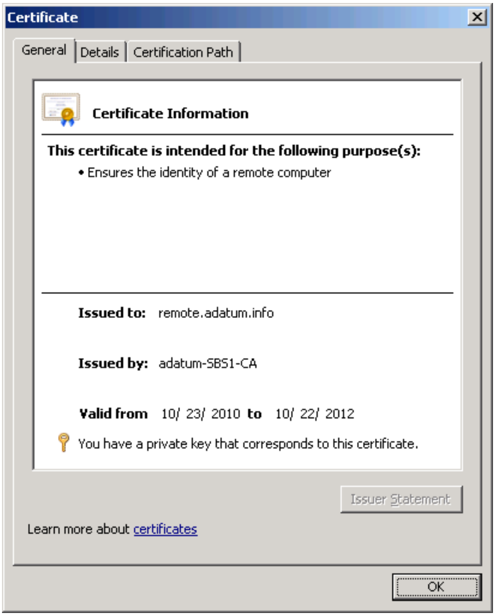
This page provides the following two options:

- *I want the server to manage the domain name for me* To use this option, your domain name must be registered with one of the registrars supported by the wizard. If you have registered your domain with another registrar, the wizard gives you the opportunity to transfer the domain to one of the supported registrars, a process that can take several days. Once you have completed the transfer, the wizard proceeds as with a newly registered domain.
- *I want to manage the domain name myself* If you decide to leave your domain name with another registrar, the wizard configures your server and your router, but it cannot create the new resource records your network needs on your registrar's DNS servers. In this case, you must create those resource records yourself, using the interface supplied by the registrar and the information in the next section.

Understanding the Wizard's Configurations

During the configuration phase, the Internet Address Management Wizard makes a variety of changes to the various components involved in your presence on the Internet. First, on your server running Windows SBS 2011, the wizard configures the following services:

- **Certification Authority (CA)** The wizard has the CA on the server issue a certificate for the Remote Web Workplace website, as shown in Figure 4-8. This certificate enables users on the Internet to confirm that the RWW that they are connecting to is authentic.



Certificate Information

This certificate is intended for the following purpose(s):
- Ensures the identity of a remote computer

Issued to: remote.adatum.info

Issued by: adatum-SBS1-CA

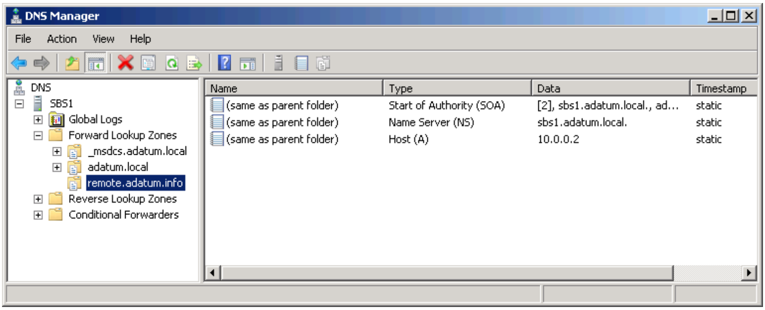
Valid from 10/ 23/ 2010 to 10/ 22/ 2012

You have a private key that corresponds to this certificate.

Learn more about certificates

FIGURE 4-8 The certificate for the RWW site, issued by the CA.

- **Domain Name System (DNS)** On the server's DNS server, the wizard creates a zone for the *remote* third-level domain beneath the Internet domain that you registered, as shown in Figure 4-9. This makes the DNS server the authoritative source for information about this third-level domain.



Name	Type	Data	Timestamp
(same as parent folder)	Start of Authority (SOA)	[2], sbs1.adatum.local., ad...	static
(same as parent folder)	Name Server (NS)	sbs1.adatum.local.	static
(same as parent folder)	Host (A)	10.0.0.2	static

FIGURE 4-9 The DNS Manager Console, showing the third-level domain created by the Internet Address Management Wizard.

- **Internet Information Services (IIS)** The wizard configures IIS on the server to recognize incoming web traffic addressed to the *remote* domain and forward it to the Remote Web Workplace site.
- **Simple Mail Transfer Protocol (SMTP)** The wizard configures Exchange Server 2010 to process incoming SMTP traffic addressed to the domain you registered.

Next, the wizard uses the credentials you supplied to connect to your registrar's website and configure DNS records for your newly registered domain. What you are actually paying for when you register a domain is space on the registrar's DNS servers, in which you can create resource records in that domain.

MORE INFO **For more information on domain names and the Domain Name System (DNS), see the section entitled "Understanding Domains" in Chapter 2, "A Networking Primer."**

Using the interface provided by the registrar, the wizard automatically creates the resource records listed in Table 4-1.

TABLE 4-1 DNS Resource Records for Your Internet Domain

RECORD TYPE	NAME	RECORD SETTINGS	RECORD FUNCTION
Host (A)	remote	IP address of your router's external interface	Maps the remote name in your domain to your router's Internet IP address
Mail Exchanger (MX)	domain.com	remote.domain.com	Directs SMTP mail traffic to your server running Windows SBS 2011

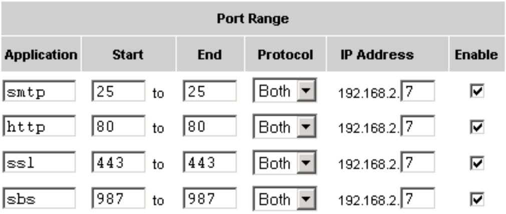
RECORD TYPE	NAME	RECORD SETTINGS	RECORD FUNCTION
Text (TXT)	domain.com	v=spf1 a mx ~all	Prevents email sent by your internal users from being flagged as spam

Service (SRV)	_autodiscover	Protocol = _tcp
		Priority = 0
		Weight = 0
		Port = 443
		Target = remote.*domain.com*
			Enables remote email users to configure the Outlook Anywhere client automatically

NOTE **In this table, replace *domain.com* with your full Internet domain name and suffix.**

Finally, if your router conforms to the Universal Plug and Play (UPnP) standard, the wizard configures your router by opening ports 25, 80, 443, and 987, so that traffic arriving from the Internet using those ports can pass through the firewall to your server running Windows SBS 2011.

If your router does not support UpnP, you must configure it yourself to admit traffic through those ports and forward it to the server's IP address. A router's configuration site typically provides an interface for this like the one shown in Figure 4-10.



Port Range						
Application	**Start**		**End**	**Protocol**	**IP Address**	**Enable**
smtp	25	to	25	Both	192.168.2.7	☑
http	80	to	80	Both	192.168.2.7	☑
ssl	443	to	443	Both	192.168.2.7	☑
sbs	987	to	987	Both	192.168.2.7	☑

FIGURE 4-10 A typical port-forwarding interface in a router's configuration site.

Configure a Smart Host for Internet Email

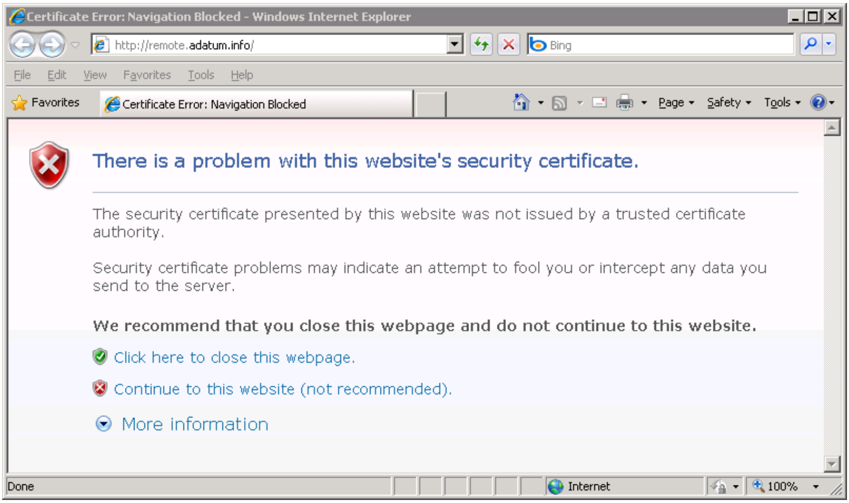
A *smart host* is an external email server, typically operated by an ISP, which you can use as an intermediate stop for your users' outgoing email. For more information on configuring a smart host, see Chapter 15, "Administering Email."

Add a Trusted Certificate

Digital certificates are electronic documents that verify the identity of a computer or a user. By default, a server running Windows SBS 2011 creates self-signed certificates for the intranet websites it hosts and for its domain controller functions. Self-signed certificates are sufficient for internal functions because users on the network can trust the authority of their local server.

When a client computer first uses one of these internal functions, it automatically applies for and receives a certificate from the server, a process called *autoenrollment*. The process is invisible to the users on the network, but they can open the Certificates snap-in on their computers and look at the certificates they have received.

However, Internet users are not logged on to the AD DS domain, so they cannot obtain certificates using autoenrollment. When a remote user on the Internet connects to a Windows SBS 2011 resource on your network, such as the RWW website, the browser displays an error message, as shown in Figure 4-11. This message appears because the web server has generated its own certificate, and on the Internet, a computer that verifies its own identity is not trustworthy.


Certificate Error: Navigation Blocked - Windows Internet Explorer
http://remote.adatum.info/
Bing
File Edit View Favorites Tools Help
Favorites
Certificate Error: Navigation Blocked
Page Safety Tools
Done
Internet
100%

There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

More information

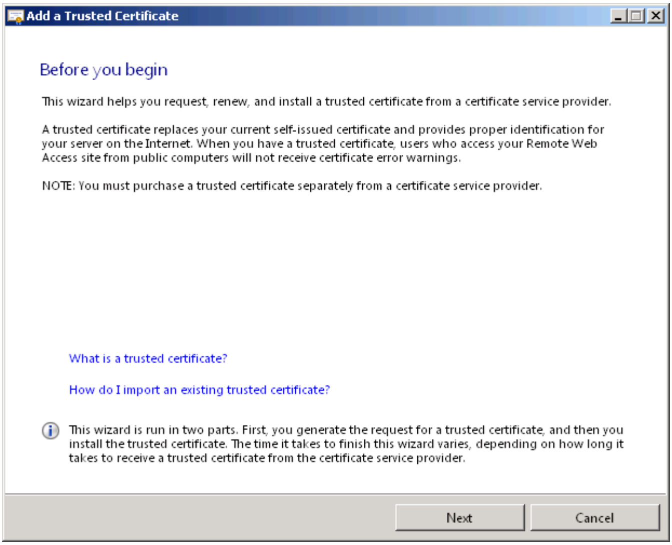
FIGURE 4-11 A certificate error in a web browser.

For users conscious of this situation, clicking the *Continue to this website (not recommended)* link presents no danger, but to eliminate the error message, the server must have a certificate issued by a third party that both the clients and the server trust. The third party is typically a commercial CA that is in the business of confirming the identities of clients and issuing certificates attesting to that identity.

> ***MORE INFO*** **You can also eliminate the error message by deploying your server's self-signed certificate on the remote computer. For more information, see Chapter 13, "Managing Windows SBS 2011."**

The Getting Started Tasks page provides an Add A Trusted Certificate Wizard that simplifies the process of enrolling for and installing a third-party certificate. To run the wizard, use the following procedure:

1. Log on to your Windows SBS 2011 primary server, using an account with network Administrator privileges. The Windows SBS Console window appears.
2. On the Home page of the Windows SBS Console, click *Add a trusted certificate*. The Add A Trusted Certificate Wizard appears, displaying the Before You Begin page.



Before you begin

This wizard helps you request, renew, and install a trusted certificate from a certificate service provider.

A trusted certificate replaces your current self-issued certificate and provides proper identification for your server on the Internet. When you have a trusted certificate, users who access your Remote Web Access site from public computers will not receive certificate error warnings.

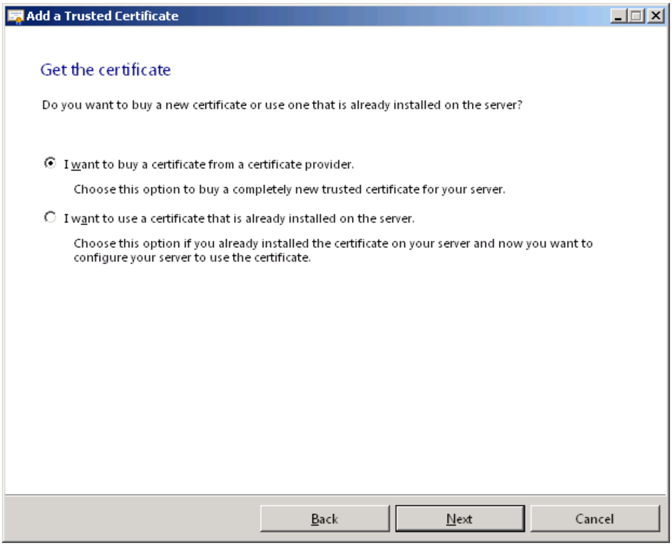
NOTE: You must purchase a trusted certificate separately from a certificate service provider.

What is a trusted certificate?

How do I import an existing trusted certificate?

This wizard is run in two parts. First, you generate the request for a trusted certificate, and then you install the trusted certificate. The time it takes to finish this wizard varies, depending on how long it takes to receive a trusted certificate from the certificate service provider.

3. Click *Next*. The Get The Certificate page appears.



Get the certificate

Do you want to buy a new certificate or use one that is already installed on the server?

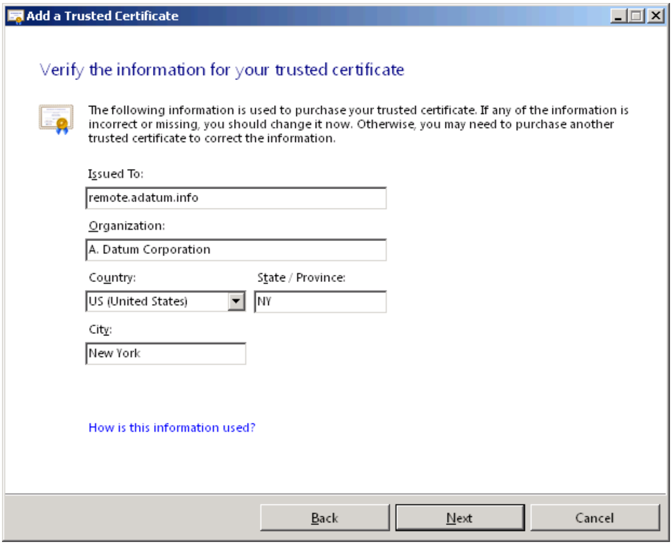
● I want to buy a certificate from a certificate provider.

Choose this option to buy a completely new trusted certificate for your server.

○ I want to use a certificate that is already installed on the server.

Choose this option if you already installed the certificate on your server and now you want to configure your server to use the certificate.

4. Select the *I want to buy a certificate from a certificate provider* option and click *Next*. The Verify The Information For Your Trusted Certificate page appears, containing the name of your *remote* site and the company and address information you supplied during the Windows SBS 2011 installation.



Verify the information for your trusted certificate

The following information is used to purchase your trusted certificate. If any of the information is incorrect or missing, you should change it now. Otherwise, you may need to purchase another trusted certificate to correct the information.

Issued To: remote.adatum.info

Organization: A. Datum Corporation

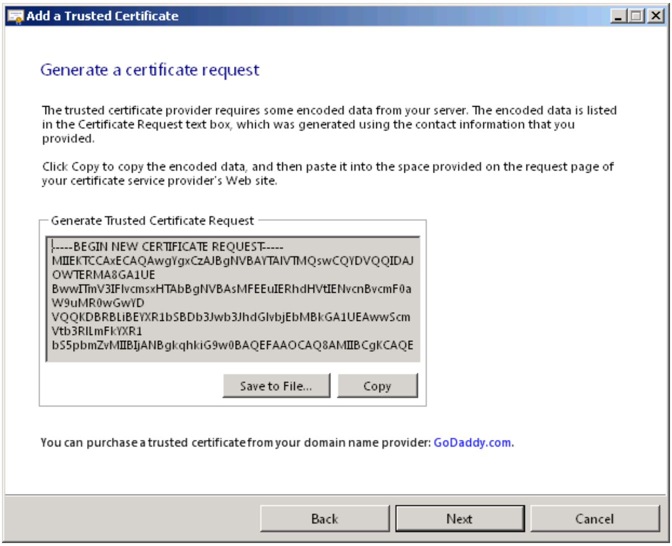
Country: US (United States)

State / Province: NY

City: New York

How is this information used?

5. Modify the company and address information, if necessary, and click *Next*. The Generate A Certificate Request page appears.



Generate a certificate request

The trusted certificate provider requires some encoded data from your server. The encoded data is listed in the Certificate Request text box, which was generated using the contact information that you provided.

Click Copy to copy the encoded data, and then paste it into the space provided on the request page of your certificate service provider's Web site.

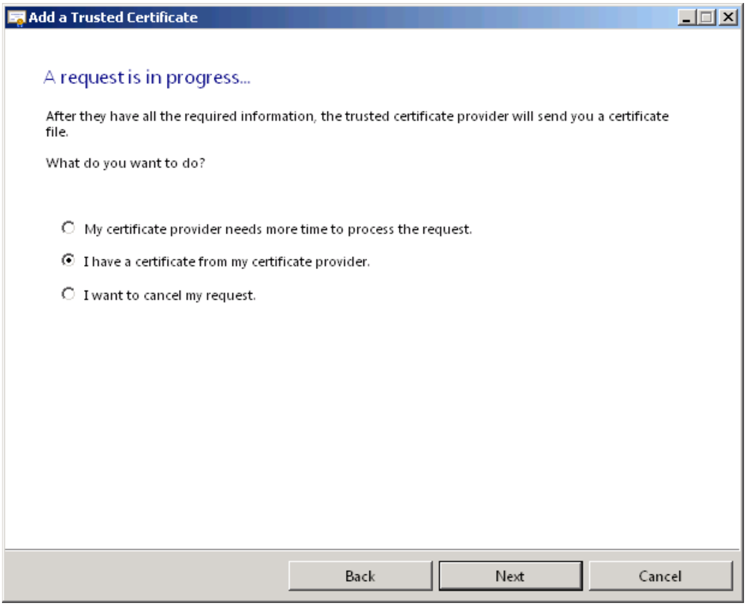
Generate Trusted Certificate Request

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIEKTCCAxECAQAwgYgxCzAJBgNVBAYTAlVTMQswCQYDVQQIDAJ
OWTERMA8GA1UE
BwwITmV3IFlvcmsxHTAbBgNVBAsMFEEuIERhdHVtIENvcnBvcmF0a
W9uMR0wGwYD
VQQKDBRBLiBEYXR1bSBDb3Jwb3JhdGlvbjEbMBkGA1UEAwwScm
Vtb3RlLmFkYXR1
bS5pbmZvMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQE
```

You can purchase a trusted certificate from your domain name provider: GoDaddy.com.

NOTE If your domain name registrar can also supply certificates, the wizard displays a link to its site. However, you can use any provider you want to obtain your certificate.

6. Click *Copy* to copy the certificate request to the clipboard or click *Save to file* to save the request as a file on your local drive.
7. Click *Next*. The A Request Is In Progress page appears.



Add a Trusted Certificate

A request is in progress...

After they have all the required information, the trusted certificate provider will send you a certificate file.

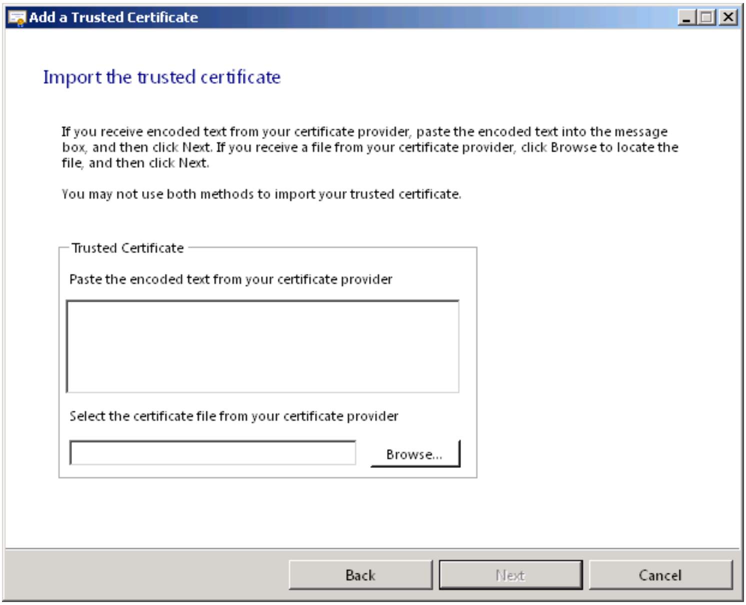
What do you want to do?

○ My certificate provider needs more time to process the request.

● I have a certificate from my certificate provider.

○ I want to cancel my request.

8. Open the website of the certificate provider that you want to use and submit your request by pasting the contents of the Clipboard into the appropriate form or uploading the request file that you saved. After you pay a fee and supply the correct information, the provider issues a certificate, either as text you can copy to the Clipboard or as a file you can download.
9. Return to the Add A Trusted Certificate Wizard, make sure that the *I have a certificate from my certificate provider* option is selected, and click *Next*. The Import The Trusted Certificate page appears.



Import the trusted certificate

If you receive encoded text from your certificate provider, paste the encoded text into the message box, and then click Next. If you receive a file from your certificate provider, click Browse to locate the file, and then click Next.

You may not use both methods to import your trusted certificate.

Trusted Certificate

Paste the encoded text from your certificate provider

Select the certificate file from your certificate provider

10. In the *Trusted certificate* box, either paste the text that you copied from the certificate provider's site or click *Browse* to select the file that you downloaded, and then click *Next*. A The Trusted Certificate Is Imported Successfully page appears.
11. Click *Finish*. The wizard closes.

Configure Server Backup

The *Getting started tasks* list contains a link to the Configure Server Backup Wizard, which you can also access from the Backup And Server Storage page of the Windows SBS Console. For information on performing backups and restores on your server running Windows SBS 2011, see Chapter 12, "Backing Up and Restoring."

Adding Users and Computers

To connect workstations to your network, you must create user accounts and join the computers to your AD DS domain. The Add A New User Account Wizard in the *Getting started tasks* list is also accessible from the Users And Groups page in the Windows SBS Console. The Connect Computers To Your Network Wizard is also accessible from the Network page. For information on using these wizards, see Chapter 6.

CHAPTER 5

Migrating to Windows SBS 2011

For users of previous versions of Windows SBS, Windows SBS 2011 is not a simple upgrade. Microsoft does not provide an in-place upgrade path from Windows SBS 2003 R2 or Windows SBS 2008 to Windows SBS 2011 for several reasons, including these:

- **Hardware requirements** Windows SBS 2003 R2 runs on a computer with a 32-bit processor and a maximum of 4 GB of memory. The Microsoft Exchange Server 2003 SP2 product is also a 32-bit application. Windows SBS 2008 and Windows SBS 2011 both require a 64-bit processor and a minimum of 4 GB and 8 GB of memory, respectively. All versions of Exchange since Exchange Server 2007 are also 64-bit applications.
- **Network configuration** Windows SBS 2003 R2 is designed to function as a router between a private small-business network and the Internet. The Premium Edition includes the Internet and Security Acceleration (ISA) Server 2004 product to help secure this configuration. However, in Windows SBS 2008, Microsoft recognized that connecting a domain controller to the Internet is an inherently insecure practice, and in response, the company redesigned the default configuration to use a single network interface on the server and a separate router device connecting the network to the Internet. Windows SBS 2011 maintains the same configuration.

- **Application compatibility** Each subsequent version of Windows SBS includes new applications or new application versions that do not support in-place upgrades. For example, Windows SBS 2008 omits the ISA Server 2004 product from Windows SBS 2003 R2, in favor of the Network Policy Server role now included in Windows Server 2008 R2. However, the two are not exact equivalents, and there is no direct upgrade path between them. In the same way, Windows Server 2011 includes Exchange Server 2010, which does not support in-place upgrades from Exchange Server 2007.
- **Edition configurations** The Premium editions of Windows SBS 2003 R2 and Windows SBS 2008 both add SQL Server to the package, but the 2003 product incorporates it into its single-server environment. Windows SBS 2008 Premium calls for a second computer, on which you install SQL Server. In Windows SBS 2011, Microsoft has changed the second server option to a separate add-on product, rather than an alternate version of the main SBS product.

To upgrade from Windows SBS 2003 R2 or Windows SBS 2008 to Windows SBS 2011, you must install a new server computer; migrate your domain, configuration settings, and data from the old system to the new; and then demote or remove the old computer. If you purchase Windows SBS 2008 Premium or the Windows SBS 2011 Premium Add-On product, you can conceivably perform the migration to a new server and then use the old computer as your secondary server.

Understanding the Migration Process

The process of migrating from Windows SBS 2003 R2 or Windows SBS 2008 to Windows SBS 2011 consists of six basic steps:

1. Prepare the existing Windows SBS source server for migration.
2. Create a migration answer file.
3. Install Windows SBS 2011 on a new server using the answer file.
4. Run the Migration Wizard to transfer settings and data.
5. Demote the old Windows SBS source server.
6. Reconfigure Folder Redirection.

The following sections examine each of these steps in greater detail.

Preparing for Migration

For the migration process to complete successfully, you must properly prepare your existing server running Windows SBS. Windows SBS 2011 includes a Migration Preparation Tool that you must install on your existing Windows SBS server, to prepare it for the migration. Among other things, this tool:

- Raises the domain and forest functional levels
- Updates the Active Directory Domain Services schema

- Extends the allowable migration timeline
- Enables the migration of Exchange Server data
- Scans the source server for potential problems

Be sure to complete all the tasks in the following sections to begin your server migration.

Back Up

The migration process makes significant changes to your existing server, so it is imperative that you perform a full backup, including the system state, before you proceed with the migration. You should also perform some test restores of individual files to make sure that you have a viable backup. If the migration fails, or you want to return to your old Windows SBS version for any reason, your only recourse might be to restore the server from this backup.

Install Updates

Install the latest service packs on your existing Windows SBS server, as well as all the latest critical and optional updates. You must also install the latest service packs for Windows Server itself, Exchange Server, SharePoint Services, SQL Server Express, and Microsoft Core XML Services (MSXML) 6.0. Finally, make sure that the computer has the latest updates of the Microsoft .NET Framework environment.

Install Required Software

Before you can install and run the Migration Preparation Tool on your source server, you must download and install the following components:

- **Windows PowerShell 2.0** PowerShell 2.0 is included as part of the Windows Management Framework package, available as a free download from Microsoft Support at *http://go.microsoft.com/FWLink/?Linkid=188528*
- **Microsoft Baseline Configuration Analyzer 2.0** Available from the Microsoft Download Center at *http://go.microsoft.com/FWLink/?Linkid=188529*

Reconfigure the Network

If you are running Windows SBS 2003 R2 and your server provides the shared Internet connection for your network, you must unplug the network adapter connected to the modem or other Internet access device. Then you must purchase and install a separate router device and configure it to connect to the Internet, as described in the sections “Selecting a Router” and “Connecting Your Router” in Chapter 3, “Installing Windows Small Business Server 2011.” If you are running Windows SBS 2008, you should already have a separate router connecting your network to the Internet.

If you are running any third-party applications on your server, you should consult the product documentation or the software manufacturers for information on how to migrate them to your new server. In most cases, you must reinstall the application on your new server running Windows SBS 2011 and migrate your data from the old one.

Synchronize Computer Clocks

For the migration process to succeed, the source server running Windows SBS 2003 R2 or Windows SBS 2008 and the new server running Windows SBS 2011 must have the same date and time zone settings, and their clocks must be set to within five minutes of each other.

Install the Migration Preparation Tool

To install the Migration Preparation Tool, follow these steps:

1. Log on to your Windows SBS source server, using an account that is a member of the Domain Admins, Enterprise Admins, and Schema Admins groups.
2. Insert Windows SBS 2011 Disk 1 into the computer's DVD-ROM drive. The Windows Small Business Server 2011 screen appears, as shown in Figure 5-1.

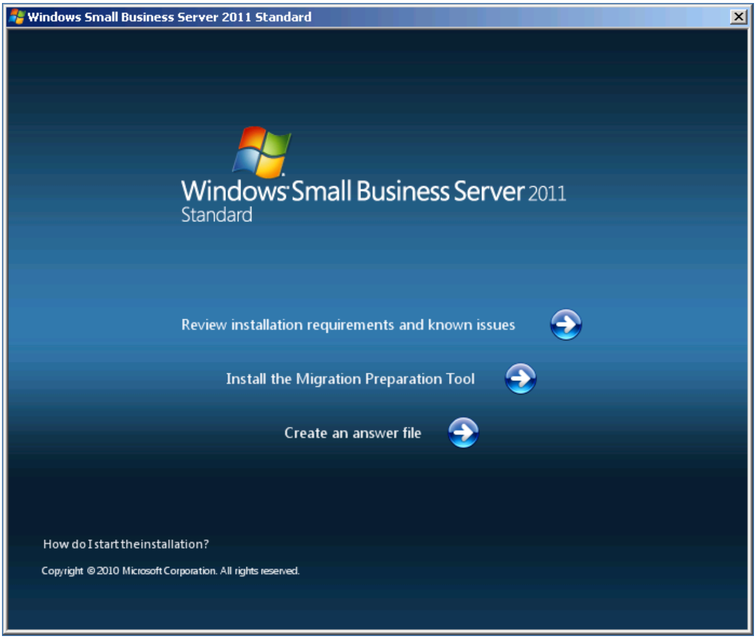

Windows Small Business Server 2011 Standard
Windows Small Business Server 2011
Standard
Review installation requirements and known issues
Install the Migration Preparation Tool
Create an answer file
How do I start the installation?
Copyright © 2010 Microsoft Corporation. All rights reserved.

FIGURE 5-1 The Windows Small Business Server 2011 screen.

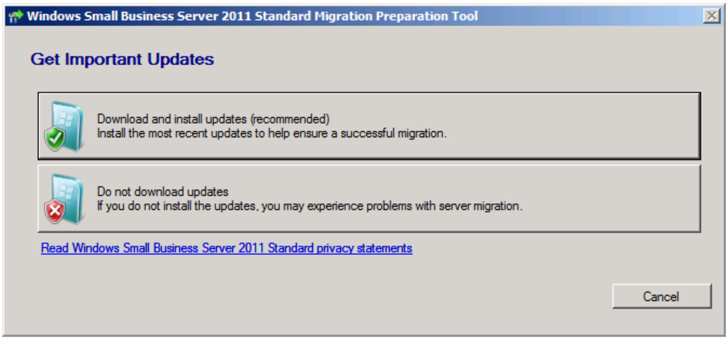
3. Click *Install the migration preparation tool*. The Windows Small Business Server 2011 Migration Preparation Tool Setup Wizard appears.
4. Click *Next* to bypass the Welcome page. The Windows Small Business Server 2011 Migration Preparation Tool License Agreement page appears.
5. Select the *I accept the terms in the license agreement* check box and click Install. A User Account Control message box appears.
6. Click *Continue*. The wizard installs the tool, and the Completed The Windows Small Business Server 2011 Migration Preparation Tool Setup Wizard page appears.
7. Click *Finish*. The wizard closes.

Run the Migration Preparation Tool

Active Directory Domain Services (AD DS) is based on a set of *schema*, which specify what kinds of objects can exist in the directory and what attributes are associated with each object type. The schema for Windows SBS 2003 R2 and Windows SBS 2008 are different from those in Windows SBS 2011, so you must update your existing server by running the Migration Preparation Tool you installed from Disk 1 of your Windows Server 2011 product package.

To run the tool, use the following procedure:

1. Click *Start* and then click *All Programs* > *Windows Small Business Server Tools* > *Windows Small Business Server 2011 Migration Preparation Tool*. A User Account Control message box appears.
2. Click *Continue*. The tool appears, displaying the Get Important Updates page.



Windows Small Business Server 2011 Standard Migration Preparation Tool

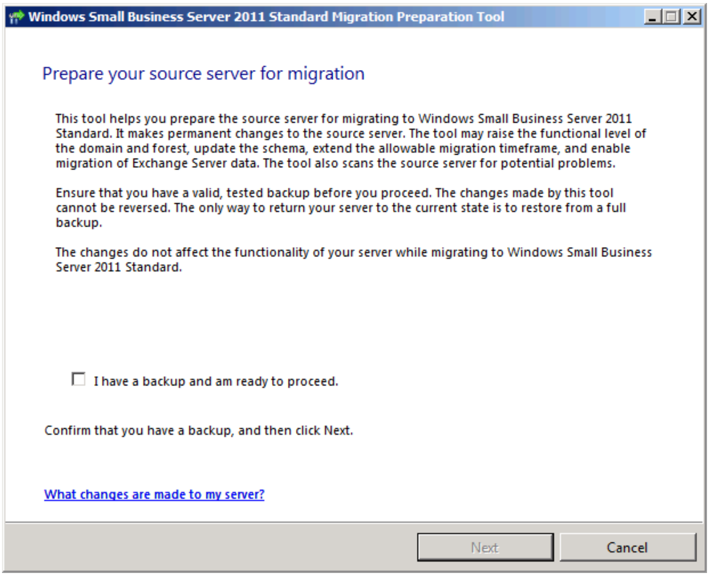
Get Important Updates

Download and install updates (recommended)
Install the most recent updates to help ensure a successful migration.

Do not download updates
If you do not install the updates, you may experience problems with server migration.

Read Windows Small Business Server 2011 Standard privacy statements

3. Click *Download and install updates (recommended)*. The system downloads and installs any required updates, after which the Prepare Your Source Server For Migration page appears.



Windows Small Business Server 2011 Standard Migration Preparation Tool

Prepare your source server for migration

This tool helps you prepare the source server for migrating to Windows Small Business Server 2011 Standard. It makes permanent changes to the source server. The tool may raise the functional level of the domain and forest, update the schema, extend the allowable migration timeframe, and enable migration of Exchange Server data. The tool also scans the source server for potential problems.

Ensure that you have a valid, tested backup before you proceed. The changes made by this tool cannot be reversed. The only way to return your server to the current state is to restore from a full backup.

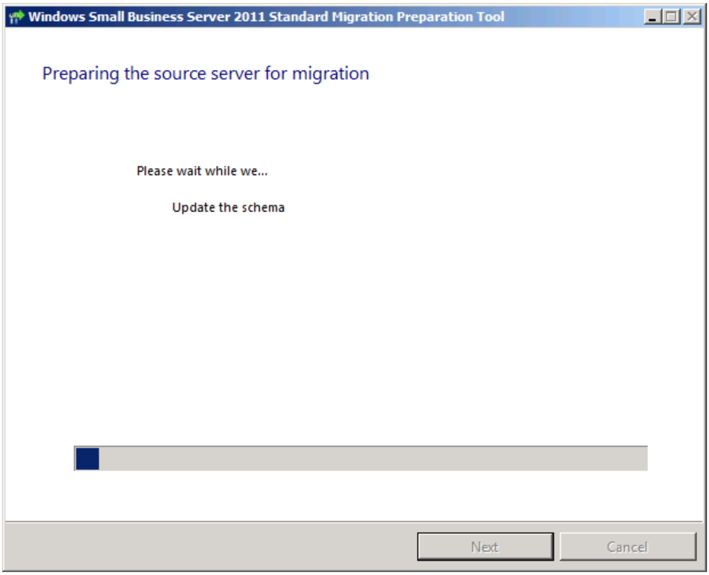
The changes do not affect the functionality of your server while migrating to Windows Small Business Server 2011 Standard.

□ I have a backup and am ready to proceed.

Confirm that you have a backup, and then click Next.

What changes are made to my server?

4. Select the *I have a backup and am ready to proceed* check box and click *Next*. The Preparing The Source Server For Migration page appears and displays the tool's progress as it updates the schema. When the schema update process is complete, click *Next*.



Windows Small Business Server 2011 Standard Migration Preparation Tool

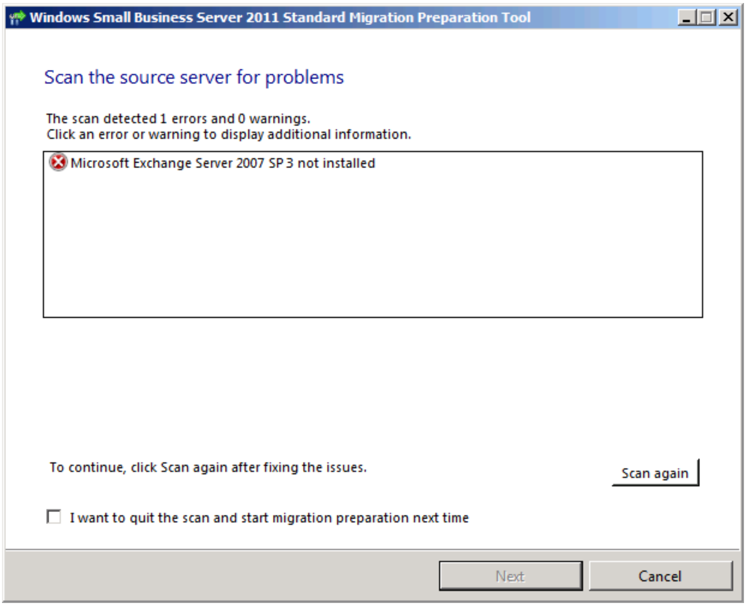
Preparing the source server for migration

Please wait while we...

Update the schema

NOTE **In addition to updating the schema, the tool also modifies the permissions to enable the migration to Windows SBS 2011 to occur, converts Exchange Server from mixed mode to native mode, and sets a time limit during which the Windows SBS network can have two domain controllers. Once you have completed the migration, your original server can function as a domain controller for up to 21 days before you must demote it.**

5. Consult the Scan The Source Server For Problems page that appears. If the tool detects any problems preventing the preparation of the server, it lists them on the page, and provides you with the options to repeat the scan or quit the tool while you correct the problems. If no problems are listed, click *Next*.


Windows Small Business Server 2011 Standard Migration Preparation Tool

Scan the source server for problems

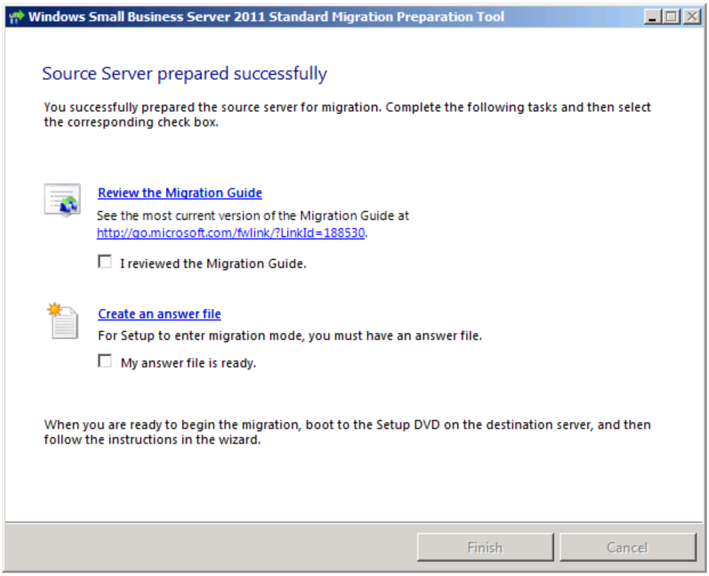
The scan detected 1 errors and 0 warnings.
Click an error or warning to display additional information.

Microsoft Exchange Server 2007 SP 3 not installed

To continue, click Scan again after fixing the issues.

□ I want to quit the scan and start migration preparation next time

6. The tool prepares the server and displays the Source Server Prepared Successfully page. This page provides links to the Windows SBS Migration Guide document on the Internet and to the Windows Small Business Server 2011 Answer File Tool.



Windows Small Business Server 2011 Standard Migration Preparation Tool

Source Server prepared successfully

You successfully prepared the source server for migration. Complete the following tasks and then select the corresponding check box.

Review the Migration Guide

See the most current version of the Migration Guide at http://go.microsoft.com/fwlink/?LinkId=188530.

□ I reviewed the Migration Guide.

Create an answer file

For Setup to enter migration mode, you must have an answer file.

□ My answer file is ready.

When you are ready to begin the migration, boot to the Setup DVD on the destination server, and then follow the instructions in the wizard.

CAUTION **The changes made to the computer running Windows Server 2003 R2 by the Migration Preparation Tool at this time are permanent and irrevocable. The only way to return to your previous server configuration is to perform a full restore from a system backup.**

7. Select the *I reviewed the Migration Guide* and *My answer file is ready* check boxes and click *Finish*. The migration tool closes.

NOTE **If desired, you can click *Create an answer file* to run the Windows Small Business Server 2008 Answer File Tool at this time. However, you can also choose to create the answer file at a later time, using any other computer running Windows. See the next section for instructions on running the tool and creating an answer file.**

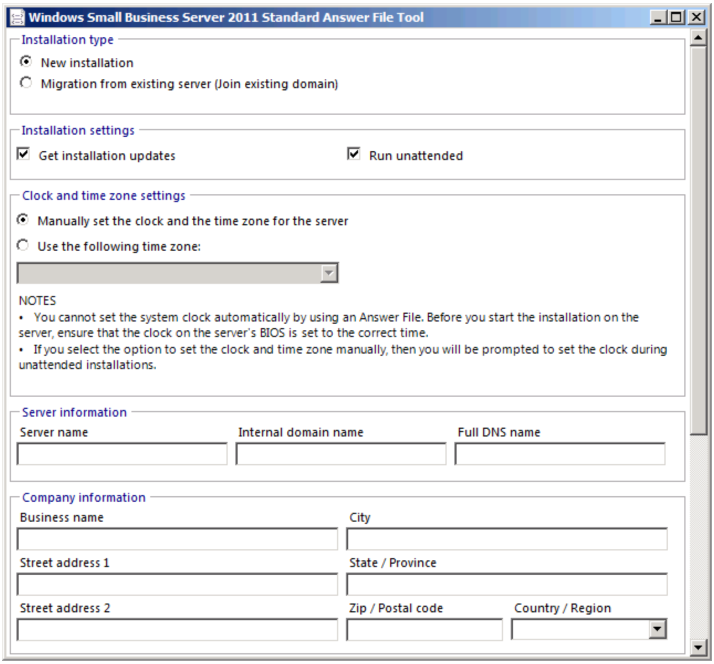
Creating an Answer File

An *answer file* is a script containing responses to the prompts generated by the Windows SBS 2011 Setup program during the operating system installation. The use of an answer file is optional in a clean Windows SBS 2011 installation, but it is required for a migration.

Although the Migration Preparation Tool enables you to run the Windows Small Business Server 2011 Answer File Tool right on your source server, you do not have to run it there, nor do you have to run it immediately after preparing the source server for migration. You can run the Answer File Tool from any computer running Windows at any time.

To create a migration answer file, use this procedure:

1. Insert Windows SBS 2011 Disk 1 into the computer's DVD-ROM drive. The Windows Small Business Server 2011 screen appears.
2. Click *Create an answer file*. The Windows Small Business Server 2011 Answer File Tool appears.



Windows Small Business Server 2011 Standard Answer File Tool

Installation type

● New installation

○ Migration from existing server (Join existing domain)

Installation settings

☑ Get installation updates

☑ Run unattended

Clock and time zone settings

● Manually set the clock and the time zone for the server

○ Use the following time zone:

NOTES

- You cannot set the system clock automatically by using an Answer File. Before you start the installation on the server, ensure that the clock on the server's BIOS is set to the correct time.
- If you select the option to set the clock and time zone manually, then you will be prompted to set the clock during unattended installations.

Server information

Server name

Internal domain name

Full DNS name

Company information

Business name

City

Street address 1

State / Province

Street address 2

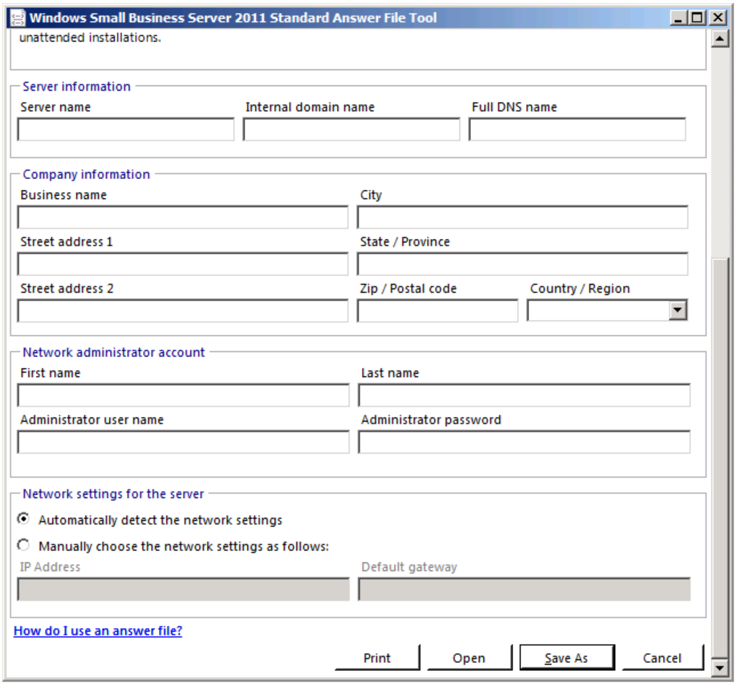
Zip / Postal code

Country / Region

3. In the *Installation type* box, select the *Migration from existing server (Join existing domain)* check box.
4. Fill out the fields in each of the following sections of the Answer File Tool:
   - **Installation settings** Specifies whether the new server should download the latest installation updates from the Microsoft Updates website during the setup process and whether the setup program should perform an unattended installation. In an unattended installation, the setup program does not display the options for which it finds settings in the answer file; if you leave this check box cleared, all the options appear during the installation, with the settings from the answer file preloaded for the installer's approval.
   - **Clock and time zone settings** Enables you to specify a time zone for the new server. You cannot modify the actual system clock time using an answer file, so if you select the Manually set the clock and the time zone for the server option, you must set the clock in the system BIOS before beginning the new server installation.

- **Company information** Contains the same name and address fields as the Company Information page in the Install Windows Wizard.

5. Scroll down to see the rest of the dialog box, and fill out the fields in each of the remaining sections:



Windows Small Business Server 2011 Standard Answer File Tool

unattended installations.

Server information

Server name | Internal domain name | Full DNS name

Company information

Business name | City

Street address 1 | State / Province

Street address 2 | Zip / Postal code | Country / Region

Network administrator account

First name | Last name

Administrator user name | Administrator password

Network settings for the server

● Automatically detect the network settings

○ Manually choose the network settings as follows:

IP Address | Default gateway

How do I use an answer file?

- **Source (existing) server information** Contains fields in which you specify information about your existing server running Windows SBS and your domain, including the server and domain names, the computer's IP Address and Default Gateway settings, and the name and password for an administrative account.
- **Destination (new) server information** Contains fields in which you specify the name and IP address values you want to assign to the new server on which you will install Windows SBS 2011. When performing a migration, the name that you specify for your new server must be unique on your network. You cannot use the same name for your source server and your new one.

6. Click *Save as*. The *Save as* combo box appears. Save the answer file to the root of a USB flash drive or floppy disk, using the file name **SBSAnswerFile.xml**, and click *Save*.

7. Click *Cancel* to close the Windows Small Business Server 2011 Answer File Tool.

NOTE **The previous procedure covers the information fields you must fill out when creating an answer file for a migration to Windows SBS 2011. When you select the *New installation* option in the tool's Installation type section, the program replaces the migration-specific sections—*Source (existing) server information* and *Destination (new) server information*—with three new sections:**

- **Server information** Enables you to specify server name and internal domain name values for the new server installation. There is also a Full DNS name text box, in which you can specify a name for your AD DS domain with a suffix other than local.
- **Network administrator account** Contains the same fields as the Add A Network Administrator Account page, which the setup program uses to create an administrative account on the new server running Windows SBS 2011.
- **Network settings for the server** Enables you to specify whether the setup program should detect a router on the network and configure the server's TCP/IP client using the router information automatically or use the IP Address and Default Gateway settings that you supply.

Apart from these field changes, the procedure for creating an answer file for the installation of a new server running Windows SBS 2011 is exactly the same.

Installing Windows SBS 2011 with an Answer File

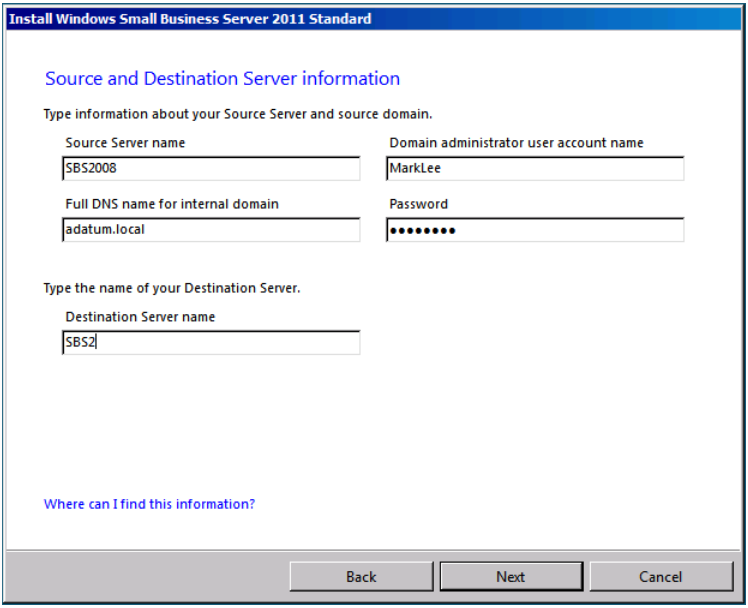
Once you have created your answer file and saved it to a removable drive, you can begin the Windows SBS 2011 installation. To perform a migration installation, use these steps:

1. Turn on the computer and insert Disk 1 from the Windows SBS 2011 package into the DVD-ROM drive.
2. Press a key to boot from the DVD if the system prompts you to do so. The computer reads from the DVD and displays the first page of the Install Windows Wizard.
3. If you plan to use language, time, and currency format, or keyboard settings other than the defaults, select your preferences from the three drop-down lists. Then click *Next*. The Install Now page appears.
4. Insert the storage device containing the answer file in the appropriate drive or slot and click *Install now*. The Please Read The License Terms page appears.
5. Select the *I accept the license terms* check box and click *Next*. The Which Type Of Installation Do You Want? page appears.
6. Click *Custom (advanced)*. The Where Do You Want To Install Windows? page appears.
7. Select or create a partition on a disk, using the *Drive options (advanced)* controls, if necessary. Then click *Next*. The Installing Windows page appears, and the setup program proceeds through the various stages of the Windows Server 2008 R2 operating system installation.

NOTE **When communicating with your source server, if the setup program detects any migration requirements that the server does not meet, it displays a Source Server Does Not Meet Minimum Requirements For Migration page that lists the issues that you must address before the migration can proceed.**

When this phase of the setup process is completed, the computer restarts, locates the answer file, and proceeds with the rest of the installation. If you configured the answer file to perform an unattended installation, the setup process continues without displaying the various configuration pages, but it restarts several times and displays the various progress indicator pages, such as Expanding And Installing Files.

If you left the *Run unattended* check box cleared, the setup program displays the individual configuration pages, such as the Source And Destination Server Information page, as shown in Figure 5-2, with the information from your answer file inserted into the various fields. You do not have to type your information into the fields again, but you do have to click *Next* to proceed from each page to the next.one.


Install Windows Small Business Server 2011 Standard

Source and Destination Server information

Type information about your Source Server and source domain.

Source Server name: SBS2008

Domain administrator user account name: MarkLee

Full DNS name for internal domain: adatum.local

Password: ••••••••

Type the name of your Destination Server.

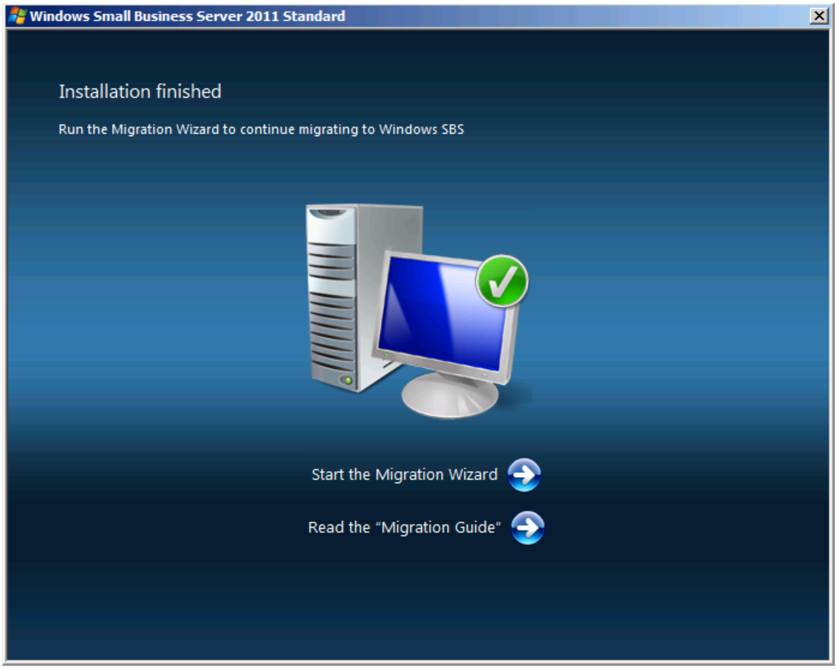
Destination Server name: SBS2

Where can I find this information?
Back
Next
Cancel

FIGURE 5-2 Optional Setup pages for attended installation.

TIP **If the screen saver appears and locks the desktop during the installation process, you can unlock it by pressing Ctrl+Alt+Del and entering the appropriate password. Depending on where in the installation process the lock occurs, you might have to unlock it using either the new server's local Administrator account, which has a blank password at this point, or the domain account for which you supplied a name and password in the answer file.**

8. When the installation is complete (which can take a great deal longer than a new Windows SBS 2011 installation), the Installation Finished page appears.

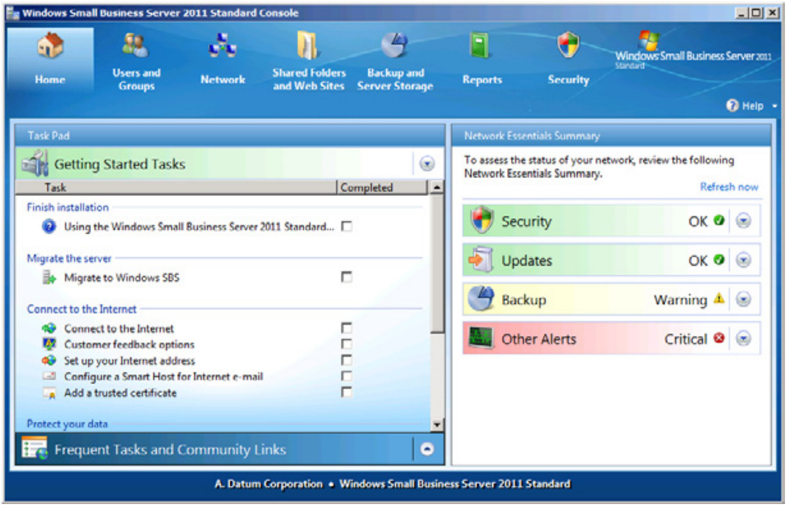


Windows Small Business Server 2011 Standard

Installation finished

Run the Migration Wizard to continue migrating to Windows SBS

The Installation Finished page prompts you to proceed by running the Migration Wizard. Clicking the *Start the Migration Wizard* link simply closes the page and starts the Windows Small Business Server 2011 Standard Console. When you perform a migration installation, the console contains an extra *Migrate to Windows SBS* entry in the *Getting started tasks* list, as shown in Figure 5-3.


Windows Small Business Server 2011 Standard Console
Home
Users and Groups
Network
Shared Folders and Web Sites
Backup and Server Storage
Reports
Security
Windows Small Business Server 2011 Standard
Help
Task Pad
Getting Started Tasks
Network Essentials Summary
Refresh now
Frequent Tasks and Community Links

Task	Completed
Finish installation	
Using the Windows Small Business Server 2011 Standard...	□
Migrate the server	
Migrate to Windows SBS	□
Connect to the Internet	
Connect to the Internet	□
Customer feedback options	□
Set up your Internet address	□
Configure a Smart Host for Internet e-mail	□
Add a trusted certificate	□
Protect your data	

To assess the status of your network, review the following Network Essentials Summary.

Security	OK ✓
Updates	OK ✓
Backup	Warning ⚠
Other Alerts	Critical ✖

A. Datum Corporation • Windows Small Business Server 2011 Standard

FIGURE 5-3 The Windows SBS Console after a migration installation.

Performing Post-Migration Tasks

When you perform a migration installation of Windows SBS 2011, your new server joins the existing AD DS domain, and the setup program promotes it to a domain controller. Normally, Windows SBS does not permit more than one domain controller on the network, but for a 21-day period after the migration installation, your new server and your old one can coexist. During that time, you must complete the migration process by performing the tasks in the Migration Wizard. Once you have completed those tasks, the new server is ready to take over as the network's sole domain controller. You can then demote your old server and remove it from the network.

The following sections examine the various tasks involved in completing a migration from an earlier version of Windows SBS.

Reconfiguring Folder Redirection

Folder redirection is a Windows feature that enables workstations in an AD DS environment to store the contents of certain folders, such as a user's Documents folder, on a server instead of the local disk. In a network environment, storing data files and other critical folders on server drives rather than local ones is generally preferable because it enables users to access their files from any computer and it enables administrators to back up the files more easily.

To use folder redirection, you configure Group Policy settings that specify where each workstation should store the contents of specific folders. These Group Policy settings are part of the AD DS database and are therefore copied to your new server as part of the Windows SBS migration process. However, although the migration installation process copies the settings themselves to the new server, it does not modify those settings; they still specify the old server's disk as the location for the redirected folders.

If you have been using folder redirection on your existing network running Windows SBS 2003 or Windows SBS 2008, you must reconfigure it by performing the following steps:

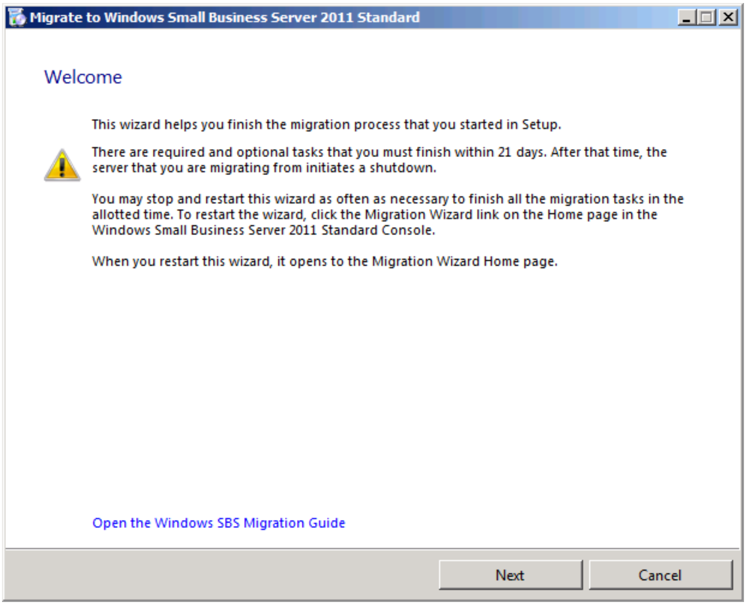
1. Modify the migrated Group Policy settings to point to your new server instead of the old one.
2. Enable folder redirection on your server running Windows SBS 2011 using the Windows SBS Console.

MORE INFO **For instructions on how to modify the migrated Group Policy settings and enable folder redirection in Windows SBS2011, see Chapter 9, "Managing Storage."**

These steps ensure that all the redirected data from your existing server running Windows SBS gets migrated to your new server running Windows SBS 2011, and that the required Group Policy settings are in place to ensure the future redirection of the desired folders.

Running the Migration Wizard

Clicking the *Migrate to Windows SBS* link in the Windows SBS Console starts the Migrate To Windows Small Business Server 2011 Wizard, as shown in Figure 5-4, which guides you through a series of tasks that completes the migration process.



Welcome

This wizard helps you finish the migration process that you started in Setup.

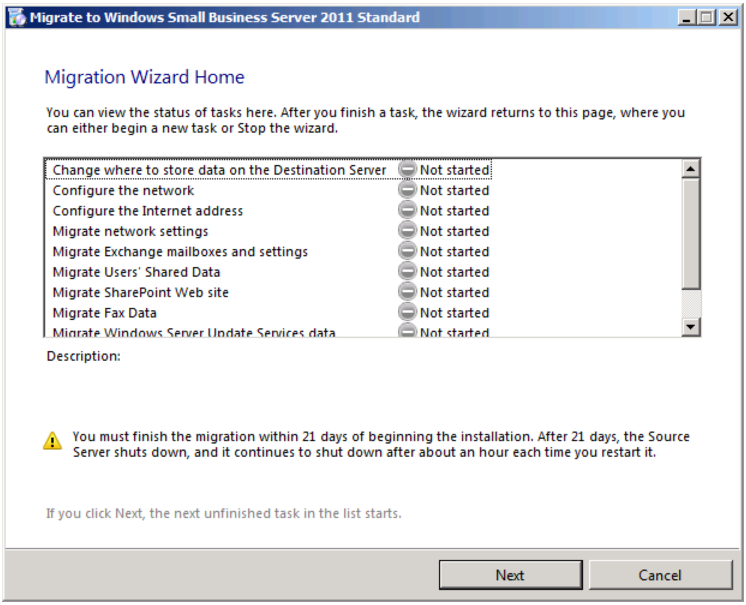
There are required and optional tasks that you must finish within 21 days. After that time, the server that you are migrating from initiates a shutdown.

You may stop and restart this wizard as often as necessary to finish all the migration tasks in the allotted time. To restart the wizard, click the Migration Wizard link on the Home page in the Windows Small Business Server 2011 Standard Console.

When you restart this wizard, it opens to the Migration Wizard Home page.

FIGURE 5-4 The Migrate To Windows Small Business Server 2011 Wizard.

When you click *Next* to bypass the Welcome page, the Migration Wizard Home page appears, as shown in Figure 5-5. The Migrate To Windows Small Business Server 2011 Wizard is essentially a shell that provides access to information and links to other wizards, and tracks your progress through the list of tasks. Some of the tasks are optional, and others are required. You must complete the tasks in the order given, although you do not have to perform them all in one session. As mentioned previously, you have 21 days to work your way through the list, skipping optional tasks, if desired, and completing the required ones.



Migration Wizard Home

You can view the status of tasks here. After you finish a task, the wizard returns to this page, where you can either begin a new task or Stop the wizard.

Change where to store data on the Destination Server	Not started
Configure the network	Not started
Configure the Internet address	Not started
Migrate network settings	Not started
Migrate Exchange mailboxes and settings	Not started
Migrate Users' Shared Data	Not started
Migrate SharePoint Web site	Not started
Migrate Fax Data	Not started
Migrate Windows Server Update Services data	Not started

Description:

You must finish the migration within 21 days of beginning the installation. After 21 days, the Source Server shuts down, and it continues to shut down after about an hour each time you restart it.

If you click Next, the next unfinished task in the list starts.

FIGURE 5-5 The Migration Wizard Home page in the Migrate To Windows Small Business Server 2011 Wizard.

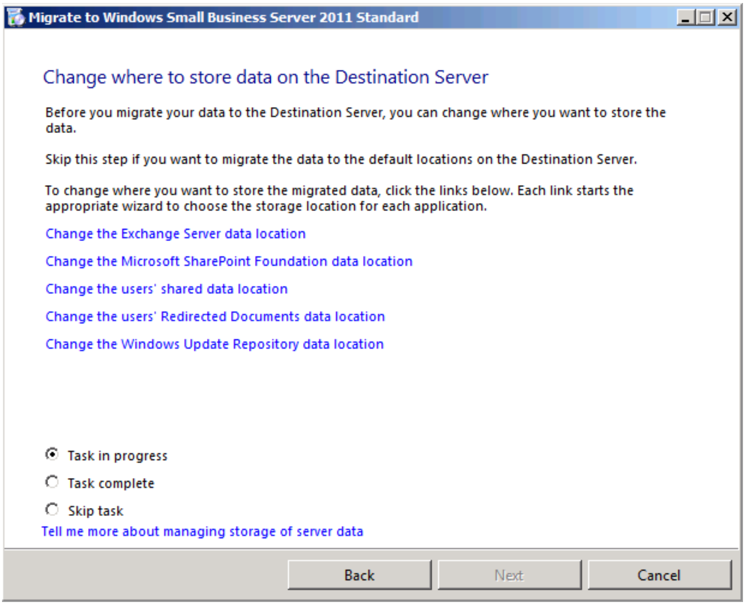
As you access each task in the list, an initial wizard page appears that explains what you must do and provides links to help pages, other wizards, or both. This page also contains option buttons that enable you to specify the current status of the task: *Task in progress*, *Task complete*, or *Skip task* (for optional procedures). As you complete each task, you designate it as such, and the wizard allows you to proceed to the next one. You can cancel out of the wizard at any time, and your status indicators remain in place, so that the next time you start the wizard, you resume where you left off.

The following sections examine the various tasks in the Migrate To Windows Small Business Server 2011 Wizard.

Change Where to Store Data on the Destination Server Page

The optional Change Where to Store Data on the Destination Server task enables you to specify alternatives to the default data file locations on your server. By default, Windows SBS 2011 stores all its data files on the system drive because it is likely to be the only one available during the installation process. However, if you have other hard disks on the computer, you might want to store your data files on a different drive to distribute the input/output (I/O) load among the storage devices.

When you perform the Change Where To Store Data On The Destination Server task, a page appears that contains links to individual wizards that enable you to specify locations for the various types of data files, as shown in Figure 5-6. By changing the locations before you migrate the data from your old server, you avoid having to allocate space for the data on the system drive and move it to another location later.



Change where to store data on the Destination Server

Before you migrate your data to the Destination Server, you can change where you want to store the data.

Skip this step if you want to migrate the data to the default locations on the Destination Server.

To change where you want to store the migrated data, click the links below. Each link starts the appropriate wizard to choose the storage location for each application.

Change the Exchange Server data location

Change the Microsoft SharePoint Foundation data location

Change the users' shared data location

Change the users' Redirected Documents data location

Change the Windows Update Repository data location

● Task in progress

○ Task complete

○ Skip task

Tell me more about managing storage of server data

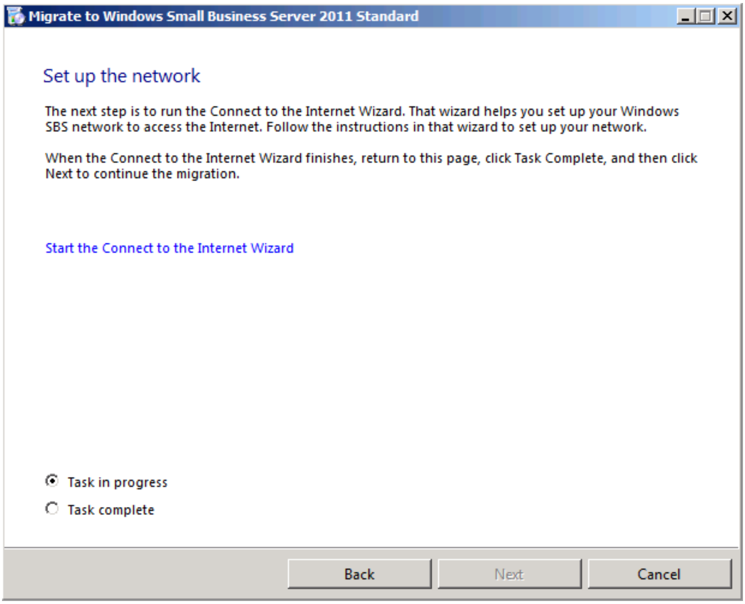
FIGURE 5-6 The Change Where To Store Data On The Destination Server page in the Migration Wizard.

To store data files on a different volume, you must create the volume before you run the individual wizards. You might have created simple volumes on other disks during the Windows SBS 2011 installation process, but if you intend to use the other volume types that Windows SBS 2011 supports (such as striped, spanned, or RAID-5), or if you intend to use a third-party redundant array of independent disks (RAID) solution, you must create the volumes now by using the Disk Management snap-in for the Microsoft Management Console (MMC) or some other tool.

MORE INFO **For more information on creating and working with disk volumes, see Chapter 7, "Managing Disks."**

Set up the Network

The Configure the Network task displays a page, shown in Figure 5-7, containing a link to the same Connect To The Internet Wizard that you can access from the *Getting started tasks* list. As in a new Windows SBS 2011 installation, you must run this wizard to configure your server's TCP/IP client and DHCP Server. As in a clean Windows SBS installation, you must complete this task before you can proceed to the next one.



Migrate to Windows Small Business Server 2011 Standard

Set up the network

The next step is to run the Connect to the Internet Wizard. That wizard helps you set up your Windows SBS network to access the Internet. Follow the instructions in that wizard to set up your network.

When the Connect to the Internet Wizard finishes, return to this page, click Task Complete, and then click Next to continue the migration.

Start the Connect to the Internet Wizard

● Task in progress

○ Task complete

FIGURE 5-7 The Set Up The Network page in the Migration Wizard.

> ***MORE INFO*** **For information on running the Connect To The Internet Wizard, see the section entitled "Connecting to the Internet," in Chapter 4, "Getting Started."**

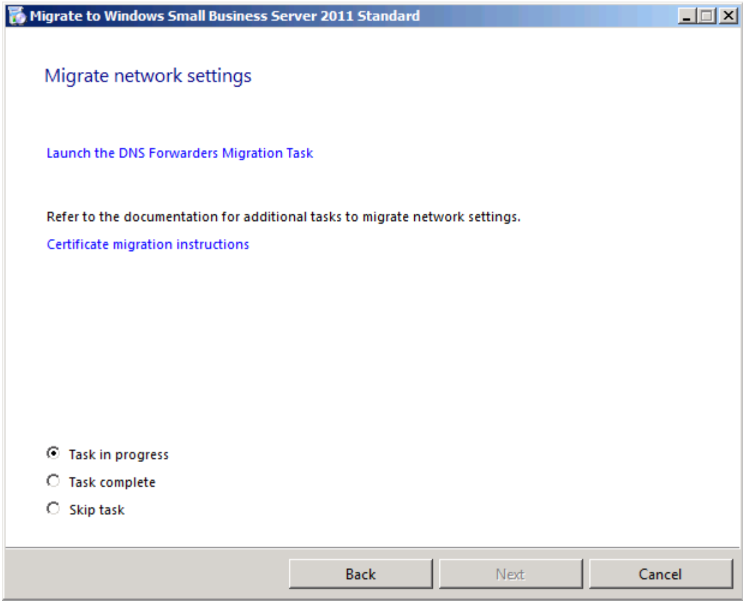
Configure the Internet Address

Starting the Configure The Internet Address task displays a page that includes a link to the same Internet Address Management Wizard discussed in Chapter 4. The page also has a link to a help page providing information on how to distribute the server's self-signed certificates to remote users.

> ***MORE INFO*** **For information on running the Internet Address Management Wizard, see the section entitled "Set up Your Internet Address," in Chapter 4.**

Migrate Network Settings

The Migrate Network Settings task displays a page, shown in Figure 5-8, from which you can migrate DNS forwarder settings from your old server running Windows SBS to your new one and display information about migrating certificates. Both of these tasks are optional, depending on whether you have configured the DNS server on your existing network to use forwarders and whether you have certificates you need to migrate.



Migrate network settings

Launch the DNS Forwarders Migration Task

Refer to the documentation for additional tasks to migrate network settings.

Certificate migration instructions

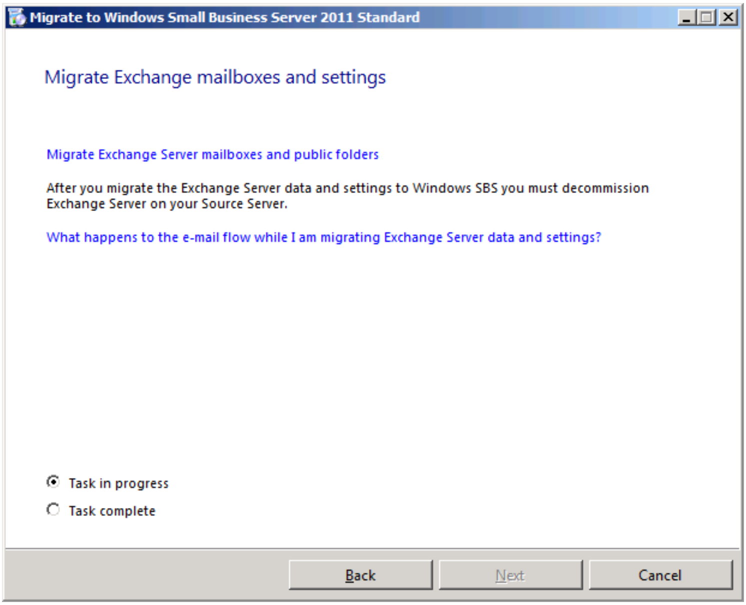
● Task in progress
○ Task complete
○ Skip task

FIGURE 5-8 The Migrate Network Settings page in the Migration Wizard.

A *forwarder* is a DNS server that receives name resolution requests from other DNS servers, usually on another network, and takes responsibility for completing the entire name resolution process before returning a response to the original server. For example, you might want to configure your DNS Server service to forward requests to your ISP's DNS server. This can reduce the amount of your Internet bandwidth consumed by DNS traffic. If you have configured your existing Windows SBS server to use DNS forwarders, clicking the *Launch the DNS forwarders migration task* link transfers those settings to your new server running Windows SBS 2011.

Migrate Exchange Mailboxes and Settings

The required Migrate Exchange Mailboxes and Settings task migrates all the Exchange Server mail stores and public folders from your source server to your new server running Windows SBS 2011. Depending on how many users you have on your network and how much mail they have stored, this procedure can take a long time. Clicking the *Migrate Exchange Server mailboxes and public folders* link on the Migrate Exchange Mailboxes And Settings page, shown in Figure 5-9, displays a web page containing instructions for migrating the various Exchange Server elements.



Migrate Exchange mailboxes and settings

Migrate Exchange Server mailboxes and public folders

After you migrate the Exchange Server data and settings to Windows SBS you must decommission Exchange Server on your Source Server.

What happens to the e-mail flow while I am migrating Exchange Server data and settings?

● Task in progress

○ Task complete

FIGURE 5-9 The Migrate Exchange Mailboxes And Settings page in the Migration Wizard.

> ***MORE INFO*** **For more information on migrating Exchange Server elements, see Chapter 15, "Administering Email."**

Migrate Users' Shared Data

Windows SBS 2011 provides no wizard or other automated mechanism for migrating the contents of users' shared folders from the old server to the new one. The Migrate Users' Shared Data page provides a link to a help screen that describes the procedures by which you can complete the following basic steps manually:

1. On your new server running Windows SBS 2011, create and share folders corresponding to the shared folders on your source server.
2. Note the permissions on the source server's shared folders and duplicate them on the new shared folders that you created.
3. Copy the files in the shared folders on your source server to the shared folders you created on your new server.

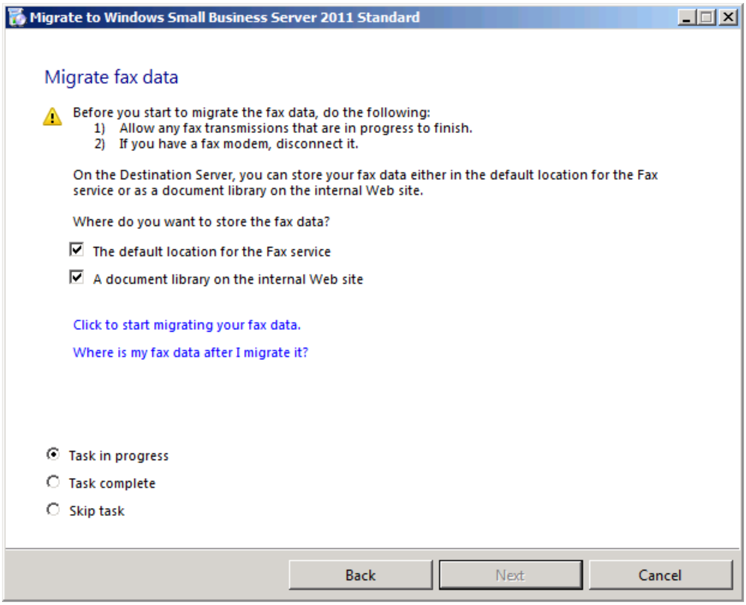
> ***MORE INFO*** **For more information on creating shares and managing permissions, see Chapter 8, "Working with Permissions," and Chapter 9.**

Migrate SharePoint Website

Migrating your existing SharePoint website and its database is a complex procedure that is described on a help screen that appears when you click the link on the Migrate Your Internal Web Site page. For more information on completing this process, see Chapter 17, "Working with SharePoint."

Migrate Fax Data

If you have the Windows SBS Fax service installed and running on your server, the Migrate Fax Data page, shown in Figure 5-10, enables you to transfer the existing fax data from your old server to your new one. You can transfer the data to the default folders for the Fax service or to your SharePoint database.



Migrate to Windows Small Business Server 2011 Standard

Migrate fax data

Before you start to migrate the fax data, do the following:
1) Allow any fax transmissions that are in progress to finish.
2) If you have a fax modem, disconnect it.

On the Destination Server, you can store your fax data either in the default location for the Fax service or as a document library on the internal Web site.

Where do you want to store the fax data?

☑ The default location for the Fax service

☑ A document library on the internal Web site

Click to start migrating your fax data.

Where is my fax data after I migrate it?

● Task in progress
○ Task complete
○ Skip task

FIGURE 5-10 The Migrate Fax Data page in the Migrate To Windows Small Business Server 2011 Wizard.

To migrate your fax data, wait for any fax transmissions currently in progress to finish and unplug your fax modem or modems. Then select the *Click to start migrating your fax data* link to begin the transfer.

Migrate Windows Server Update Services Data

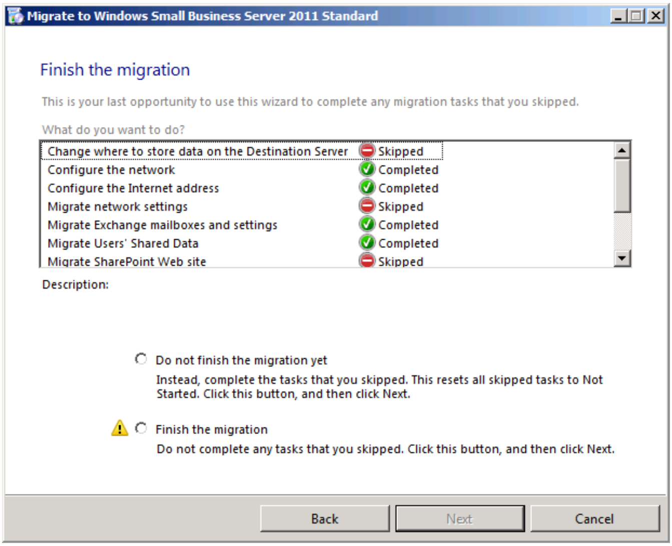
Migrating Windows Server Update Services (WSUS) data and settings is an optional task, because the service on your new server running Windows SBS 2011 will eventually reach the same level of synchronicity as your old server, assuming that you use the same WSUS configuration and Group Policy settings. The server will download all the same updates, create the same computer group memberships, and perform all the same automatic approvals.

If, however, you have devoted a lot of effort to creating group memberships and approving updates manually, you can migrate your WSUS data to the new server. The Migrate Windows Server Update Services Data page provides a link to a help page that describes the procedure for exporting your software updates and metadata from your source server and importing them into the destination server.

> ***MORE INFO*** **For more information on exporting and importing WSUS data and metadata, see Chapter 11, "Deploying Updates."**

Finish Migration

The final task in the Migrate To Windows Small Business Server 2011 Wizard first gives you an opportunity to return to any of the previous tasks you have skipped, as shown in Figure 5-11. If you select the *Finish the migration* option or if all the previous tasks show a status of Completed, The Finish The Migration page appears, which leads you through the process of demoting your old server so that it no longer functions as an AD DS domain controller.



Finish the migration

This is your last opportunity to use this wizard to complete any migration tasks that you skipped.

What do you want to do?

Change where to store data on the Destination Server	⛔ Skipped
Configure the network	✓ Completed
Configure the Internet address	✓ Completed
Migrate network settings	⛔ Skipped
Migrate Exchange mailboxes and settings	✓ Completed
Migrate Users' Shared Data	✓ Completed
Migrate SharePoint Web site	⛔ Skipped

Description:

○ Do not finish the migration yet

Instead, complete the tasks that you skipped. This resets all skipped tasks to Not Started. Click this button, and then click Next.

⚠ ○ Finish the migration

Do not complete any tasks that you skipped. Click this button, and then click Next.

FIGURE 5-11 The Finish The Migration page in the Migrate To Windows Small Business Server 2011 Wizard.

CAUTION **Before you demote the server running Windows SBS 2003 or Windows SBS 2008, you must uninstall the old version of Exchange Server using Control panel to remove all vestiges of it from the AD DS database.**

To complete the migration and remove the source server from the network, you must complete the following tasks:

1. Uninstall Exchange Server.
2. Remove Active Directory Certificate Services.
3. Disconnect printers from the source server.
4. Demote the source server.
5. Remove the source server from the domain.
6. Edit the Software Updates Group Policy object (GPO).

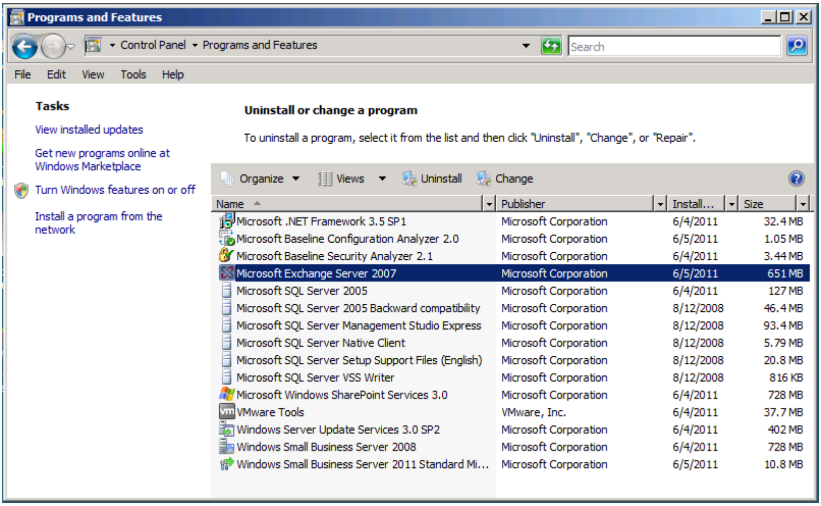
These tasks are covered in the following sections.

NOTE **Although you are removing the old server from your network, you cannot simply shut it down or reformat its drives. The AD DS database that you migrated to your new server running Windows SBS 2011 still contains references to the old server, and you must remove them by uninstalling Exchange Server and demoting the old server before you can physically remove it from the network.**

UNINSTALLING EXCHANGE SERVER

Now that you have migrated all your Exchange Server data from the source server to your new destination server, you no longer need the old Exchange Server installation. However, you still want to uninstall the old version of Exchange Server from the source server to remove all vestiges of it from AD DS before you demote the source server.

If you are running Windows SBS 2008 on your source server, you must use the Programs And Features Control panel to remove Exchange Server 2007, as shown in Figure 5-12. If you are running Windows SBS 2003 on your old server, you must use the Add Or Remove Programs Control panel to remove Exchange Server 2003.


Programs and Features
Control Panel ▸ Programs and Features
Search
File
Edit
View
Tools
Help
Tasks
View installed updates
Get new programs online at Windows Marketplace
Turn Windows features on or off
Install a program from the network
Organize
Views
Uninstall
Change

Uninstall or change a program

To uninstall a program, select it from the list and then click "Uninstall", "Change", or "Repair".

Name	Publisher	Install...	Size
Microsoft .NET Framework 3.5 SP1	Microsoft Corporation	6/4/2011	32.4 MB
Microsoft Baseline Configuration Analyzer 2.0	Microsoft Corporation	6/5/2011	1.05 MB
Microsoft Baseline Security Analyzer 2.1	Microsoft Corporation	6/4/2011	3.44 MB
Microsoft Exchange Server 2007	Microsoft Corporation	6/5/2011	651 MB
Microsoft SQL Server 2005	Microsoft Corporation	6/4/2011	127 MB
Microsoft SQL Server 2005 Backward compatibility	Microsoft Corporation	8/12/2008	46.4 MB
Microsoft SQL Server Management Studio Express	Microsoft Corporation	8/12/2008	93.4 MB
Microsoft SQL Server Native Client	Microsoft Corporation	8/12/2008	5.79 MB
Microsoft SQL Server Setup Support Files (English)	Microsoft Corporation	8/12/2008	20.8 MB
Microsoft SQL Server VSS Writer	Microsoft Corporation	8/12/2008	816 KB
Microsoft Windows SharePoint Services 3.0	Microsoft Corporation	6/4/2011	728 MB
VMware Tools	VMware, Inc.	6/4/2011	37.7 MB
Windows Server Update Services 3.0 SP2	Microsoft Corporation	6/4/2011	402 MB
Windows Small Business Server 2008	Microsoft Corporation	6/4/2011	728 MB
Windows Small Business Server 2011 Standard Mi...	Microsoft Corporation	6/5/2011	10.8 MB

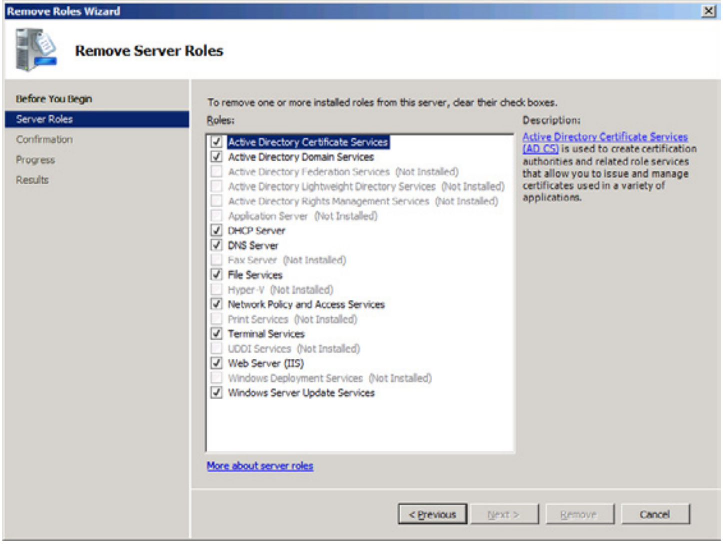
FIGURE 5-12 The Windows SBS 2008 Programs And Features Control panel .

REMOVING ACTIVE DIRECTORY CERTIFICATE SERVICES

If your source server is running Windows SBS 2008, you must remove Active Directory Certificate Services before the server will allow you to demote the domain controller.

To remove Active Directory Certificate Services, use the following procedure:

1. Log on to your server running Windows SBS 2008, using an account that is a member of the Domain Admins and Enterprise Admins groups.
2. Click *Start*. Then click *Administrative Tools* > *Server Manager*. A User Account Control message box appears.
3. Click *Continue*. The Server Manager Console appears.
4. Scroll down to the *Roles summary* section and click *Remove roles*. The Remove Roles Wizard appears.
5. Click *Next* to bypass the Before You Begin page. The Remove Server Roles page appears.



To remove one or more installed roles from this server, clear their check boxes.

Roles:

- ☑ Active Directory Certificate Services
- ☑ Active Directory Domain Services
- □ Active Directory Federation Services (Not Installed)
- □ Active Directory Lightweight Directory Services (Not Installed)
- □ Active Directory Rights Management Services (Not Installed)
- □ Application Server (Not Installed)
- ☑ DHCP Server
- ☑ DNS Server
- □ Fax Server (Not Installed)
- ☑ File Services
- □ Hyper-V (Not Installed)
- ☑ Network Policy and Access Services
- □ Print Services (Not Installed)
- ☑ Terminal Services
- □ UDDI Services (Not Installed)
- ☑ Web Server (IIS)
- □ Windows Deployment Services (Not Installed)
- ☑ Windows Server Update Services

More about server roles

Description:

Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.

6. Clear the *Active Directory Certificate Services* check box and click *Next*. The Confirm Removal Selections page appears.
7. Click *Remove*. The wizard removes the role.
8. Click *Close*. The wizard closes.

DISCONNECTING PRINTERS

If you have any printers that are physically connected to your source server, disconnect them and make sure that any AD DS objects for those printers are removed from the directory.

DEMOTING THE SOURCE SERVER

To demote your domain controller running Windows SBS 2003 or Windows SBS 2008, use the following procedure:

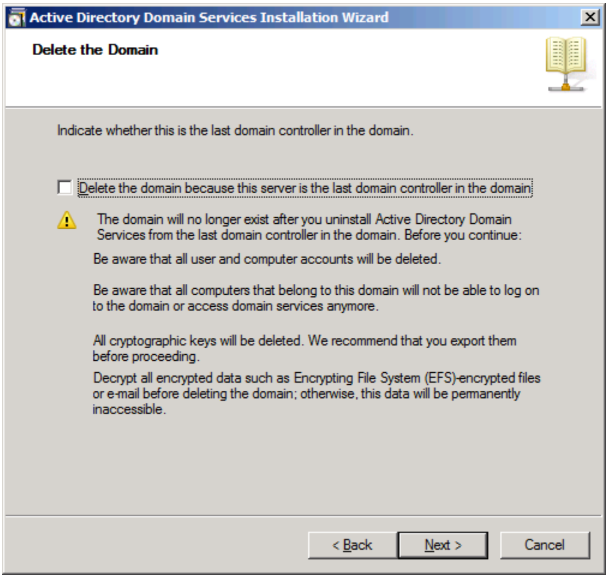
1. Log on to your server using an account with network Administrator privileges.
2. Click *Start*, and then click *Run*. The Run dialog box appears.
3. In the *Open* text box, type **dcpromo** and click *OK*. A User Account Control message box appears.
4. Click *Continue*. The Active Directory Domain Services Installation Wizard appears.

NOTE If you are demoting a server running Windows SBS 2003, there is no User Account Control message box, and the procedure launches the nominally different Active Directory Installation Wizard.

5. Click *Next* to bypass the Welcome page. An Active Directory Domain Services Installation Wizard message box appears, warning about the server's Global Catalog status.

   NOTE **Because your new server is functioning as a Global Catalog server, you can safely demote the old server, despite this warning.**

6. Click *OK*. The Delete The Domain page appears.



Active Directory Domain Services Installation Wizard

Delete the Domain

Indicate whether this is the last domain controller in the domain.

□ Delete the domain because this server is the last domain controller in the domain

The domain will no longer exist after you uninstall Active Directory Domain Services from the last domain controller in the domain. Before you continue:

Be aware that all user and computer accounts will be deleted.

Be aware that all computers that belong to this domain will not be able to log on to the domain or access domain services anymore.

All cryptographic keys will be deleted. We recommend that you export them before proceeding.

Decrypt all encrypted data such as Encrypting File System (EFS)-encrypted files or e-mail before deleting the domain; otherwise, this data will be permanently inaccessible.

7. Leave the *Delete the domain because the server is the last domain controller in the domain* check box cleared and click *Next*. The Remove DNS Delegation page appears.
8. Click *Next* to accept the default setting, and then click *Next*. A Windows Security message box appears.
9. Type credentials with network Administrator privileges in the *User name* and *password* text boxes, and then click *OK*. The Administrator Password page appears.
10. Type a strong password in the *Password* and *confirm password* text boxes. Then click *Next*. The Summary page appears.
11. Click *Next*. The wizard demotes the server and the *Completing the Active Directory* Domain Services Installation Wizard page appears.
12. Click *Finish*. An Active Directory Domain Services Installation Wizard message box appears, prompting you to restart the computer.
13. Click *Restart now*. The computer restarts.

REMOVING THE SOURCE SERVER FROM THE DOMAIN

Your old Windows SBS server is now no longer a domain controller; it is a member server in your domain. To remove the server from the domain completely, you must make it a member of a workgroup using the following procedure:

1. Log on to your old server running Windows SBS using an account with network Administrator privileges.
2. Click *Start*. Then click *Control panel*. The Control panel window appears.
3. Double-click *System*. The System Control panel appears.
4. Click *Change settings*. A User Account Control message box appears.
5. Click *Continue*. The System Properties sheet appears.

   NOTE **If you are working on a server running Windows SBS 2003, there is no User Account Control message box, and the procedure to reach the System Properties sheet is slightly different than it is in Windows SBS 2008.**

6. Select the *Computer name* tab, and then click *Change*. The Computer Name/Domain Changes dialog box appears.
7. Select the *Workgroup* option, type a workgroup name in the text box, and then click *OK*.
8. A Computer Name/Domain Changes dialog box appears, prompting you for credentials to remove the computer from the domain.
9. In the *User name* and *password* text boxes, type the credentials for an administrative account in your domain. Then click *OK*.
10. A message box appears, welcoming you to the workgroup that you specified.
11. Click *OK*. A message box appears, informing you that you must restart the computer for the changes to take effect.
12. Click *OK*.
13. Click *Close* to close the System Properties sheet. A Windows message box appears, prompting you to restart the computer.
14. Click *Restart now*. The computer restarts.

Finally, you must remove the computer object from the AD DS database. Demoting the old server from a domain controller to a member computer moves the computer object to a different organizational unit (OU), but removing the old server from the domain does not delete the computer object from the AD DS directory.

To delete the computer object manually, use the following procedure:

1. Log on to your new server running Windows SBS 2011 using an account with network Administrator privileges.

2. Click *Start*. Then click *Administrative Tools > Active Directory Users and Computers*. The Active Directory Users And Computers Console appears.
3. Browse to the *domain.Local\MyBusiness\Computers\SBSComputers* container.
4. Delete the object representing your computer running the earlier version of Windows SBS.
5. Close the Active Directory Users And Computers Console.

EDITING THE SOFTWARE UPDATES GPO

The computer that was your old Windows SBS domain controller is now gone from the domain, but there is still one artifact left that you should remove. The old server still exists in a WSUS GPO, which you can remove using the following procedure:

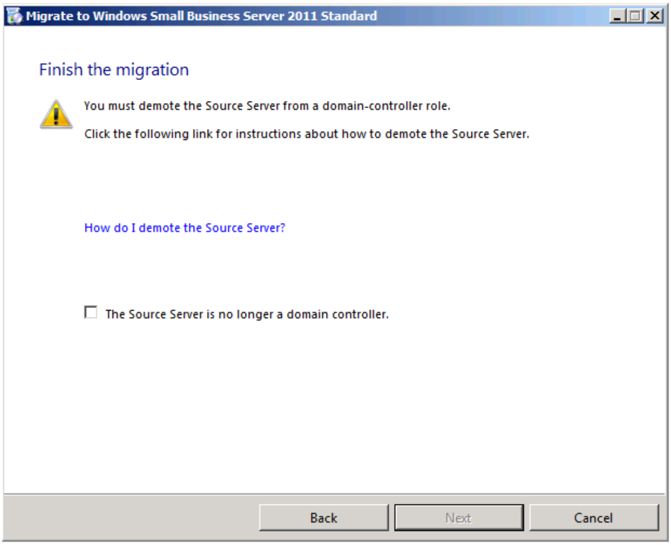
1. Log on to your new server running Windows SBS 2011 using an account with network Administrator privileges.
2. Click *Start*. Then click *Administrative Tools > Group Policy Management*. The Group Policy Management Console appears.
3. Browse to the GPOs container in your domain and select the *Update Services Server Computers Policy GPO*.
4. On the *Scope* tab, under *Security filtering*, locate the object identified with a security identifier (SID) beginning with S-1-5 and select it.

   NOTE **Because you have already deleted the computer object for your old server in the previous section, its SID is now unresolvable. This is why the computer does not appear by name in the Group Policy Management Console.**

5. Click *Remove*. A Group Policy Management message box appears, confirming your action.
6. Click *OK*. The object is removed.
7. Close the Group Policy Management Console.

Completing the Migration Wizard

When you have fully decommissioned your old server, return to the Finish The Migration page (see Figure 5-13), select the *The source server is no longer a domain controller* check box, and then click *Next*.



Finish the migration

You must demote the Source Server from a domain-controller role.

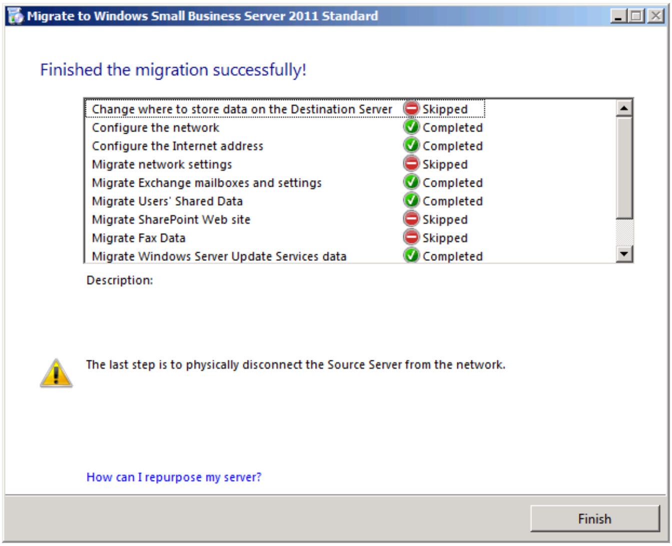
Click the following link for instructions about how to demote the Source Server.

How do I demote the Source Server?

☐ The Source Server is no longer a domain controller.

FIGURE 5-13 The Finish The Migration page of the Migrate To Windows Small Business Server 2011 Wizard.

The Finished The Migration Successfully page appears, as shown in Figure 5-14. Click *Finish* to close the wizard.



Finished the migration successfully!

Change where to store data on the Destination Server	Skipped
Configure the network	✓ Completed
Configure the Internet address	✓ Completed
Migrate network settings	Skipped
Migrate Exchange mailboxes and settings	✓ Completed
Migrate Users' Shared Data	✓ Completed
Migrate SharePoint Web site	Skipped
Migrate Fax Data	Skipped
Migrate Windows Server Update Services data	✓ Completed

Description:

The last step is to physically disconnect the Source Server from the network.

How can I repurpose my server?

FIGURE 5-14 The Finished The Migration Successfully page of the Migrate To Windows Small Business Server 2011 Wizard.

Repurposing the Migrated Server

Once you have completed the migration process, you can use the old server for another purpose, such as a computer running Microsoft SQL Server, if you purchased the Windows SBS 2011 Premium Add-On, or as a file and print server. However, it is strongly recommended that you do not use the server in its post-migration state without reinstalling an operating system, as it might be left in an unstable condition.

CHAPTER 6

Working with Users, Computers, and Groups

With your Windows Small Business Server (SBS) 2011 server installation and configuration all but complete, it is time to start thinking about the other computers on your network: the workstations and their users. To connect workstations to your Windows SBS network, you must create accounts for your users and then join the computers to your domain.

An Active Directory Primer

Active Directory Domain Services (AD DS) is a key element of the Windows SBS 2011 infrastructure, one that provides centralized authentication and authorization services for the entire network. It is important for Windows SBS administrators to understand the basic architecture of AD DS, although in most cases it is not necessary to delve into its vast complexities.

AD DS Functions

AD DS is, at its heart, a *directory service*; that is, a database that functions as a repository for information about your network. When Windows SBS network users sit down at their workstations and log on, they are logging on to the directory service, not to the individual workstations. Their user accounts and passwords are stored in AD DS, and the directory service grants them access to the network.

Two of the primary functions performed by AD DS are authentication and authorization. *Authentication* is the process by which a system verifies a user's identity. Computers can authenticate a user's identify by requiring that the user supply any or all of the following:

- Something the user knows, such as a password
- Something the user has: a possession, such as a smart card
- Something the user is: a physical attribute, such as a fingerprint

Authentication protocols, such as *Kerberos*, enable these processes to occur without endangering passwords by transmitting them over the network. *Authorization* is the process by which a system grants a user access to specific resources. Once AD DS has authenticated a user, it can grant access to network resources by associating the user's verified identity with the access control system built into the resource. For example, every file on the NTFS disks in your Windows SBS 2011 servers and workstations has a list of the users who are permitted access to that file.

Without AD DS, users would require separate accounts and passwords on every computer they need to access. Imagine how arduous your role as an administrator would be if, each time a new employee joined the company, you had to create 10 or 20 separate user accounts for the same person, on 10 or 20 different computers. Imagine having to modify 10 or 20 separate accounts each time a user is required to change his or her password (which, for security reasons, should be pretty frequently). AD DS uses one centralized user account and password for all network resources, greatly simplifying the administration process.

Domains and Domain Controllers

In AD DS, the fundamental administrative unit is the domain. An *AD DS domain* is a logical grouping of computers, users, and other network resources. By grouping elements into domains, administrators can create policies and assign them to all or part of a network at once.

AD DS is a highly flexible directory service that is sufficiently scalable to support networks of almost any size. A large enterprise network can consist of multiple domains, grouped in a hierarchical structure called a *domain tree*, and can even have multiple domain trees grouped in a structure called a *forest*. However, Windows SBS 2011 supports the use of only a single domain, which is more than sufficient to support the maximum of 75 workstations you can connect to the network.

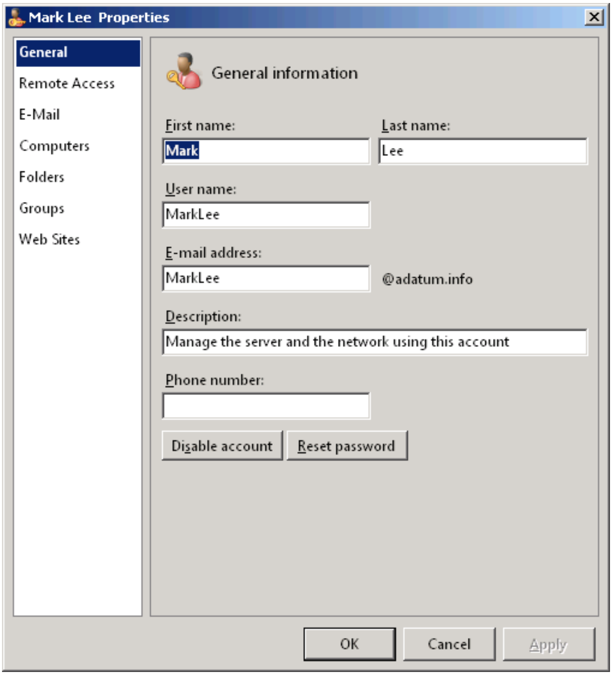
One of the most complex parts of a large-scale AD DS deployment is designing the AD DS tree structure. Administrators of large networks must often devote a great deal of time and effort to creating a domain hierarchy that adequately represents their organizations. With Windows SBS 2011, however, there is no need for this effort. All you have to do is supply a name for your domain, and the Windows SBS setup program installs AD DS, creates the domain, and configures your server to support it.

A Windows server with AD DS installed and configured is called a *domain controller*. The domain controller contains a copy of the AD DS database, as well as the various applications and services that enable AD DS to function. When a user logs on to the domain, it is the domain controller that authenticates the user's identity. When a user on a Windows SBS workstation accesses a server disk, the domain controller (which, in this case, is the same computer) authenticates the user's identity and authorizes access to the files that the user requests. Even when a user accesses resources on another workstation instead of a server, the domain controller is involved in the authentication and authorization processes. The computers on the network, therefore, require continual access to the domain controller.

Larger networks usually have multiple domain controllers for each domain, which replicate information back and forth to keep them all updated and in the same state. Windows SBS 2011, however, supports only one domain and one domain controller. This simplifies the network design and eliminates the need for complex replication systems, but it also makes the continued operation of the Windows SBS domain controller all the more critical. It is strongly recommended that you use fault-tolerance mechanisms, such as an uninterruptible power supply (UPS) and regular server backups, to prevent extended domain controller downtime.

Objects and Attributes

The AD DS database consists of *objects*, which represent specific network resources, both physical and logical. Every user, computer, and group on your network has an AD DS object that represents it. Each object consists of a set of *attributes*, which contain information about that object. For example, some of the attributes of a user object are designed to hold the individual's first and last names, address information, and password. When you open the Properties sheet for a user account, as shown in Figure 6-1, the properties that you can modify are actually attributes of the user object. Group objects contain, as an attribute, a list of the other objects that are members of the group.



First name: Mark

Last name: Lee

User name: MarkLee

E-mail address: MarkLee @adatum.info

Description: Manage the server and the network using this account

Phone number:

FIGURE 6-1 The Properties sheet for a Windows SBS 2011 user object.

The types of objects that you can create in the AD DS database, and the attributes of each object type, are specified in the *AD DS schema*. Applications can modify the schema to add object types to the AD DS implementation, or add attributes to existing object types. For example, Microsoft Exchange modifies the schema to add specialized attributes to every user object in the directory.

It is also possible for administrators to modify the schema manually, using tools provided with Windows Server 2008 R2. However, the average Windows SBS 2011 administrator should not have reason to do this.

> ***CAUTION*** **Modifying the AD DS schema is similar to modifying a Windows computer's registry, in that a minor mistake can have a profound effect on the functionality of the system. Do not make any manual changes to the schema (or to the registry, for that matter), unless you know precisely what you are doing, and why.**

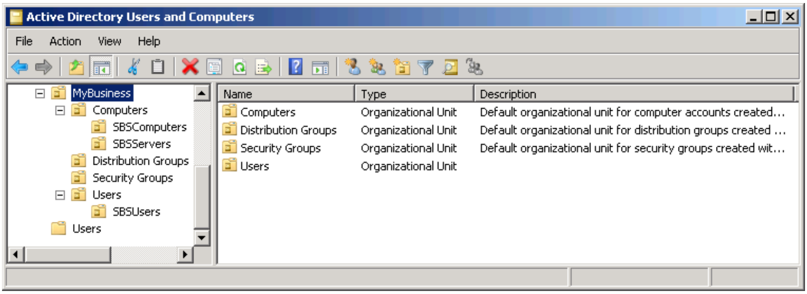
In addition to objects that represent network resources, the AD DS has objects that represent logical divisions in the network, which you can use for organizational functions. The domain is such an object, as is a forest. Within a domain, you can also create objects called *organizational units (OUs)* to subdivide the domain in various ways. Unlike domains, which you can create only by installing a new domain controller, you can create as many OUs as you want, at any time.

OUs are known as *container objects* because other objects can be subordinate to them. You can create user, group, and computer objects in an OU, or even other OUs. Objects that cannot contain other objects, such as user and computer objects, are known as *leaf objects*.

> ***NOTE*** **Four container objects appear in every domain by default: Built-in, Computers, ForeignSecurityPrincipals, and Users. These are not OUs; the name of their object type is *container*. You cannot create new objects using the container type, but you can create objects, such as OUs, that are containers (in the generic sense).**

The default domain for your Windows SBS 2011 network has a number of OUs in addition to the Domain Controllers OU found in every AD DS domain. The MyBusiness OU has four OUs beneath it, called Computers, Distribution Groups, Security Groups, and Users, as shown in Figure 6-2. The Computers OU has two subordinate OUs of its own, called SBSComputers and SBSServers, and the Users OU has a subordinate OU called SBSUsers.

> ***NOTE*** **Group objects are a special case because while they have a list of other objects that are members of the group as an attribute, they do not contain those objects in the AD DS sense. Groups are therefore not considered container objects, as domains or OUs are.**



Name	Type	Description
Computers	Organizational Unit	Default organizational unit for computer accounts created...
Distribution Groups	Organizational Unit	Default organizational unit for distribution groups created ...
Security Groups	Organizational Unit	Default organizational unit for security groups created wit...
Users	Organizational Unit	

FIGURE 6-2 The default OU hierarchy in a Windows SBS 2011 domain.

The function of these OUs is to separate the leaf objects that Windows SBS 2011 creates in your domain by their functions; users go in one OU, computers in another, and so forth. Here again, Windows SBS 2011 has made the AD DS design decisions for you. It includes specialized tools that are based on this default design. To manage AD DS user, group, and computer objects using the Windows SBS Console, the objects must be located in the appropriate OUs. You can conceivably redesign the domain hierarchy by creating your own OUs and moving the objects into them, using any organizational paradigm you want, such as the geographical locations of your company's branch offices. To do so, however, you would then have to use the standard

Windows Server 2008 R2 tools to manage them instead of the Windows SBS Console. You would also have to reconfigure the default Windows SBS 2011 Group Policy objects (GPOs), which are designed around the default OU hierarchy.

> ***CAUTION*** **It is strongly recommended that you do not modify the default AD DS hierarchy, at least at first, until you fully understand the ramifications of your actions.**

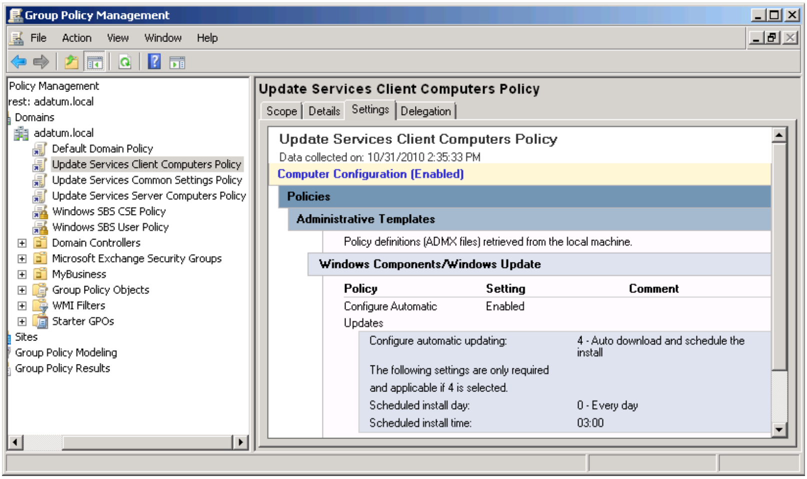
Group Policy

One of the most powerful administration tools in AD DS is Group Policy. *Group Policy* is a feature that enables you to deploy combinations of configuration settings (which are essentially registry settings) to large numbers of users or computers on an AD DS network at once.

To use Group Policy, you create a *Group Policy object (GPO)*, which is a collection of computer and/or user configuration settings packaged as a single unit. You then link the GPO to a domain, OU, or site object in AD DS. Once you do this, every leaf object in the domain, OU, or site to which you linked the GPO receives the configuration settings in it and applies them to the computer or the currently logged-in user.

> ***NOTE*** **You can link GPOs only to domain, OU, or site objects. You cannot link them to individual leaf objects (including groups, strangely enough), nor can you link them to the predefined objects that use the container object type, such as the Computers and Users objects.**

For example, you can use the Windows Update client on an individual computer to configure the system to download and install new operating system updates as they become available. Windows SBS 2011 includes Windows Server Update Services (WSUS), however, which enables your server to supply updates to the client workstations on the network. Rather than make you configure each individual workstation to download updates from the WSUS server, the Windows SBS 2011 setup program creates a GPO called Update Services Client Computers Policy, which contains Windows Update configuration settings, and links it to your domain, as shown in Figure 6-3. As a result, all the computers in the domain receive these settings and configure themselves to use WSUS for their updates.



Update Services Client Computers Policy

Data collected on: 10/31/2010 2:35:33 PM

Computer Configuration (Enabled)

Policies

Administrative Templates

Policy definitions (ADMX files) retrieved from the local machine.

Windows Components/Windows Update

Policy	Setting	Comment
Configure Automatic Updates	Enabled	

Configure automatic updating:	4 - Auto download and schedule the install
The following settings are only required and applicable if 4 is selected.	
Scheduled install day:	0 - Every day
Scheduled install time:	03:00

FIGURE 6-3 The Windows Update settings in the Update Services Client Computers Policy GPO.

Because the Update Services Client Computers Policy GPO is linked to your domain object, all the computers on your network receive its settings. One of the main reasons for creating OUs, however, is to segregate objects that you want to receive different settings. For example, Windows SBS creates separate SBSComputers and SBSServers OUs in your domain so that it can assign different GPOs to the workstations and server.

Windows SBS 2011 includes a number of GPOs with different functions, which it links to appropriate objects in the default AD DS hierarchy. This is an excellent example of good Group Policy organization. GPOs have hundreds of possible settings, and keeping track of which ones you have deployed to which locations can be difficult. Although you can conceivably create a single GPO that contains all the settings you want to deploy to certain users and computers, it is much more efficient, from an organizational standpoint, to create multiple GPOs for specific purposes.

Hierarchy and Inheritance

The use of terms such as *tree* and *leaf* in AD DS terminology should give some idea of the directory service's hierarchical architecture. AD DS is based on domains, which you can group into trees and forests, but within each domain, you can build a root-like structure using OUs. Just as in a file system, influence in a domain flows downward through the container objects to the individual leaf objects. When you link a GPO to a domain object, the settings in that GPO flow down to all the OUs in the domain and all the leaf objects in the OUs. In the same way, linking a GPO to an OU causes all the leaf objects inside to receive the settings, even objects within subordinate OUs.

You can see one example of how the design of the AD hierarchy is useful to administrators in the default Windows SBS 2011 domain. As mentioned earlier, there is a Computers OU in your domain's MyBusiness OU, and in the Computers OU, there are two more OUs: SBSComputers and SBSServers. Why use three OU levels, though, when you could simply create the SBSComputers and SBSServers OUs directly beneath the MyBusiness OU?

One reason is that adding the level containing the Computers OU enables you to apply Group Policy settings in three different ways. By linking a GPO to the SBSComputers OU or the SBSServers OU, you can apply settings to all the client computers or all the servers in the domain. However, by linking a GPO to the Computers OU, you can apply settings to all the computer objects in the domain clients and servers at once.

The downward flow of influence in an AD DS domain is not limited to Group Policy settings. AD DS has a system of permissions that define who can access particular objects and what they can do with the objects they access. The AD DS permissions system is completely independent from the other permission systems in Windows Server 2008 R2, such as NTFS and registry permissions, but it works in very much the same way. If you assign permissions to a container object, such as a domain or an OU, every object in that container inherits those permissions, including other container objects.

Using AD DS Tools

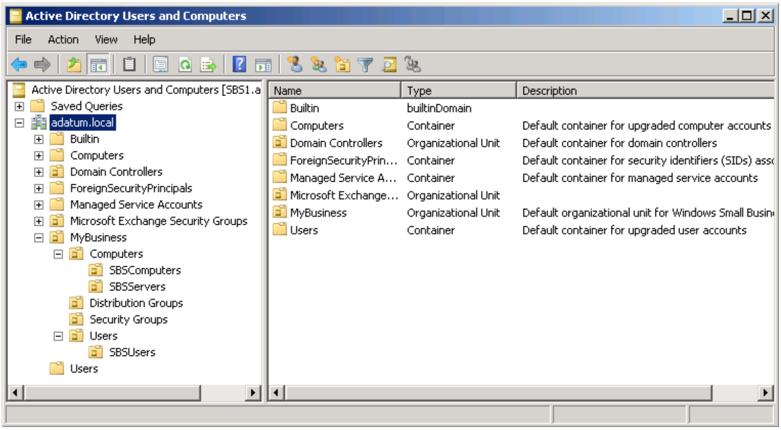
The Windows SBS Console enables you to perform many of the most common AD DS maintenance tasks, although it generally does not identify them as such. Windows SBS 2011 tries to insulate administrators from the complexities of AD DS, but when you create or manage a user or a group in the Windows SBS Console, you are actually creating an AD DS object and modifying its attributes.

Although you might want to stick to the Windows SBS Console when performing administrative tasks at first, you should also be aware of the AD DS tools included with the Windows Server 2008 R2 operating system. These tools provide more comprehensive access to the AD DS and enable you to work with AD DS objects on any Windows computer.

> ***NOTE*** **The procedures in this book use Windows SBS 2011 tools whenever possible. However, you can use the Windows Server 2008 R2 tools to perform all the same tasks.**

Using Active Directory Users and Computers

The Active Directory Users And Computers Console is the most commonly used AD DS management tool. Like most Windows Server 2008 R2 tools, it is a snap-in for the Microsoft Management Console (MMC) utility. Unlike Windows SBS Console, which displays only certain AD DS objects, Active Directory Users And Computers is based on a tree display of your entire domain, as shown in Figure 6-4.

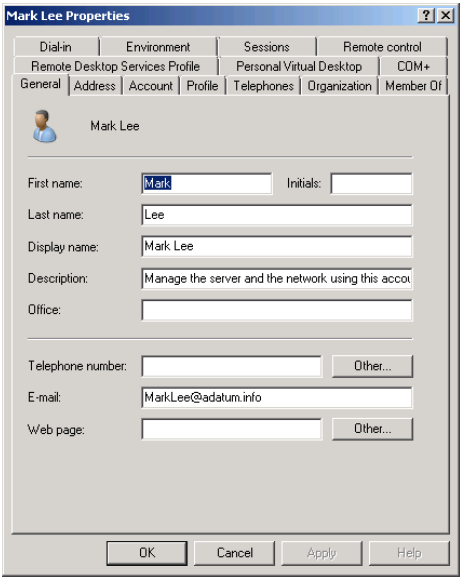


- Active Directory Users and Computers [SBS1.a
  - Saved Queries
  - adatum.local
    - Builtin
    - Computers
    - Domain Controllers
    - ForeignSecurityPrincipals
    - Managed Service Accounts
    - Microsoft Exchange Security Groups
    - MyBusiness
      - Computers
        - SBSComputers
        - SBSServers
      - Distribution Groups
      - Security Groups
      - Users
        - SBSUsers
    - Users

Name	Type	Description
Builtin	builtinDomain	
Computers	Container	Default container for upgraded computer accounts
Domain Controllers	Organizational Unit	Default container for domain controllers
ForeignSecurityPrin...	Container	Default container for security identifiers (SIDs) asso
Managed Service A...	Container	Default container for managed service accounts
Microsoft Exchange...	Organizational Unit	
MyBusiness	Organizational Unit	Default organizational unit for Windows Small Busin
Users	Container	Default container for upgraded user accounts

FIGURE 6-4 The Active Directory Users And Computers Console.

In the Active Directory Users And Computers Console, the left pane (also called the *Scope pane*) displays your domain and all the container and OU objects beneath it, using an expandable tree arrangement, just like the file system in Windows Explorer. Selecting a container or OU in the Scope pane displays all the objects it contains in the right pane (also called the *Detail pane*). Double-clicking a leaf object, such as user, computer, or group, opens the Properties sheet for the object, as shown in Figure 6-5.



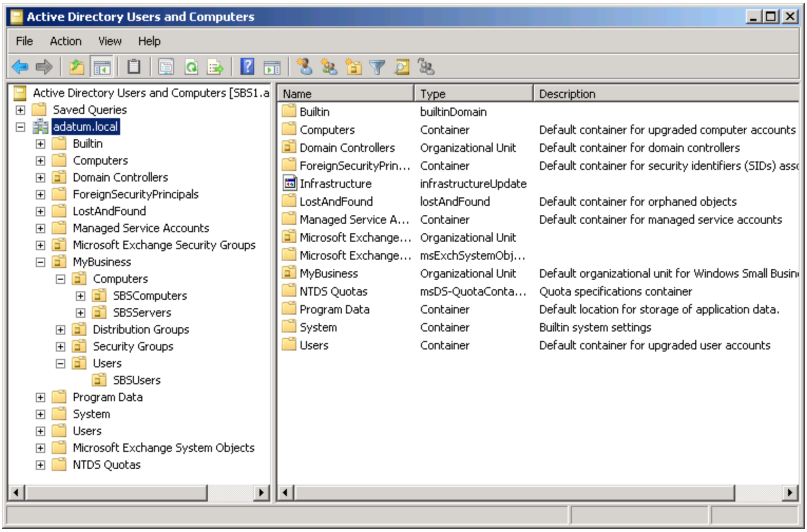
Mark Lee

First name: Mark
Initials:
Last name: Lee
Display name: Mark Lee
Description: Manage the server and the network using this accou
Office:

Telephone number:
E-mail: MarkLee@adatum.info
Web page:

FIGURE 6-5 The Properties sheet for a user object in the Active Directory Users And Computers Console.

As you can see in Figure 6-5, a user object's Properties sheet in the Active Directory Users And Computers Console contains much more information than its Windows SBS Console equivalent, and enables you to modify many more of the object's attributes. This is not the full extent of the console's capabilities, though. To see even more information about your AD DS domain, you can select *Advanced features* from the *View* menu to display additional objects, as shown in Figure 6-6. Few administrators require access to these advanced features on a regular basis, but it is good to know that they are available.

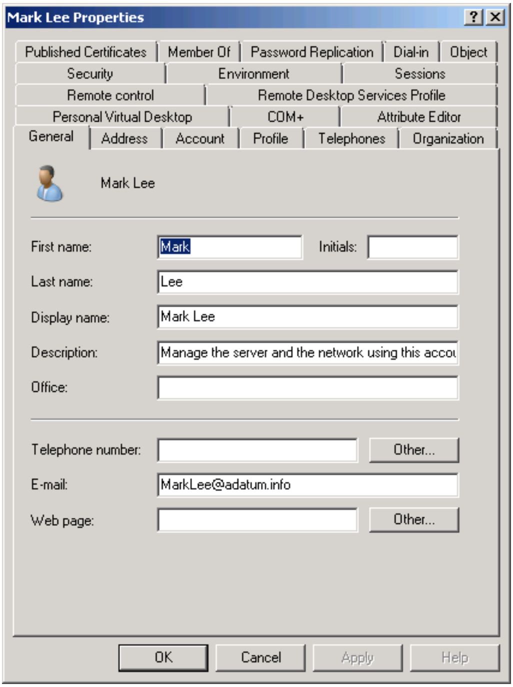


- Active Directory Users and Computers [SBS1.a
  - Saved Queries
  - adatum.local
    - Builtin
    - Computers
    - Domain Controllers
    - ForeignSecurityPrincipals
    - LostAndFound
    - Managed Service Accounts
    - Microsoft Exchange Security Groups
    - MyBusiness
      - Computers
        - SBSComputers
        - SBSServers
      - Distribution Groups
      - Security Groups
      - Users
        - SBSUsers
    - Program Data
    - System
    - Users
    - Microsoft Exchange System Objects
    - NTDS Quotas

Name	Type	Description
Builtin	builtinDomain	
Computers	Container	Default container for upgraded computer accounts
Domain Controllers	Organizational Unit	Default container for domain controllers
ForeignSecurityPrin...	Container	Default container for security identifiers (SIDs) ass
Infrastructure	infrastructureUpdate	
LostAndFound	lostAndFound	Default container for orphaned objects
Managed Service A...	Container	Default container for managed service accounts
Microsoft Exchange...	Organizational Unit	
Microsoft Exchange...	msExchSystemObj...	
MyBusiness	Organizational Unit	Default organizational unit for Windows Small Busin
NTDS Quotas	msDS-QuotaConta...	Quota specifications container
Program Data	Container	Default location for storage of application data.
System	Container	Builtin system settings
Users	Container	Default container for upgraded user accounts

FIGURE 6-6 The Active Directory Users And Computers Console, in Advanced Features mode.

The Advanced Features mode also displays additional attributes for each object. The Properties sheet for a user object, for example, has five additional tabs, as shown in Figure 6-7.



Mark Lee

First name: Mark

Initials:

Last name: Lee

Display name: Mark Lee

Description: Manage the server and the network using this accou

Office:

Telephone number:

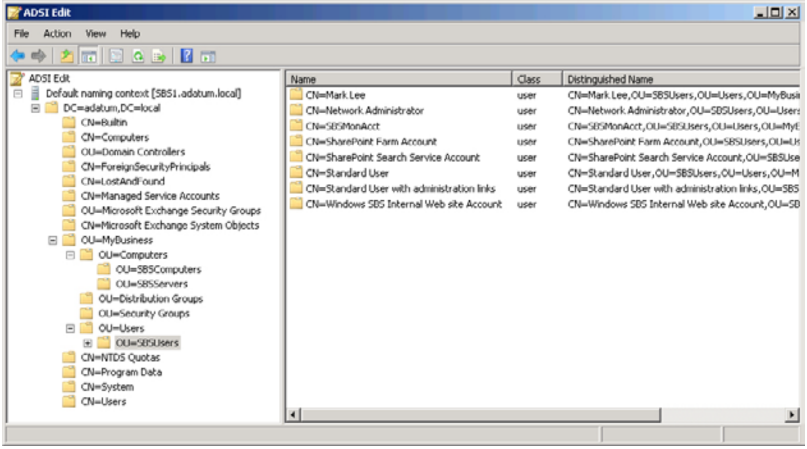
E-mail: MarkLee@adatum.info

Web page:

FIGURE 6-7 The Properties sheet for a user object in the Advanced Features mode of the Active Directory Users And Computers Console.

Using ADSI Edit

For even more complete access to object attributes, you can use the Active Directory Services Interface Editor (ADSI Edit) Console, shown in Figure 6-8. This tool provides full access to all the attributes of every object in your AD DS domain, including a great many that the average administrator never has to use.

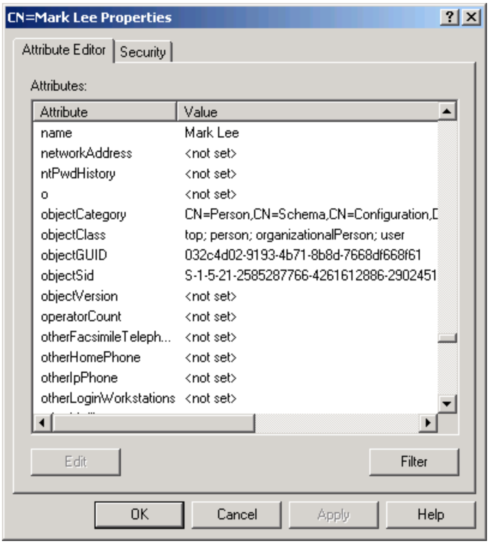


- ADSI Edit
  - Default naming context [SBS1.adatum.local]
    - DC=adatum,DC=local
      - CN=Builtin
      - CN=Computers
      - OU=Domain Controllers
      - CN=ForeignSecurityPrincipals
      - CN=LostAndFound
      - CN=Managed Service Accounts
      - OU=Microsoft Exchange Security Groups
      - CN=Microsoft Exchange System Objects
      - OU=MyBusiness
        - OU=Computers
          - OU=SBSComputers
          - OU=SBSServers
        - OU=Distribution Groups
        - OU=Security Groups
        - OU=Users
          - OU=SBSUsers
      - CN=NTDS Quotas
      - CN=Program Data
      - CN=System
      - CN=Users

Name	Class	Distinguished Name
CN=Mark Lee	user	CN=Mark Lee,OU=SBSUsers,OU=Users,OU=MyBusi
CN=Network Administrator	user	CN=Network Administrator,OU=SBSUsers,OU=Users
CN=SBSMonAcct	user	CN=SBSMonAcct,OU=SBSUsers,OU=Users,OU=MyE
CN=SharePoint Farm Account	user	CN=SharePoint Farm Account,OU=SBSUsers,OU=Us
CN=SharePoint Search Service Account	user	CN=SharePoint Search Service Account,OU=SBSUse
CN=Standard User	user	CN=Standard User,OU=SBSUsers,OU=Users,OU=M
CN=Standard User with administration links	user	CN=Standard User with administration links,OU=SBS
CN=Windows SBS Internal Web site Account	user	CN=Windows SBS Internal Web site Account,OU=SB

FIGURE 6-8 The ADSI Edit Console.

Opening the Properties sheet for an object in ADSI Edit displays an interface like that shown in Figure 6-9. Instead of the intuitive controls found in Active Directory Users and Computers, ADSI Edit provides direct access to the attributes and assumes that you are familiar with the correct syntax for the attributes that you intend to modify.

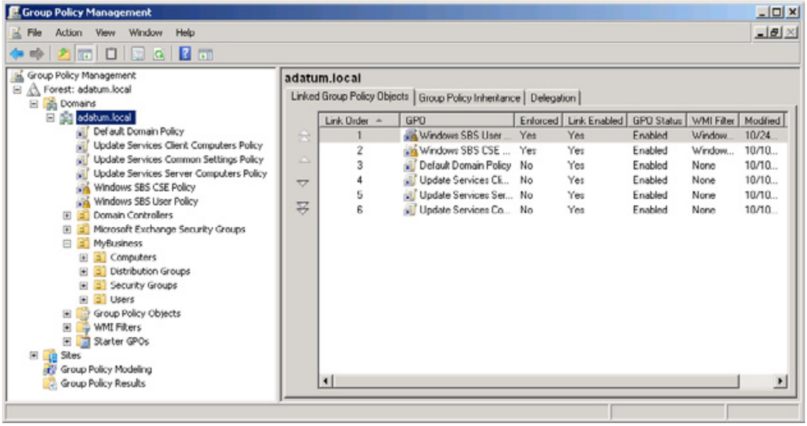


Attribute	Value
name	Mark Lee
networkAddress	<not set>
ntPwdHistory	<not set>
o	<not set>
objectCategory	CN=Person,CN=Schema,CN=Configuration,D
objectClass	top; person; organizationalPerson; user
objectGUID	032c4d02-9193-4b71-8b8d-7668df668f61
objectSid	S-1-5-21-2585287766-4261612886-2902451
objectVersion	<not set>
operatorCount	<not set>
otherFacsimileTeleph...	<not set>
otherHomePhone	<not set>
otherIpPhone	<not set>
otherLoginWorkstations	<not set>

FIGURE 6-9 The Properties sheet for a user object in the ADSI Edit Console.

Using Group Policy Management

To manage Group Policy settings for your AD DS network, the primary tool is the Group Policy Management Console, shown in Figure 6-10. Group Policy Management, like Active Directory Users and Computers, is an MMC snap-in that displays your GPOs; the settings they contain; and the domain, site, and OU objects to which you can link them.

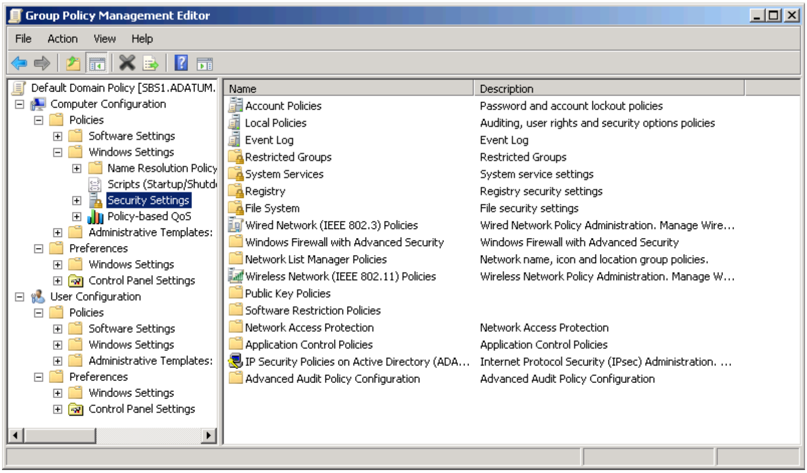


adatum.local

Link Order	GPO	Enforced	Link Enabled	GPO Status	WMI Filter	Modified
1	Windows SBS User ...	Yes	Yes	Enabled	Window...	10/24...
2	Windows SBS CSE ...	Yes	Yes	Enabled	Window...	10/10...
3	Default Domain Policy	No	Yes	Enabled	None	10/10...
4	Update Services Cli...	No	Yes	Enabled	None	10/10...
5	Update Services Ser...	No	Yes	Enabled	None	10/10...
6	Update Services Co...	No	Yes	Enabled	None	10/10...

FIGURE 6-10 The Group Policy Management Console.

The basic functions of the Group Policy Management Console are to display information about GPOs and manage the links between GPOs and AD DS objects. To edit the GPOs, you use the Group Policy Management Editor Console, shown in Figure 6-11. Each GPO has two main sections, one containing settings that apply to computers and one that applies to users. When a computer on the network starts, it downloads all the GPOs linked to it and applies the Computer Configuration settings. Then, when a user logs on to the domain, the system applies the User Configuration settings.

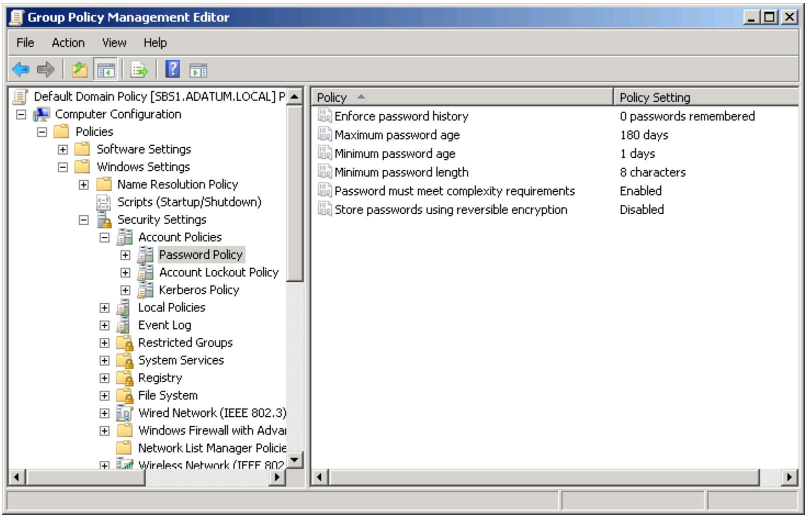


- Default Domain Policy [SBS1.ADATUM.
  - Computer Configuration
    - Policies
      - Software Settings
      - Windows Settings
        - Name Resolution Policy
        - Scripts (Startup/Shutd
        - Security Settings
        - Policy-based QoS
      - Administrative Templates:
    - Preferences
      - Windows Settings
      - Control Panel Settings
  - User Configuration
    - Policies
      - Software Settings
      - Windows Settings
      - Administrative Templates:
    - Preferences
      - Windows Settings
      - Control Panel Settings

Name	Description
Account Policies	Password and account lockout policies
Local Policies	Auditing, user rights and security options policies
Event Log	Event Log
Restricted Groups	Restricted Groups
System Services	System service settings
Registry	Registry security settings
File System	File security settings
Wired Network (IEEE 802.3) Policies	Wired Network Policy Administration. Manage Wire…
Windows Firewall with Advanced Security	Windows Firewall with Advanced Security
Network List Manager Policies	Network name, icon and location group policies.
Wireless Network (IEEE 802.11) Policies	Wireless Network Policy Administration. Manage W…
Public Key Policies	
Software Restriction Policies	
Network Access Protection	Network Access Protection
Application Control Policies	Application Control Policies
IP Security Policies on Active Directory (ADA…	Internet Protocol Security (IPsec) Administration. …
Advanced Audit Policy Configuration	Advanced Audit Policy Configuration

FIGURE 6-11 The Group Policy Management Editor Console.

Within each of the two sections is a hierarchy of nodes and folders containing hundreds of individual policy settings, as shown in Figure 6-12. You can enable as many or as few policy settings as you want in a particular GPO.

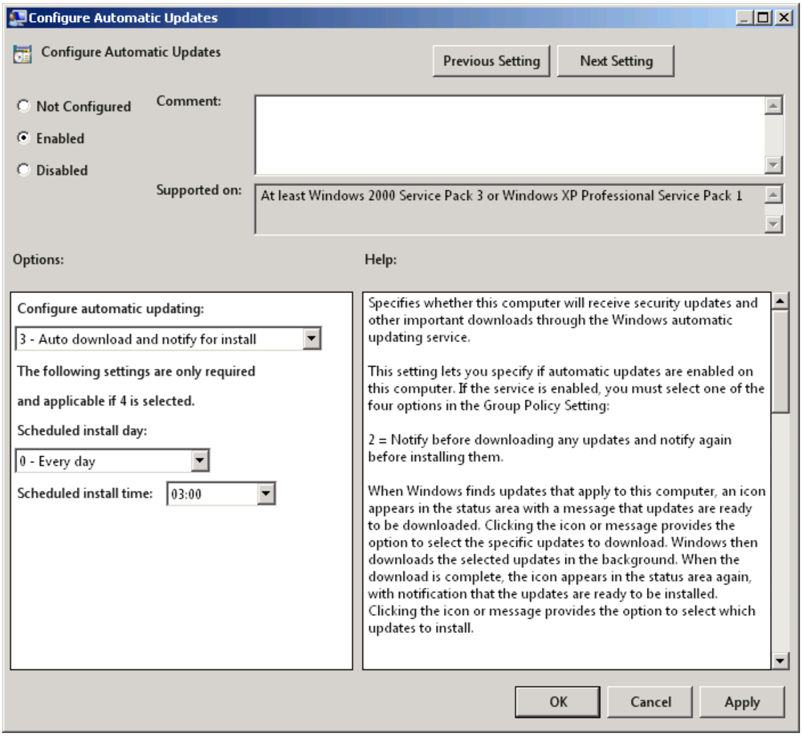


- Default Domain Policy [SBS1.ADATUM.LOCAL] P
  - Computer Configuration
    - Policies
      - Software Settings
      - Windows Settings
        - Name Resolution Policy
        - Scripts (Startup/Shutdown)
        - Security Settings
          - Account Policies
            - Password Policy
            - Account Lockout Policy
            - Kerberos Policy
          - Local Policies
          - Event Log
          - Restricted Groups
          - System Services
          - Registry
          - File System
          - Wired Network (IEEE 802.3)
          - Windows Firewall with Advai
          - Network List Manager Policie
          - Wireless Network (IEEE 802

Policy	Policy Setting
Enforce password history	0 passwords remembered
Maximum password age	180 days
Minimum password age	1 days
Minimum password length	8 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

FIGURE 6-12 Nodes and folders in the Group Policy Management Editor Console.

When you select a Group Policy setting, a Properties sheet appears, as shown in Figure 6-13, containing controls that you use to configure the setting.



○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows 2000 Service Pack 3 or Windows XP Professional Service Pack 1

Options:

Configure automatic updating: 3 - Auto download and notify for install

The following settings are only required and applicable if 4 is selected.

Scheduled install day: 0 - Every day

Scheduled install time: 03:00

Help:

Specifies whether this computer will receive security updates and other important downloads through the Windows automatic updating service.

This setting lets you specify if automatic updates are enabled on this computer. If the service is enabled, you must select one of the four options in the Group Policy Setting:

2 = Notify before downloading any updates and notify again before installing them.

When Windows finds updates that apply to this computer, an icon appears in the status area with a message that updates are ready to be downloaded. Clicking the icon or message provides the option to select the specific updates to download. Windows then downloads the selected updates in the background. When the download is complete, the icon appears in the status area again, with notification that the updates are ready to be installed. Clicking the icon or message provides the option to select which updates to install.

FIGURE 6-13 The Properties sheet for a setting in the Group Policy Management Editor Console.

> ***NOTE*** **Windows Server 2008 R2 provides several other AD DS management tools, including the Active Directory Domain And Trusts Console and the Active Directory Sites And Services Console. These tools are intended for use on larger AD DS installations, with multiple domains and sites, and are generally not needed on Windows SBS 2011 networks.**

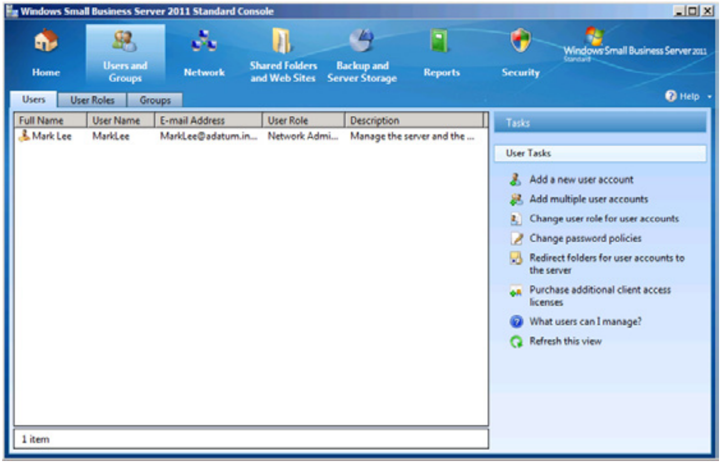
Working with Users

Before you connect a workstation to the network, you must create user accounts for all the individuals who will be logging on using that workstation. The Windows SBS Console includes a link to the Add A New User Account Wizard in the Getting Started Tasks list, as well as on the Frequent Tasks And Community Links page and on the Users And Groups page. The *Users* tab on the Users And Groups page also provides controls you can use to manage existing user accounts.

Creating a User Account

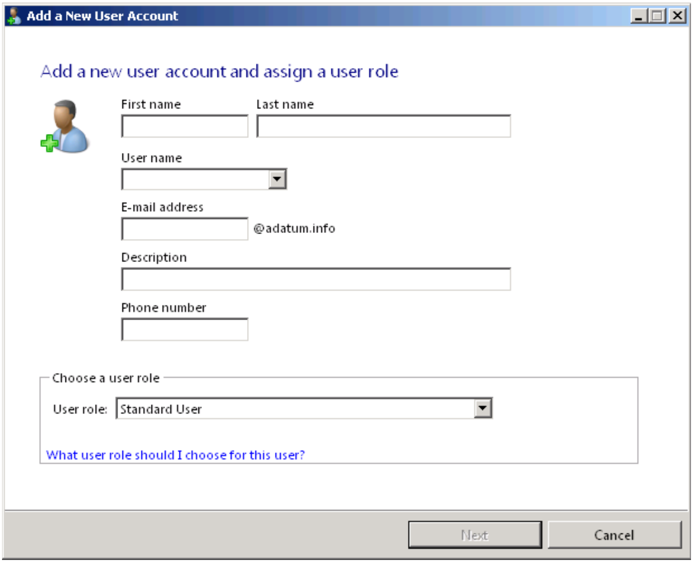
To create a new user account in the Windows SBS Console, use the following procedure:

1. Log on to your Windows SBS 2011 primary server using an account with network Administrator privileges. The Windows SBS Console appears.
2. Click *Users and groups*, and make sure the *Users* tab is selected.


Windows Small Business Server 2011 Standard Console
Home
Users and Groups
Network
Shared Folders and Web Sites
Backup and Server Storage
Reports
Security
Windows Small Business Server 2011 Standard
Users
User Roles
Groups
Help
Tasks
User Tasks
Add a new user account
Add multiple user accounts
Change user role for user accounts
Change password policies
Redirect folders for user accounts to the server
Purchase additional client access licenses
What users can I manage?
Refresh this view
1 item

Full Name	User Name	E-mail Address	User Role	Description
Mark Lee	MarkLee	MarkLee@adatum.in...	Network Admi...	Manage the server and the ...

3. In the *User tasks* list, click *Add a new user account*. The Add A New User Account Wizard appears, displaying the Add A New User Account And Assign A User Role page.

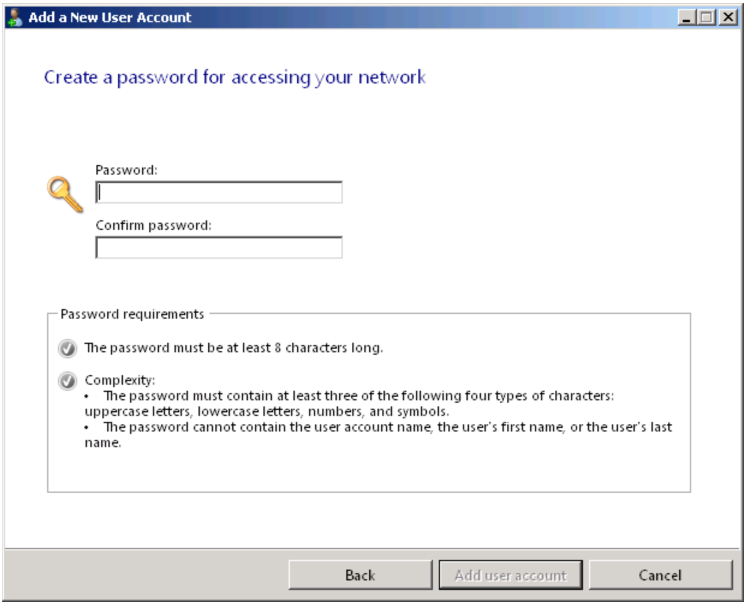


User role: Standard User

4. In the *First name* and *last name* text boxes, type the name of the user that you want to add.
5. In the User Name field, select one of the suggested names from the drop-down list or type a name of your own. The name that you specify appears in the *E-mail address* text box.

TIP **If you select one of the suggested account names in the drop-down list, the wizard remembers your selection and uses the same naming convention when you create subsequent user accounts.**

6. Add information to the *Description* and *phone number* text boxes, if desired.
7. In the *User role* drop-down list, select the role that you want to apply to the account and click *Next*. The Create A Password For Accessing Your Network page appears.



Create a password for accessing your network

Password:

Confirm password:

Password requirements

The password must be at least 8 characters long.

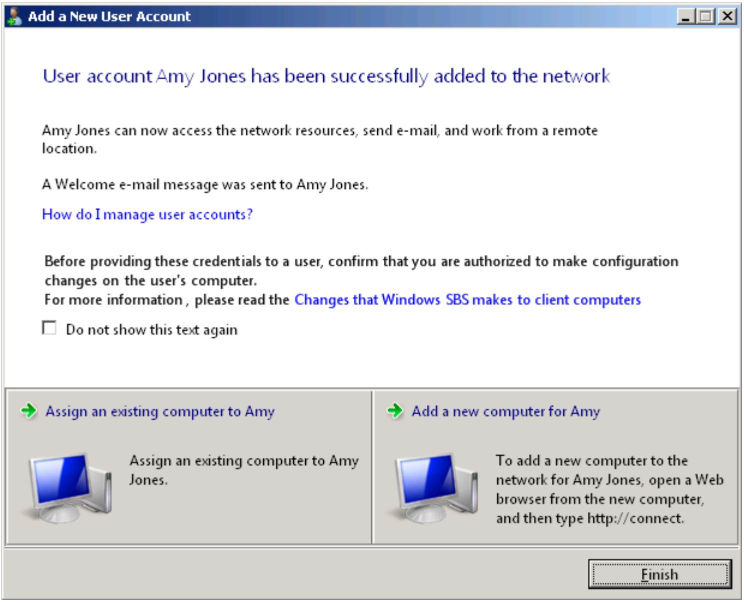
Complexity:
- The password must contain at least three of the following four types of characters: uppercase letters, lowercase letters, numbers, and symbols.
- The password cannot contain the user account name, the user's first name, or the user's last name.

8. In the *Password* and *confirm password* text boxes, type a password that conforms to the requirements stated on the page.

NOTE **Windows SBS 2011 uses Group Policy settings to enforce the password length and complexity requirements for domain user accounts. You can modify these requirements by modifying the Password Policy settings in the Default Domain Policy GPO.**

BEST PRACTICES In many cases, administrators assign the same temporary password to all user accounts when they create them and then require the users to supply their own passwords after they log on for the first time. However, you can choose to assign a unique password to each user account when you create it and then supply the password to the user.

9. Click *Add user account*. The wizard creates the user account and the User Account [User Name] Has Been Successfully Added To The Network page appears.



User account Amy Jones has been successfully added to the network

Amy Jones can now access the network resources, send e-mail, and work from a remote location.

A Welcome e-mail message was sent to Amy Jones.

How do I manage user accounts?

Before providing these credentials to a user, confirm that you are authorized to make configuration changes on the user's computer.
For more information , please read the Changes that Windows SBS makes to client computers

□ Do not show this text again

Assign an existing computer to Amy

Assign an existing computer to Amy Jones.

Add a new computer for Amy

To add a new computer to the network for Amy Jones, open a Web browser from the new computer, and then type http://connect.

TIP Selecting the *Do not show this text again* check box streamlines the user creation process if you do not intend to add or assign a computer after creating each user account. This page also contains links that enable you to assign an existing computer to the user you just created or add a new computer by proceeding directly to the Connect Computers To Your Network Wizard.

10. Click *Finish*. The wizard closes, and the user account appears on the Users And Groups page.

As mentioned earlier, the Add A New User Account Wizard creates a new user object in the AD DS database, but it also performs the following tasks:

- The wizard creates a folder, named for the user, in the C:\Users\Shares folder on the server. This folder appears on the network as \\server\UserShares, where *server* is the name of your server. Everyone has the Allow Full Control share permission for the UserShares folder, and each user has the Full Control NTFS permission to his or her own folder. Users have no NTFS permissions for other users' folders, but the Administrators group has the Allow Full Control permission.

  MORE INFO **For more information on share and NTFS permissions, see Chapter 8, "Working with Permissions."**

- The wizard creates a Microsoft Exchange Server mailbox for the user, with a maximum mailbox size of 2 gigabytes (GB). Outlook Web Access is enabled, as are the Messaging Application Programming Interface (MAPI), Post Office Protocol version 3 (POP3), and Internet Message Access Protocol (IMAP) client capabilities.

  MORE INFO **For more information on Exchange Server and the messaging protocols it supports, see Chapter 15, "Administering Email."**

- The wizard sets two storage quotas for the user in the File Server Resource Manager Console: a 2-GB soft quota, for the user's Folder Redirections folder, and a 2-GB hard quota for the user's shared folder.

  MORE INFO **In File Server Resource Manager, soft quotas merely warn the users when they reach their storage limit, while hard quotas prevent users from exceeding their limits. For more information on using storage quotas, see Chapter 9, "Managing Storage."**

- The wizard sends an email to the user's mailbox, welcoming the user to the domain.
- The wizard adds the user account to several of the default groups created by the Windows SBS 2011 setup program. The group memberships are based on the user role you selected when creating the user. Table 6-1 lists the group memberships associated with each of the three default user roles.

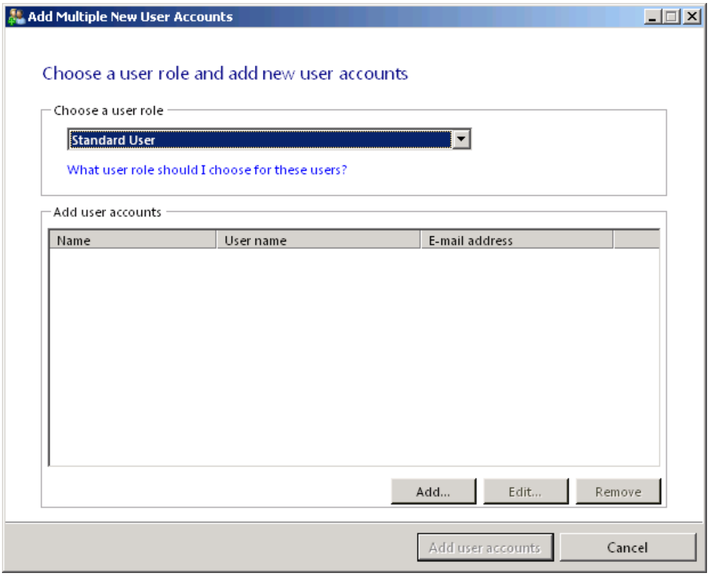
TABLE 6-1 Group Memberships of the Windows SBS 2011 Default User Roles

	STANDARD USER	STANDARD USER WITH ADMINISTRATION LINKS	NETWORK ADMINISTRATOR
All Users	X	X	X
Windows SBS Admin Tools Group		X	X
Windows SBS Administrators		X	X
Windows SBS Fax Administrators			X
Windows SBS Fax Users	X	X	X
Windows SBS Link Users	X	X	X
Windows SBS Remote Web Access Users	X	X	X
Windows SBS SharePoint_ MembersGroup	X	X	
Windows SBS SharePoint_ OwnersGroup			X
Windows SBS SharePoint_ VisitorsGroup			
Windows SBS Virtual Private Network Users			X

Creating Multiple User Accounts

If you have to create a number of user accounts based on the same role, you can run the Add Multiple New User Accounts Wizard using the following procedure:

1. Log on to your Windows SBS 2011 primary server, using an account with network Administrator privileges. The Windows SBS Console appears.
2. Click the *Users and Groups* button and make sure the *Users* tab is selected.
3. In the *User tasks* list, click *Add multiple user accounts*. The Add Multiple New User Accounts Wizard appears, displaying the Choose A User Role And Add New User Accounts page.



Add Multiple New User Accounts

Choose a user role and add new user accounts

Choose a user role

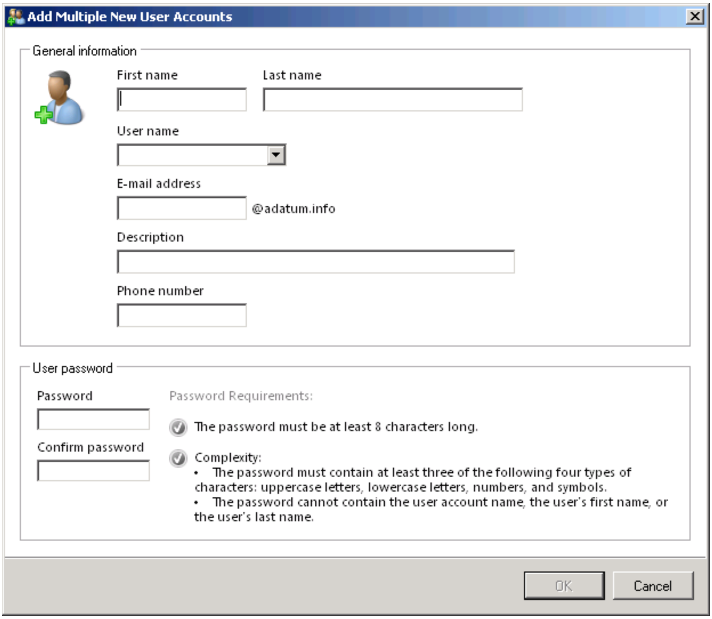
Standard User

What user role should I choose for these users?

Add user accounts

Name	User name	E-mail address

4. In the *Choose a user role* drop-down list, select the role that you want to use to create the accounts.
5. In the *Add user accounts* box, click *Add*. An Add Multiple New User Accounts dialog box appears.



Add Multiple New User Accounts

General information

First name

Last name

User name

E-mail address

@adatum.info

Description

Phone number

User password

Password

Confirm password

Password Requirements:

The password must be at least 8 characters long.

Complexity:
- The password must contain at least three of the following four types of characters: uppercase letters, lowercase letters, numbers, and symbols.
- The password cannot contain the user account name, the user's first name, or the user's last name.

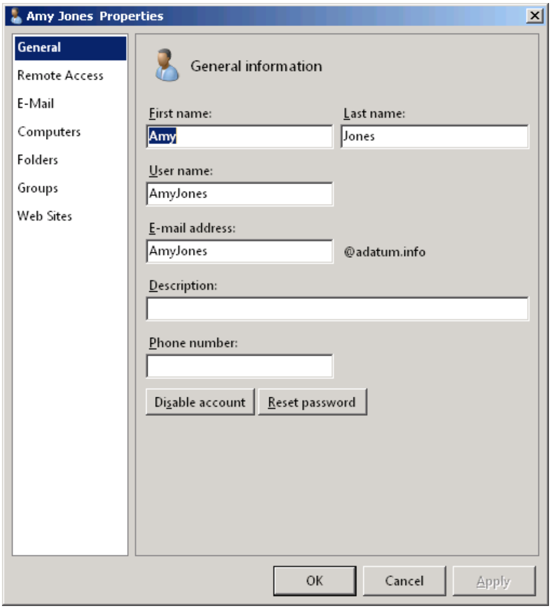
6. In the *First name* and *last name* text boxes, type the name of the user that you want to add.
7. In the *User name* field, select one of the suggested names from the drop-down list or type a name of your own. The name you specify appears in the *E-mail address* text box.
8. Add information to the *Description* and *phone number* text boxes, if desired.
9. In the *Password* and *confirm password* text boxes, type a password that conforms to the requirements stated on the page.
10. Click *OK*. The user appears in the *Add user accounts* list.
11. Repeat steps 5 to 10 to add more users to the list.
12. Click *Add user accounts*. The wizard creates all the user accounts in the list, and the All New User Accounts Have Been Successfully Added To The Network page appears.
13. Click *Finish*.

Managing User Properties

Once you have created user accounts, they appear in the Windows SBS Console on the Users And Groups page on the *Users* tab. On the right side of the page, the *Tasks list* is split into two sections: *User tasks*, which contains links to general tools, such as the Add A New User Account Wizard, and a second section containing tasks that apply to the currently selected user. These tasks enable you to work with the attributes of the selected user object.

To modify the properties of a user account, use the following procedure.

1. Log on to your Windows SBS 2011 primary server, using an account with network Administrator privileges. The Windows SBS Console appears.
2. Click *Users and groups*, and select the *Users* tab.
3. Select one of the user accounts on the page and, in the Tasks list, click *Edit user account properties*. The Properties sheet for the user account appears.
4. Select one of the following pages in the dialog box and use the controls provided to modify the user's properties:
   - **General** Contains the basic informational fields, such as name, email address, and phone number, for which you supplied values when you created the user account.


Amy Jones Properties

General information

First name: Amy

Last name: Jones

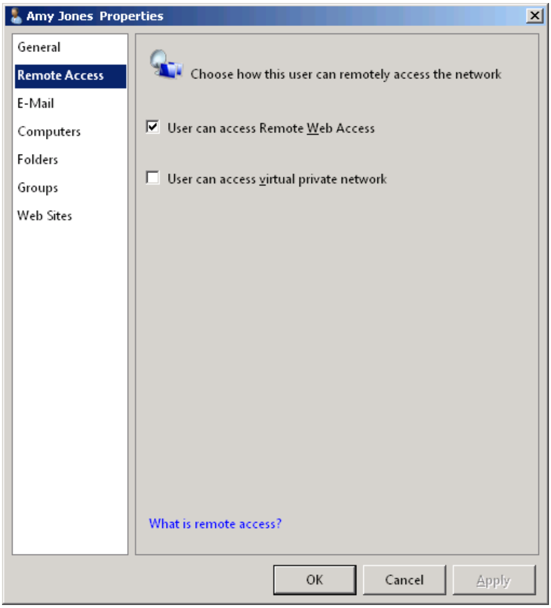
User name: AmyJones

E-mail address: AmyJones @adatum.info

Description:

Phone number:

- **Remote Access** Specifies whether the user is permitted to access the network from remote locations using Remote Web Access and virtual private networking (VPN) connections.

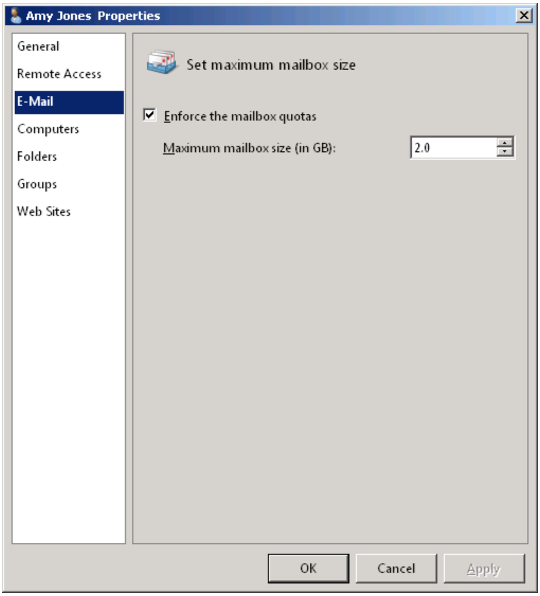

Amy Jones Properties

Choose how this user can remotely access the network

☑ User can access Remote Web Access

☐ User can access virtual private network

- **E-Mail** Specifies whether the user's Exchange Server mailbox should be limited to a maximum size, and if so, specifies that size, in gigabytes.



Amy Jones Properties

General
Remote Access
E-Mail
Computers
Folders
Groups
Web Sites

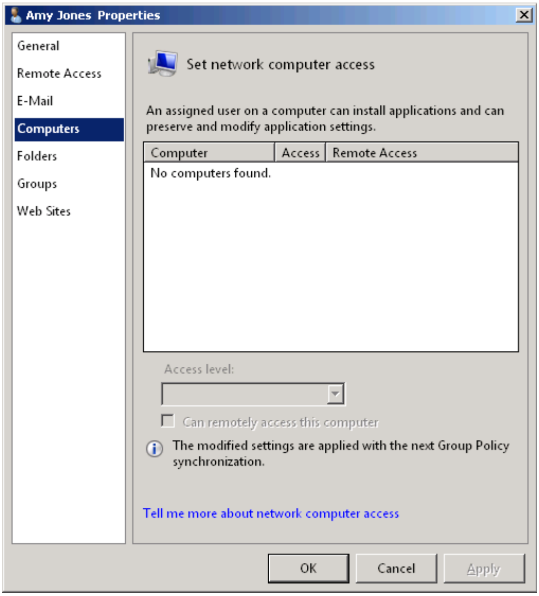
Set maximum mailbox size

☑ Enforce the mailbox quotas

Maximum mailbox size (in GB): 2.0

OK Cancel Apply

- **Computers** Specifies which computers on the network the user is permitted to access and what level of access the user is granted.



Amy Jones Properties

General
Remote Access
E-Mail
Computers
Folders
Groups
Web Sites

Set network computer access

An assigned user on a computer can install applications and can preserve and modify application settings.

Computer	Access	Remote Access
No computers found.		

Access level:

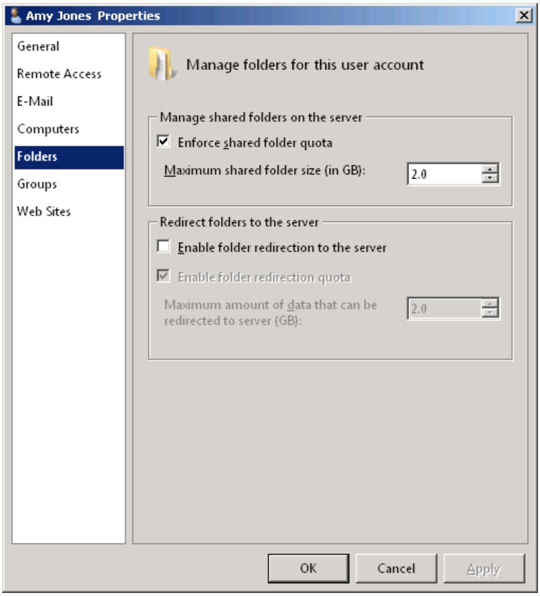
□ Can remotely access this computer

The modified settings are applied with the next Group Policy synchronization.

Tell me more about network computer access

OK Cancel Apply

- **Folders** Specifies whether the user's shared folder should have a storage quota and whether the user's data folders should be redirected to a server drive. You can also specify the size of the storage quotas for each.



Amy Jones Properties

General
Remote Access
E-Mail
Computers
Folders
Groups
Web Sites

Manage folders for this user account

Manage shared folders on the server

☑ Enforce shared folder quota

Maximum shared folder size (in GB): 2.0

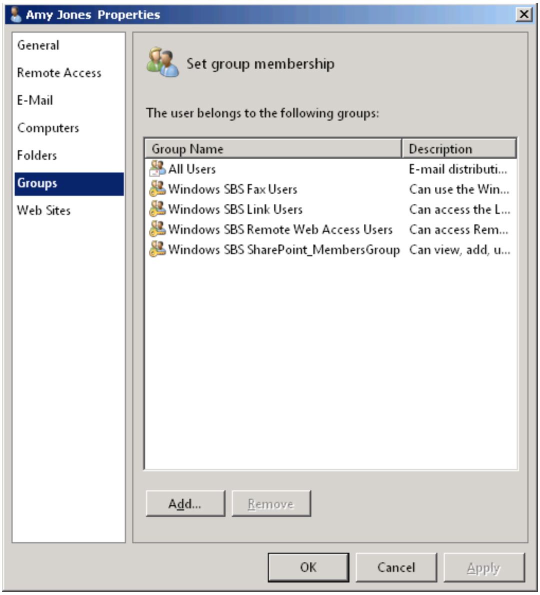
Redirect folders to the server

☐ Enable folder redirection to the server

☑ Enable folder redirection quota

Maximum amount of data that can be redirected to server (GB): 2.0

- **Groups** Specifies the groups of which the user is a member.



Amy Jones Properties

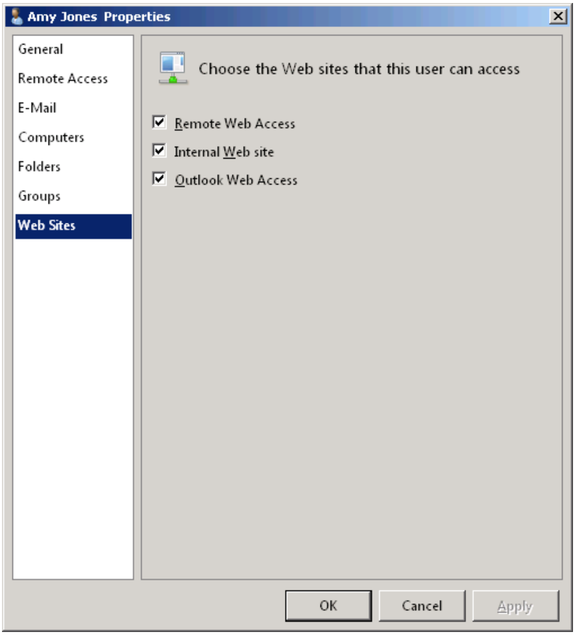
General
Remote Access
E-Mail
Computers
Folders
Groups
Web Sites

Set group membership

The user belongs to the following groups:

Group Name	Description
All Users	E-mail distributi...
Windows SBS Fax Users	Can use the Win...
Windows SBS Link Users	Can access the L...
Windows SBS Remote Web Access Users	Can access Rem...
Windows SBS SharePoint_MembersGroup	Can view, add, u...

- **Web Sites** Specifies which of the default Windows SBS 2011 websites the user is permitted to access.



Amy Jones Properties

General
Remote Access
E-Mail
Computers
Folders
Groups
Web Sites

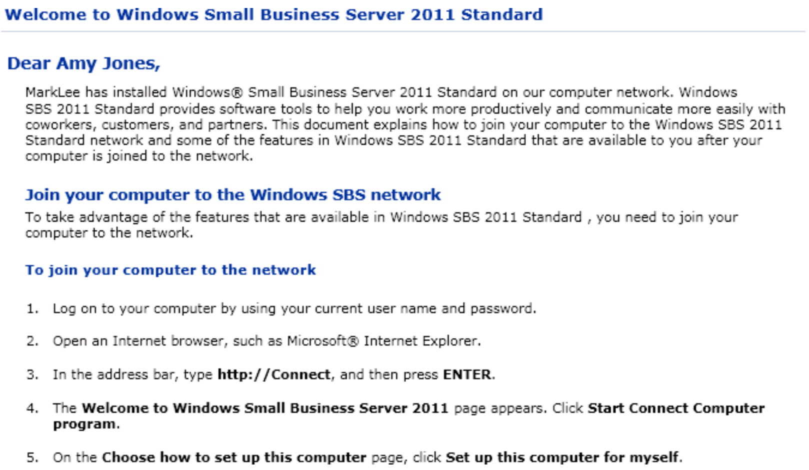
Choose the Web sites that this user can access

☑ Remote Web Access
☑ Internal Web site
☑ Outlook Web Access

5. Click *OK*. The Properties sheet closes and the console applies the changes that you have made.

Printing Customized Getting Started Pages

After creating a user account, the next step in deploying a workstation on a Windows SBS 2011 network is to connect the computer to the network. This is a procedure that users can perform themselves, and to simplify the process, Windows SBS 2011 enables you to print out a customized Getting Started page for each user, providing personalized instructions for logging on and connecting to the server, as shown in Figure 6-14.



Welcome to Windows Small Business Server 2011 Standard

Dear Amy Jones,

MarkLee has installed Windows® Small Business Server 2011 Standard on our computer network. Windows SBS 2011 Standard provides software tools to help you work more productively and communicate more easily with coworkers, customers, and partners. This document explains how to join your computer to the Windows SBS 2011 Standard network and some of the features in Windows SBS 2011 Standard that are available to you after your computer is joined to the network.

Join your computer to the Windows SBS network

To take advantage of the features that are available in Windows SBS 2011 Standard , you need to join your computer to the network.

To join your computer to the network

1. Log on to your computer by using your current user name and password.
2. Open an Internet browser, such as Microsoft® Internet Explorer.
3. In the address bar, type **http://Connect**, and then press **ENTER**.
4. The **Welcome to Windows Small Business Server 2011** page appears. Click **Start Connect Computer program.**
5. On the **Choose how to set up this computer** page, click **Set up this computer for myself.**

FIGURE 6-14 The Getting Started page for a Windows SBS 2011 user.

To print the Getting Started page, select a user account on the Users And Groups page and click *Print the getting started page for this user account*. You can then print the document using any of the printers that the computer is configured to use.

Creating User Roles

In Windows SBS 2011, a *user role* is a set of account property values that function as a template for the creation of new user accounts. Without user roles, you would have to configure all the user properties for each account that you create individually, adding users to multiple groups and specifying which resources they can access, for example. When you run the Add A New User Account Wizard, you select one of the existing user roles as the basis for the new account. Once you actually create the account, you can modify its properties as needed.

Windows SBS 2011 includes three user roles by default:

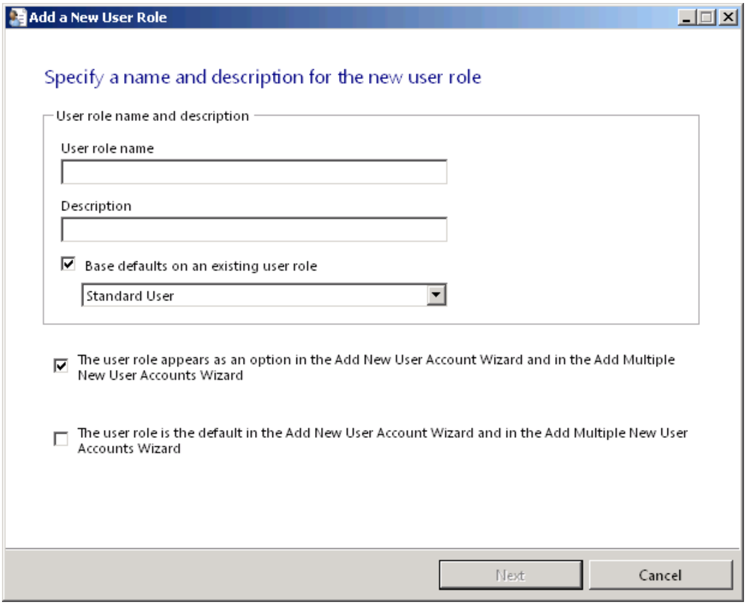
- **Standard User** Provides access to standard network resources, including network shares, printers and faxes, internal websites, Remote Web Access, and the Internet
- **Standard User with Administration Links** Same as the Standard User role, with added access to the administration links in Remote Web Access and the desktop gadget links
- **Network Administrator** Provides full access to all system resources

In addition to these three roles, you can create your own customized user roles with the procedures in the following sections.

Creating a New User Role

To create a new user role from scratch, use the following procedure:

1. Log on to your Windows SBS 2011 primary server, using an account with network Administrator privileges. The Windows SBS Console appears.
2. Click *Users and groups*, and select the *User* roles tab.
3. In the *User role tasks* list, click *Add a new user role*. The Add A New User Role Wizard appears, displaying the Specify A Name And Description For The New User Role page.



Add a New User Role

Specify a name and description for the new user role

User role name and description

User role name

Description

☑ Base defaults on an existing user role

Standard User

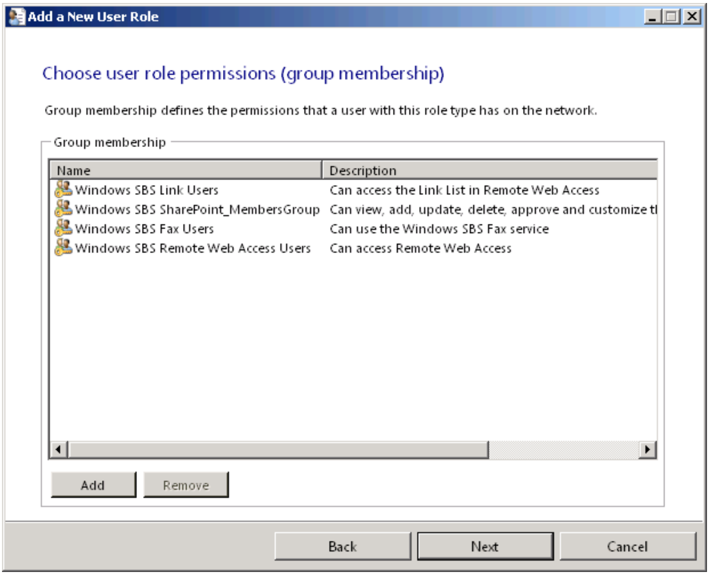
☑ The user role appears as an option in the Add New User Account Wizard and in the Add Multiple New User Accounts Wizard

□ The user role is the default in the Add New User Account Wizard and in the Add Multiple New User Accounts Wizard

4. In the *User role name* text box, type the name that you want to assign to the role. In the *Description* text box, type a description of the role's capabilities, if desired.
5. If you want to base your new user role on one of the existing roles, select the *Base defaults on an existing user role* check box and select the role that you want to use from the drop-down list.
6. Select the *The user role appears as an option in the Add New User Account Wizard and in the Add Multiple New User Accounts Wizard* check box if you intend to create user accounts based on this role.

7. Select the *The user role is the default in the Add New User Account Wizard and in the Add Multiple New User Accounts Wizard* check box if you intend to create most or all your user accounts with this role.

8. Click *Next*. The Choose User Role Permissions (Group Membership) page appears.



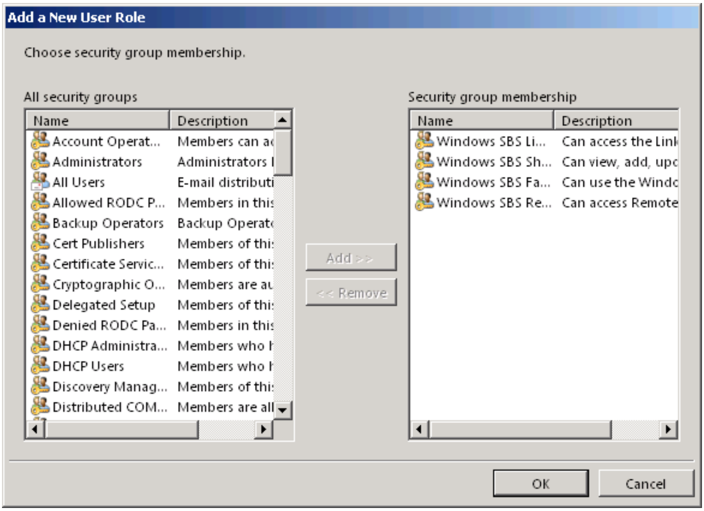
Choose user role permissions (group membership)

Group membership defines the permissions that a user with this role type has on the network.

Group membership

Name	Description
Windows SBS Link Users	Can access the Link List in Remote Web Access
Windows SBS SharePoint_MembersGroup	Can view, add, update, delete, approve and customize tl
Windows SBS Fax Users	Can use the Windows SBS Fax service
Windows SBS Remote Web Access Users	Can access Remote Web Access

9. To modify the group memberships assigned to the role, click *Add*. The Choose Security Group Membership dialog box appears.



Choose security group membership.

All security groups

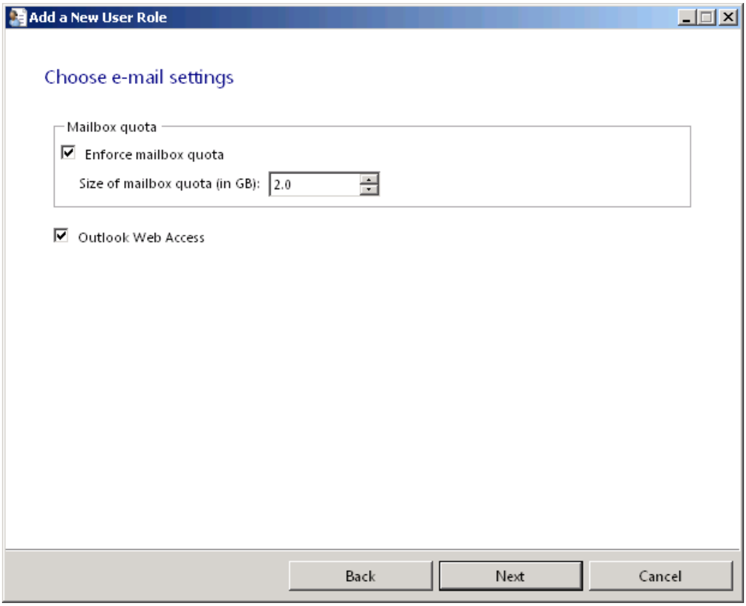
Name	Description
Account Operat...	Members can ac
Administrators	Administrators l
All Users	E-mail distributi
Allowed RODC P...	Members in this
Backup Operators	Backup Operato
Cert Publishers	Members of this
Certificate Servic...	Members of this
Cryptographic O...	Members are au
Delegated Setup	Members of this
Denied RODC Pa...	Members in this
DHCP Administra...	Members who h
DHCP Users	Members who h
Discovery Manag...	Members of this
Distributed COM...	Members are all

Security group membership

Name	Description
Windows SBS Li...	Can access the Link
Windows SBS Sh...	Can view, add, upc
Windows SBS Fa...	Can use the Windo
Windows SBS Re...	Can access Remote

10. Select the groups that you want to assign to the role in the *All security groups* list and click *Add*. Select the groups that you want to delete from the role in the *Security group membership* list and click *Remove*. Then click *OK*.

11. Click *Next*. The Choose E-Mail Settings page appears.



Choose e-mail settings

Mailbox quota

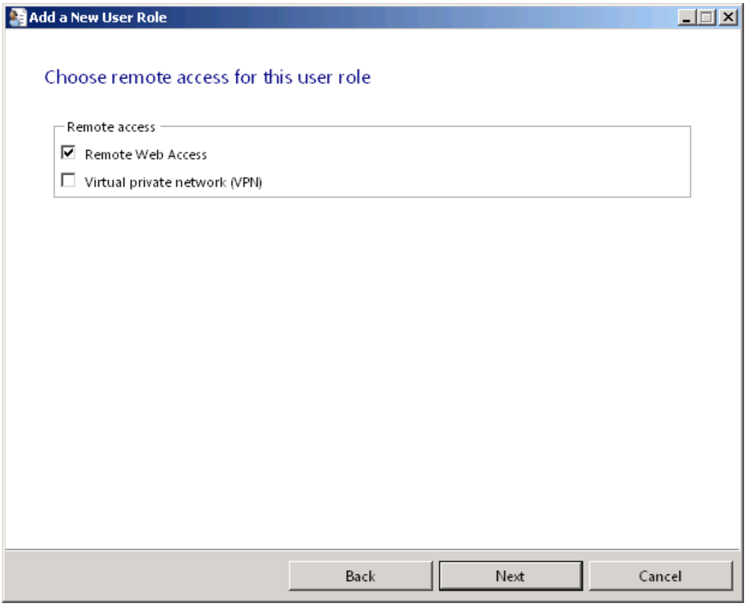
☑ Enforce mailbox quota

Size of mailbox quota (in GB): 2.0

☑ Outlook Web Access

12. Specify whether you want to apply a mailbox quota and whether users should be able to access the Outlook Web Access website.

13. Click *Next*. The Choose Remote Access For This User Role page appears.



Add a New User Role

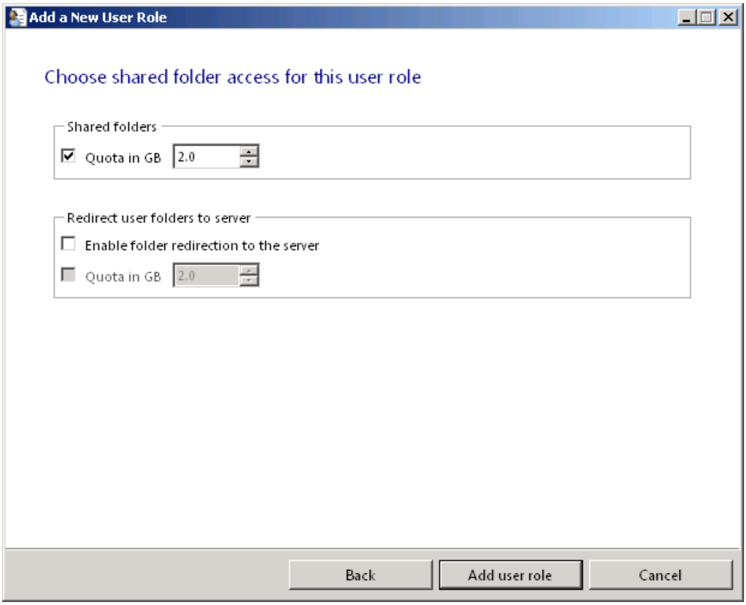
Choose remote access for this user role

Remote access

☑ Remote Web Access

□ Virtual private network (VPN)

14. Specify whether users should be permitted to access the network using Remote Web Access and VPN connections.
15. Click *Next*. The Choose Shared Folder Access For This User Role page appears.



Add a New User Role

Choose shared folder access for this user role

Shared folders

☑ Quota in GB 2.0

Redirect user folders to server

□ Enable folder redirection to the server

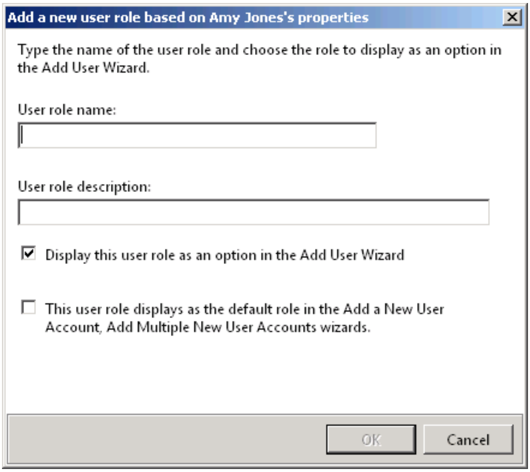
□ Quota in GB 2.0

16. Specify whether the user's shared folder should have a storage quota and whether the user's data folders should be redirected to a server drive. You can also specify the size of the storage quotas for each.
17. Click *Add user role*. The New User Role Was Added Successfully To The Network page is displayed.
18. Click *Finish*. The new role appears in the *User roles* list.

Creating a User Role from an Existing User

To create a user role based on a user account that you have modified to your requirements, use the following procedure:

1. Log on to your Windows SBS 2011 primary server, using an account with network Administrator privileges. The Windows SBS Console appears.
2. Click *Users and groups*, and make sure the *Users* tab is selected.
3. Select one of the user accounts on the page and, in the *Tasks list*, click *Add a new user role based on this user account's properties*. The Add A New User Role Based On [User Name's] Properties sheet appears.



Add a new user role based on Amy Jones's properties

Type the name of the user role and choose the role to display as an option in the Add User Wizard.

User role name:

User role description:

☑ Display this user role as an option in the Add User Wizard

□ This user role displays as the default role in the Add a New User Account, Add Multiple New User Accounts wizards.

4. In the *User role name* text box, type the name that you want to assign to the role. In the *User role description* text box, type a description of the role's capabilities, if desired.
5. Select the *Display this user role as an option in the Add User Wizard* check box if you intend to create user accounts based on this role.

6. Select the *This user role displays as the default role in the Add A New User Account, Add Multiple New User Accounts Wizards* check box if you intend to create all or most of your user accounts with this role.
7. Click *OK*. The new user role appears on the *User roles* tab.

Working with Computers

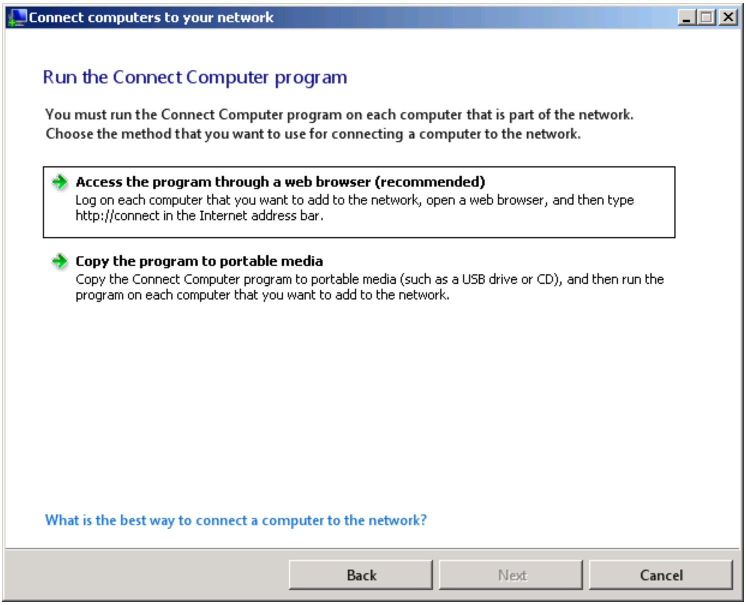
Windows SBS 2011 includes the operating system for your server, but you must purchase the Windows 7, Windows Vista, or Windows XP operating system for your workstations separately. Once you have installed Windows 7, Windows Vista, or Windows XP, you can join your workstations to the network by running the Connect Computer program on them.

> ***NOTE*** **To run successfully, the Connect Computer program requires that you use Windows 7, Windows Vista with Service Pack 2 (SP2) or later, or Windows XP with SP3 (for 32-bit) or SP2 (for 64-bit) or later. In addition, the client computer must be running Internet Explorer 7 or later and .NET Framework 4.0 or later, both of which are available as free downloads from the Microsoft Download Center.**

Connecting Computers to the Network

When you click the *Connect computers to your network* link in the Windows SBS Console's *Getting started tasks* list, a wizard appears that is primarily informational. After a page reminding you that you should create user accounts before you connect computers to the network, the wizard explains that you must run the Connect Computer program on each workstation that you want to connect to the network.

You can deploy the Connect Computer program to your workstations in two ways, as shown in the Connect Computers To Your Network Wizard (see Figure 6-15): by connecting to the Windows SBS 2011 server with Internet Explorer and downloading the program; or by copying the program from the server to a removable medium, such as a USB flash drive, and moving it to the workstation.



Run the Connect Computer program

You must run the Connect Computer program on each computer that is part of the network. Choose the method that you want to use for connecting a computer to the network.

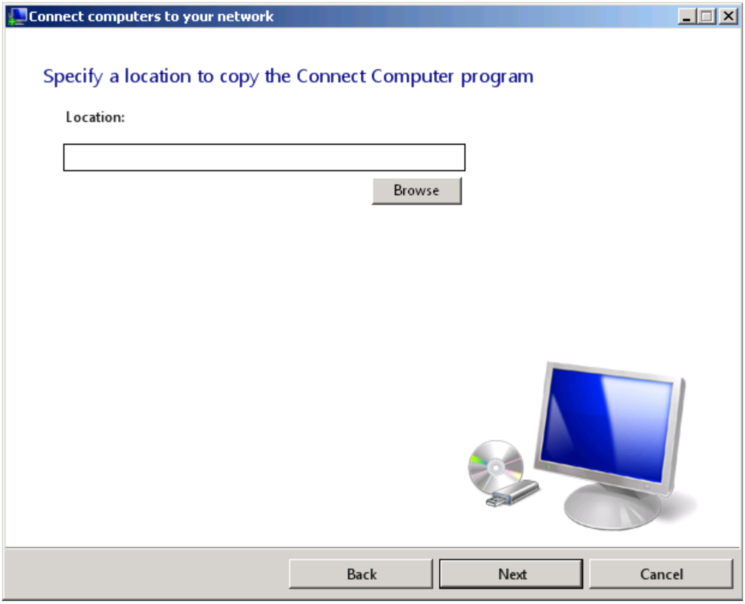
Access the program through a web browser (recommended)
Log on each computer that you want to add to the network, open a web browser, and then type http://connect in the Internet address bar.

Copy the program to portable media
Copy the Connect Computer program to portable media (such as a USB drive or CD), and then run the program on each computer that you want to add to the network.

What is the best way to connect a computer to the network?

FIGURE 6-15 The Connect Computers To Your Network Wizard.

When you select the *Access the program through a web browser (recommended)* option, the wizard displays instructions for connecting to the server from the workstation, the same instructions found in the Getting Started pages for the user. Selecting the *Copy the program to portable media* option displays the Specify A Location To Copy The Connect Computer Program page, shown in Figure 6-16, which enables you to copy the Connect Computer program to any storage device recognized by the file system. The total size of the program is only 226 kilobytes (KB); you can therefore use a floppy disk or any USB flash drive. You can also copy the program to a folder on a hard disk and burn it to a CD-ROM.



Specify a location to copy the Connect Computer program

Location:

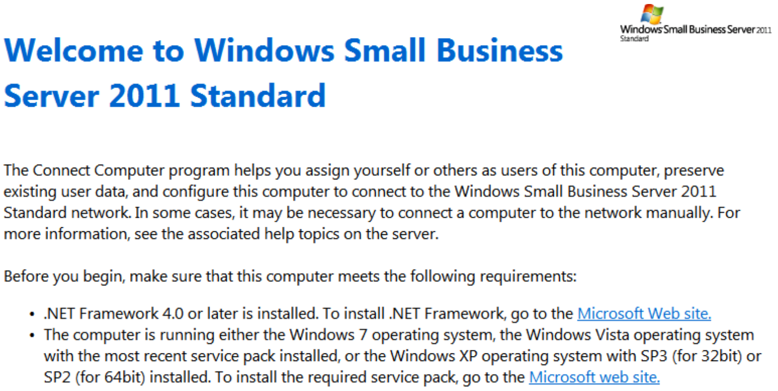
FIGURE 6-16 The Specify A Location To Copy The Connect Computer Program page in the Connect Computers To Your Network Wizard.

Running the Connect Computer Program

To run the Connect Computer program on a workstation, use the following procedure:

1. Log on to your workstation using an account with network Administrator privileges.
2. Click *Start*, and then click *Internet Explorer*. An Internet Explorer window appears.
3. In the *Address* box, type **http://connect** and press *Enter*. The Welcome To Windows Small Business Server 2011 page appears.

   If the client computer does not meet the requirements to run the Connect Computer program, a page listing the requirements appears.



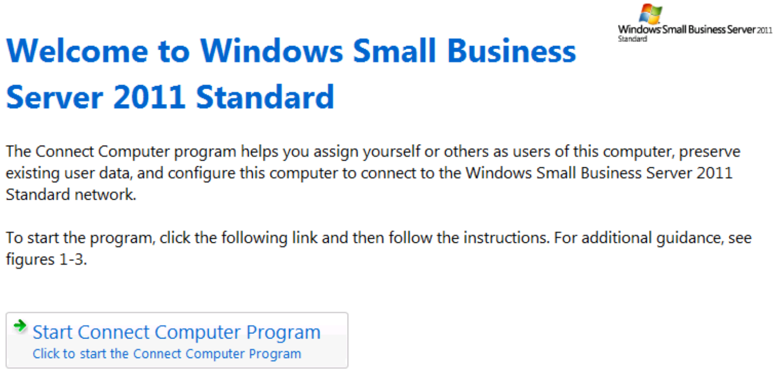
Welcome to Windows Small Business Server 2011 Standard

The Connect Computer program helps you assign yourself or others as users of this computer, preserve existing user data, and configure this computer to connect to the Windows Small Business Server 2011 Standard network. In some cases, it may be necessary to connect a computer to the network manually. For more information, see the associated help topics on the server.

Before you begin, make sure that this computer meets the following requirements:

- .NET Framework 4.0 or later is installed. To install .NET Framework, go to the Microsoft Web site.
- The computer is running either the Windows 7 operating system, the Windows Vista operating system with the most recent service pack installed, or the Windows XP operating system with SP3 (for 32bit) or SP2 (for 64bit) installed. To install the required service pack, go to the Microsoft web site.

If the client computer meets the requirements, a page appears containing a *Start connect computer program* link.


Windows Small Business Server 2011
Standard
Start Connect Computer Program
Click to start the Connect Computer Program

Welcome to Windows Small Business Server 2011 Standard

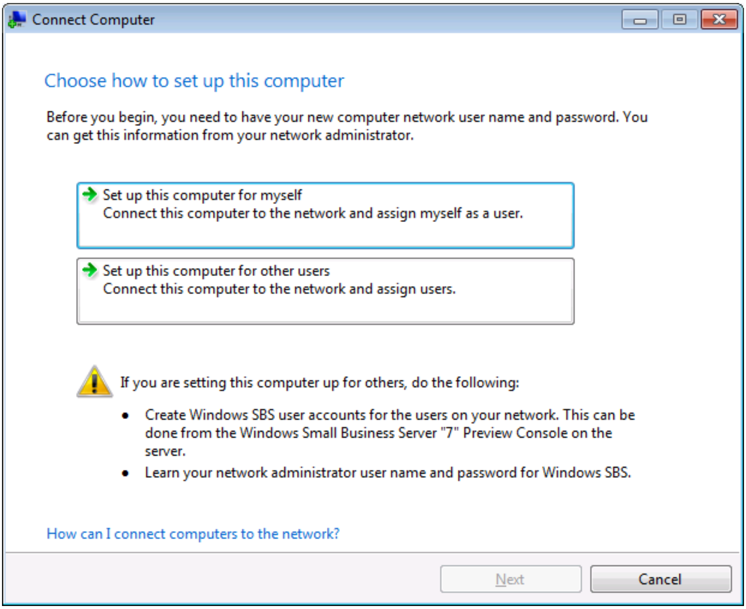
The Connect Computer program helps you assign yourself or others as users of this computer, preserve existing user data, and configure this computer to connect to the Windows Small Business Server 2011 Standard network.

To start the program, click the following link and then follow the instructions. For additional guidance, see figures 1-3.

4. Click the *Start computer connect program* link. A File Download—Security Warning message box appears, asking if you want to run or save the program.

NOTE **If you have the Connect Computer program on a removable medium, insert the disk or drive into the computer and run the Launcher.exe program.**

5. Click *Run*. Then click *Yes* in the User Account Control dialog box. The Connect Computer Wizard appears, displaying the Choose How To Set Up This Computer page.



Choose how to set up this computer

Before you begin, you need to have your new computer network user name and password. You can get this information from your network administrator.

Set up this computer for myself
Connect this computer to the network and assign myself as a user.

Set up this computer for other users
Connect this computer to the network and assign users.

If you are setting this computer up for others, do the following:

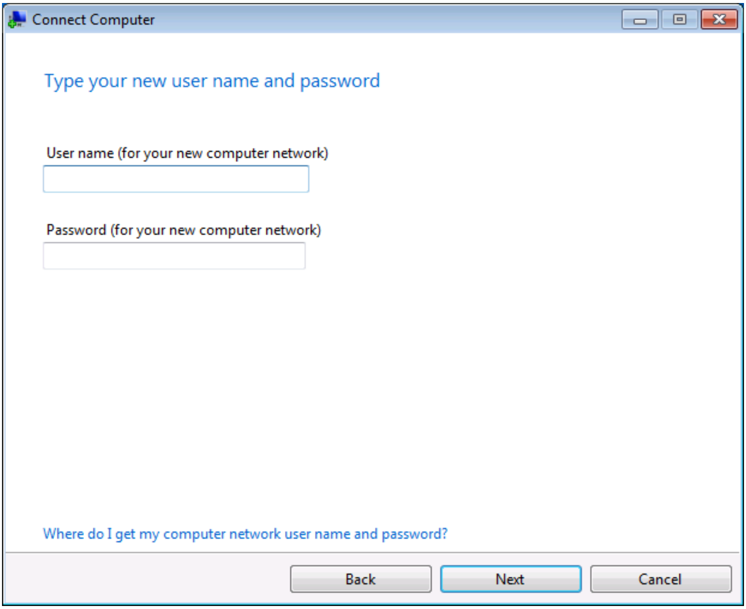
- Create Windows SBS user accounts for the users on your network. This can be done from the Windows Small Business Server "7" Preview Console on the server.
- Learn your network administrator user name and password for Windows SBS.

How can I connect computers to the network?

6. Click the *Set up this computer for myself* option. The Verifying Computer Requirements page appears as the program checks the state of the computer. If the computer meets the requirements, the Computer Requirements Are Verified page appears.

NOTE **If the computer does not meet the requirements for running the program (for example, if a Windows Vista workstation does not have SP2 or later installed), the wizard informs you what must be done before it can continue.**

7. Click *Next*. The Type Your New User Name And Password page appears.



Connect Computer

Type your new user name and password

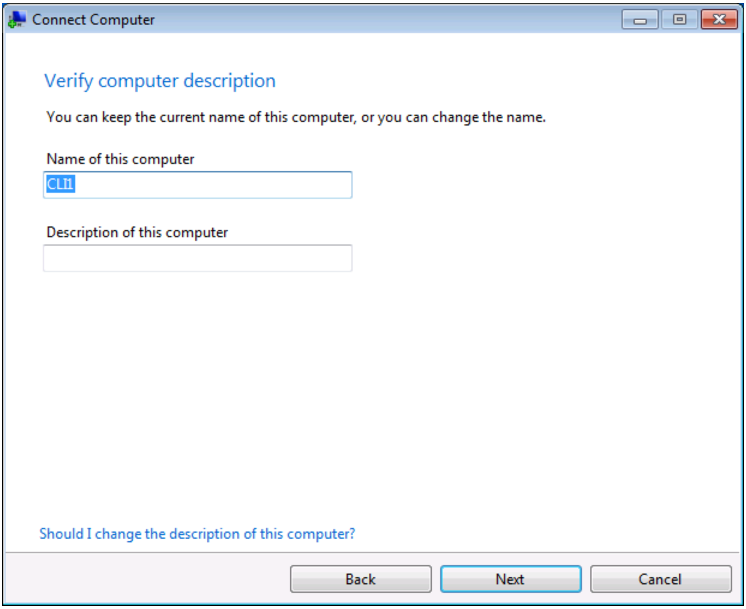
User name (for your new computer network)

Password (for your new computer network)

Where do I get my computer network user name and password?

8. In the *User name* and *password* text boxes, type the credentials for your domain user account and click *Next*. The Verify Computer Description page appears.

CAUTION **The user name and password you supply on this page must be for a domain account created using the Windows SBS Console, not the local account created during the workstation installation.**


Connect Computer

Verify computer description

You can keep the current name of this computer, or you can change the name.

Name of this computer

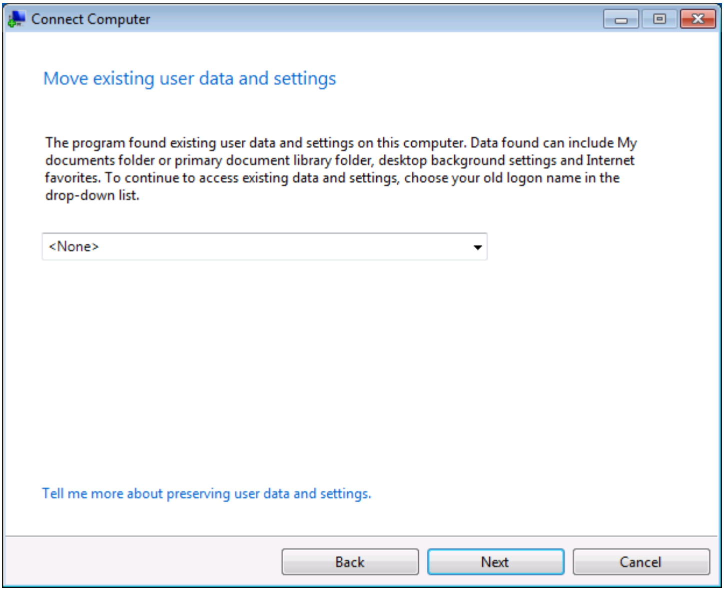
CLI1

Description of this computer

Should I change the description of this computer?

9. The computer's current name appears in the *Name of this computer* text box. You can leave it as is, or change the name and add a description, as desired. Then click *Next*. The Move Existing User Data And Settings page appears.

TIP **Computer names can be no more than 15 characters long; are not case sensitive; and can consist only of letters, numbers, and the underscore and hyphen characters.**



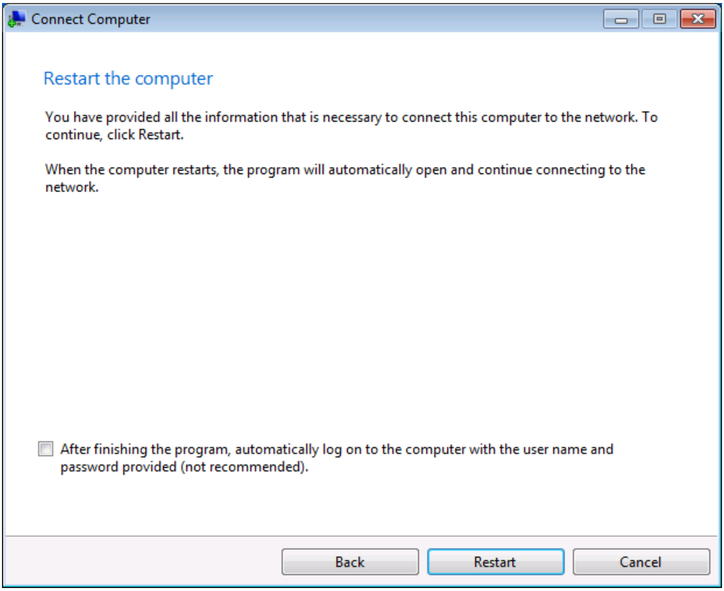
Move existing user data and settings

The program found existing user data and settings on this computer. Data found can include My documents folder or primary document library folder, desktop background settings and Internet favorites. To continue to access existing data and settings, choose your old logon name in the drop-down list.

<None>

Tell me more about preserving user data and settings.

10. If the computer has documents and settings on it that you want to retain, select the local account name from the drop-down list and click *Next*. The Confirm Your User Data And Settings Selection page appears.
11. Click *Next* to continue. The Restart The Computer page appears.



Restart the computer

You have provided all the information that is necessary to connect this computer to the network. To continue, click Restart.

When the computer restarts, the program will automatically open and continue connecting to the network.

□ After finishing the program, automatically log on to the computer with the user name and password provided (not recommended).

12. Click *Restart*. The system restarts, completes the setup process, and restarts again.
13. Log on using your domain user account. The Connect Computer Complete page appears.
14. Click *Finish*. The wizard closes, the computer appears in the *Computers* list on the Network page of the Windows SBS Console, and the workstation is now ready to use.

The Connect Computer Wizard performs a variety of configuration changes on the workstation, including the following:

- The wizard joins the computer to the AD DS domain, creating a new computer object in the MyBusiness\Computers\SBSComputers OU and adding it to the Domain Computers group.
- The wizard installs the Windows SBS 2011 ClientAgent and Windows Management Instrumentation (WMI) Provider components on the workstation.
- The wizard adds the domain user account to the local Administrators and Remote Desktop Users groups.
- Using Group Policy settings, the wizard configures the Windows Update client on the workstation to download new updates from WSUS on the Windows SBS 2011 server and install them automatically every day at 3 A.M.
- The wizard sets the Home page in Internet Explorer to the server's Internal website and creates a Windows SBS group o the Start menu, also containing a shortcut to that site.
- The wizard creates entries in the Internet Explorer Favorites list for the Internal website, Outlook Web Access, and Remote Web Access.
- The wizard opens selected ports in the Windows Firewall configuration to allow the workstation to send and receive the traffic associated with the Windows core networking, file and printer sharing, WMI, Remote Desktop, and Remote Assistance features.

Assigning Computers to Users

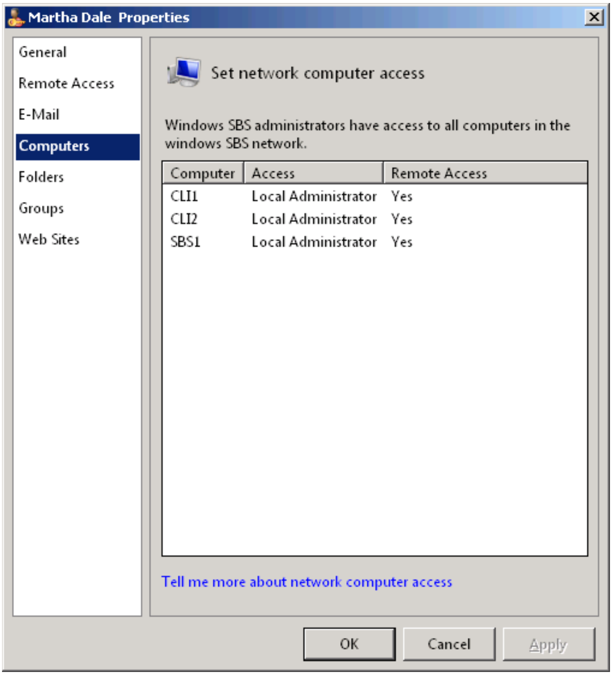
Although Windows SBS 2011 recommends that you create user accounts for your network users before you connect their workstations, it is possible to assign a new user account to an existing workstation. To do this, you must grant the user account the permissions that it needs to access the computer.

The Windows SBS Console enables you to approach this task by modifying the properties of either the user or the computer. Modifying the user properties enables you to grant a single user access to multiple computers, while modifying the computer's properties enables you to grant Computer access to multiple users.

Modifying a User's Computer Properties

To grant a user access to a computer, use the following procedure:

1. Log on to your Windows SBS 2011 primary server, using an account with network Administrator privileges. The Windows SBS Console appears.
2. Click *Users and groups* and make sure the *Users* tab is selected.
3. Select one of the user accounts on the page and, in the *Tasks* list, click *Edit user account properties*. The Properties sheet for the user account appears.
4. Select the *Computers* tab.



Set network computer access

Windows SBS administrators have access to all computers in the windows SBS network.

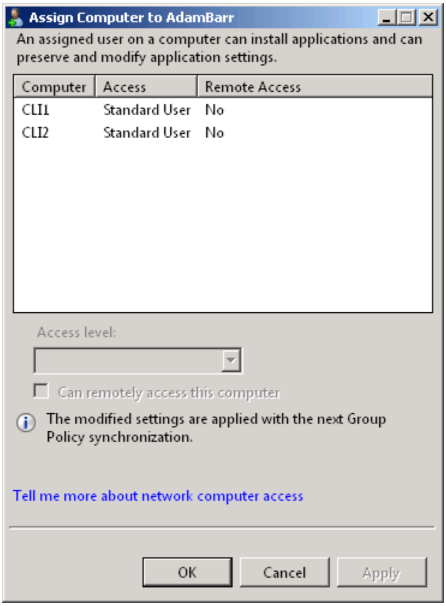
Computer	Access	Remote Access
CLI1	Local Administrator	Yes
CLI2	Local Administrator	Yes
SBS1	Local Administrator	Yes

Tell me more about network computer access

5. Select the computer that you want the user to access.
6. In the *Access level* drop-down list, specify which of the following permissions you want the user to have:
   - **Standard user** Enables the user to run most of the applications installed on the computer but prevents the user from making changes that can affect other users, including installing or uninstalling most hardware and software components, deleting system and application files, and modifying many configuration settings.
   - **Local administrator** Enables the user to make changes that affect other users, such as creating and deleting local user accounts, modifying security settings, and installing and uninstalling hardware and software.

7. Select the *Can remotely access this computer* check box if you want the user to be able to access the computer using Remote Web Access or a VPN connection.
8. Click *OK* to close the Properties sheet.

To assign a computer to a user immediately after you create the user account, you can also click the *Assign an existing computer* link on the final page of the Add A New User Account Wizard. This displays a stand-alone Assign Computer dialog box that contains the same interface as the *Computers* tab, as shown in Figure 6-17.



Assign Computer to AdamBarr

An assigned user on a computer can install applications and can preserve and modify application settings.

Computer	Access	Remote Access
CLI1	Standard User	No
CLI2	Standard User	No

The modified settings are applied with the next Group Policy synchronization.

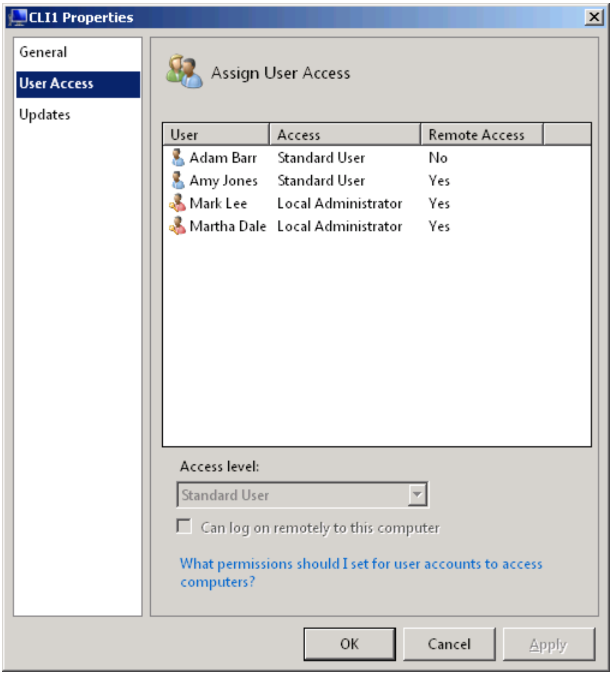
Access level:
□ Can remotely access this computer
Tell me more about network computer access
OK
Cancel
Apply

FIGURE 6-17 The Assign Computer dialog box.

Modifying a Computer's User Properties

To approach the task from the computer side, use the following procedure:

1. Log on to your Windows SBS 2011 primary server, using an account with network Administrator privileges. The Windows SBS Console appears.
2. Click *Network* and make sure the *Computers* tab is selected.
3. Select one of the computers on the page; in the *Tasks* list, click *View computer properties*. The Properties sheet for the computer appears.
4. Select the *User access* tab.


CLI1 Properties

Assign User Access

User	Access	Remote Access
Adam Barr	Standard User	No
Amy Jones	Standard User	Yes
Mark Lee	Local Administrator	Yes
Martha Dale	Local Administrator	Yes

Access level: Standard User

□ Can log on remotely to this computer

What permissions should I set for user accounts to access computers?

5. Select the user that you want to grant access to the computer.
6. In the *Access level* drop-down list, specify which of the following permissions you want the user to have:
   - **Standard user** Enables the user to run most of the applications installed on the computer, but prevents the user from making changes that can affect other users, including installing or uninstalling most hardware and software components, deleting system and application files, and modifying many configuration settings.
   - **Local administrator** Enables the user to make changes that affect other users, such as creating and deleting local user accounts, modifying security settings, and installing and uninstalling hardware and software.
7. Select the *Can log on remotely to this computer* check box if you want the user to be able to access the computer using Remote Web Access or a VPN connection.
8. Click *OK* to close the Properties sheet.

Working with Groups

Internal security in Windows SBS 2011 is largely based on permissions. *Permissions* specify which Windows SBS 2011 resources a user is permitted to access and how much access the user receives. By the time you complete your Windows SBS 2011 deployment, the server and workstations have granted your users permissions for hundreds of files, folders, printers, AD DS objects, and registry settings automatically. Assigning permissions is a regular part of a network administrator's job, but fortunately Windows SBS 2011 simplifies the process by enabling you to assign permissions to groups instead of individual users.

In Windows SBS 2011, a *group* is an AD DS object that functions as a proxy for all the other objects that the group has as its members. When you assign permissions to a group, all the group's members receive those permissions as well. The groups that Windows SBS 2011 creates by default are based on specific network functions and resources. For example, the Windows SBS Remote Web Access Users group has the permissions needed for users to access computers on the network using the Remote Web Access (RWA) interface from a remote location. When you grant a user RWA access to a computer, the Windows SBS Console simply has to add the user object to the Windows SBS Remote Web Access Users group rather than assign all the necessary permissions to each individual user account.

Group memberships are completely independent of the AD DS hierarchy. You can add objects from any container in the domain to a group. If you choose to expand the AD DS tree by creating your own OUs, you can move user objects to other OUs as needed and they remain members of their groups.

Groups can also have other groups as members, a practice called *group nesting*. When you make one group a member of another group, the permissions you assign to the top-level group flow downward through the second-level group to its members as well.

> ***NOTE*** **Windows Server 2008 R2 supports three group scopes: domain local, global, and universal. In a stand-alone Windows Server 2008 R2 installation, group nesting is subject to certain limitations, based on the group scopes and other AD DS settings. However, Windows SBS 2011 simplifies the matter. All the groups that Windows SBS 2011 creates by default are universal groups, and any universal group can be a member of any other universal group. When you create groups in the Windows SBS Console, you have no choice but to create universal groups. To create domain local or global groups, you must use the Active Directory Users And Computers Console.**

Windows SBS 2011 supports two group types, as follows:

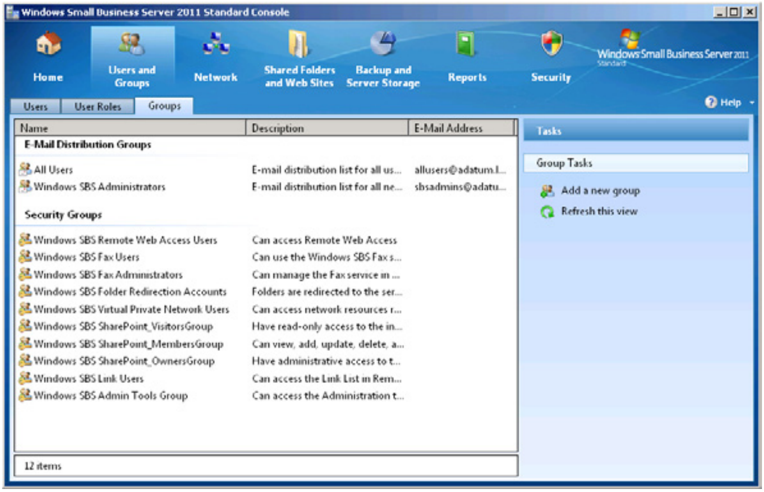
- **Security groups** Administrators use security groups to control access to network resources. Assigning permissions to a security group gives every member of the group all those permissions.
- **Distribution groups** Distribution groups, which are essentially mailing lists, enable users to send email to all members of the group at once.

Creating a New Group

You can create your own groups to control access to your network resources as needed. For example, you might want to create a group with limited access permissions called New Hires, which you use for individuals that have just joined the company. Instead of having to assign permissions to each new user object, you can simply add the users to the New Hires group. Once a user passes the probationary stage, you can give them greater access by simply moving them to other groups.

To create a new group in the Windows SBS Console, use the following procedure:

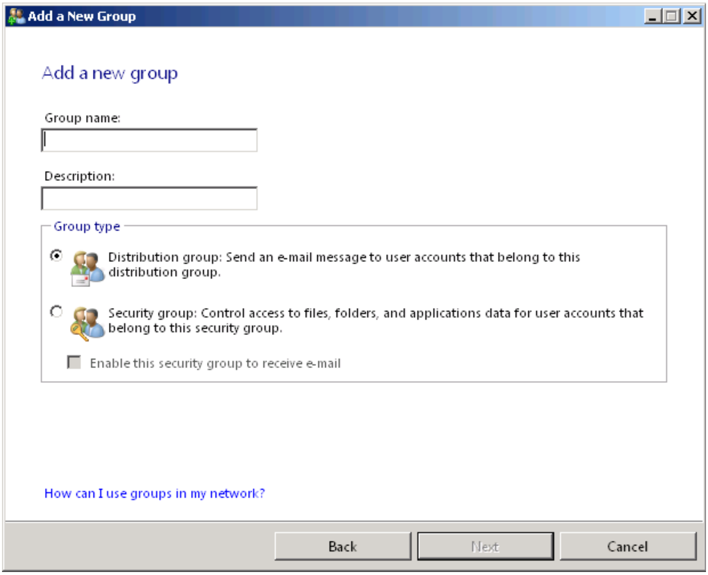
1. Log on to your Windows SBS 2011 primary server, using an account with network Administrator privileges. The Windows SBS Console appears.
2. Click *Users and groups*, and select the *Groups* tab.


Windows Small Business Server 2011 Standard Console
Home
Users and Groups
Network
Shared Folders and Web Sites
Backup and Server Storage
Reports
Security
Windows Small Business Server 2011 Standard
Users
User Roles
Groups
Help
Tasks
Group Tasks
Add a new group
Refresh this view

Name	Description	E-Mail Address
E-Mail Distribution Groups		
All Users	E-mail distribution list for all us...	allusers@adatum.l...
Windows SBS Administrators	E-mail distribution list for all ne...	sbsadmins@adatu...
Security Groups		
Windows SBS Remote Web Access Users	Can access Remote Web Access	
Windows SBS Fax Users	Can use the Windows SBS Fax s...	
Windows SBS Fax Administrators	Can manage the Fax service in ...	
Windows SBS Folder Redirection Accounts	Folders are redirected to the ser...	
Windows SBS Virtual Private Network Users	Can access network resources r...	
Windows SBS SharePoint_VisitorsGroup	Have read-only access to the in...	
Windows SBS SharePoint_MembersGroup	Can view, add, update, delete, a...	
Windows SBS SharePoint_OwnersGroup	Have administrative access to t...	
Windows SBS Link Users	Can access the Link List in Rem...	
Windows SBS Admin Tools Group	Can access the Administration t...	

12 items

3. In the *Tasks* list, click *Add a new group*. The Add A New Group Wizard appears, displaying the Getting Started page.
4. Click *Next* to continue. The Add A New Group page appears.



Add a new group

Group name:

Description:

Group type

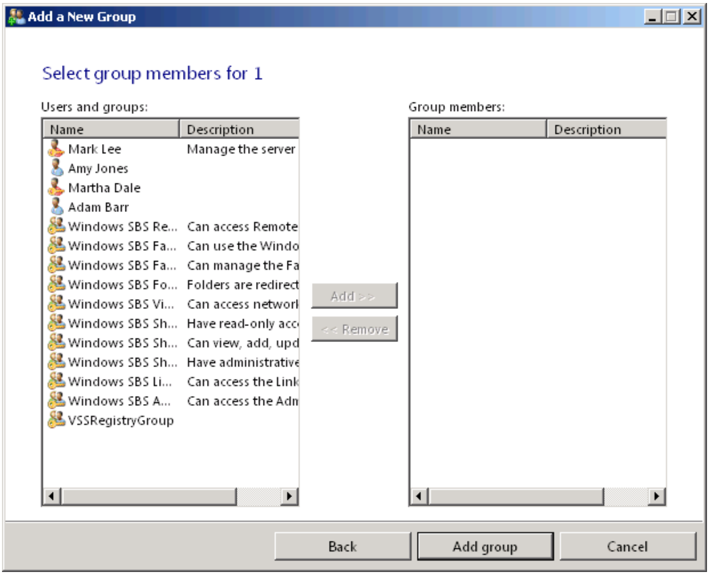
● Distribution group: Send an e-mail message to user accounts that belong to this distribution group.

○ Security group: Control access to files, folders, and applications data for user accounts that belong to this security group.

□ Enable this security group to receive e-mail

How can I use groups in my network?

5. In the *Group name* text box, type the name that you want to assign to the group. Type some informational text in the *Description* text box, if desired.
6. Select the type of group that you want to create. If you choose the *Security Group* option, specify whether you want to be able to send email to the group by selecting the *Enable this security group to receive e-mail* check box.
7. Click *Next*. The Select Group Members For 1 page appears.



Select group members for 1

Users and groups:

Name	Description
Mark Lee	Manage the server
Amy Jones	
Martha Dale	
Adam Barr	
Windows SBS Re...	Can access Remote
Windows SBS Fa...	Can use the Windo
Windows SBS Fa...	Can manage the Fa
Windows SBS Fo...	Folders are redirect
Windows SBS Vi...	Can access networl
Windows SBS Sh...	Have read-only acc
Windows SBS Sh...	Can view, add, upd
Windows SBS Sh...	Have administrative
Windows SBS Li...	Can access the Link
Windows SBS A...	Can access the Adn
VSSRegistryGroup	

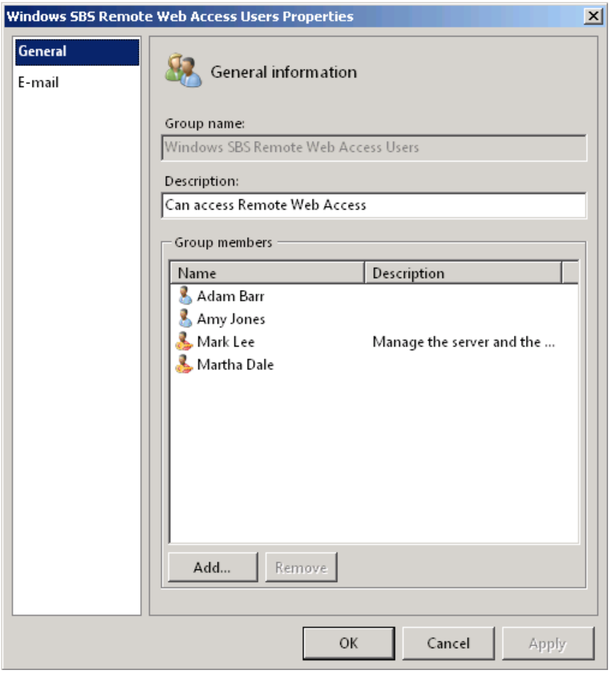
Group members:

Name	Description

8. In the *Users and groups* list, select the users and groups that you want to add as members of the new group and click *Add*.
9. Click *Add group*. The wizard creates the group and the A New Group Has Successfully Been Added To The Network page appears.
10. Click *Finish*. The wizard closes.

Managing Group Memberships

Once you have created the user and group objects that you need, you can manage your group memberships in two ways: by opening the Properties sheet for a user object and selecting the desired groups, as shown earlier in this chapter, or by opening a group's Properties sheet and selecting the desired users, as shown in Figure 6-18.



Group name: Windows SBS Remote Web Access Users

Description: Can access Remote Web Access

Group members

Name	Description
Adam Barr	
Amy Jones	
Mark Lee	Manage the server and the ...
Martha Dale	

FIGURE 6-18 The *General* tab in a group's Properties sheet.

CHAPTER 7

Managing Disks

Windows Small Business Server (SBS) 2011 includes a number of tools that administrators can use to install and manage hard disks and create volumes on those disks. In this chapter, you'll explore such disk utilities as the Windows SBS 2011 Setup program, the Disk Management snap-in, and the Diskpart.exe command-line program. Later, in Chapter 9, "Managing Storage," you'll learn how to create shares on the volumes, so that users can access them over the network.

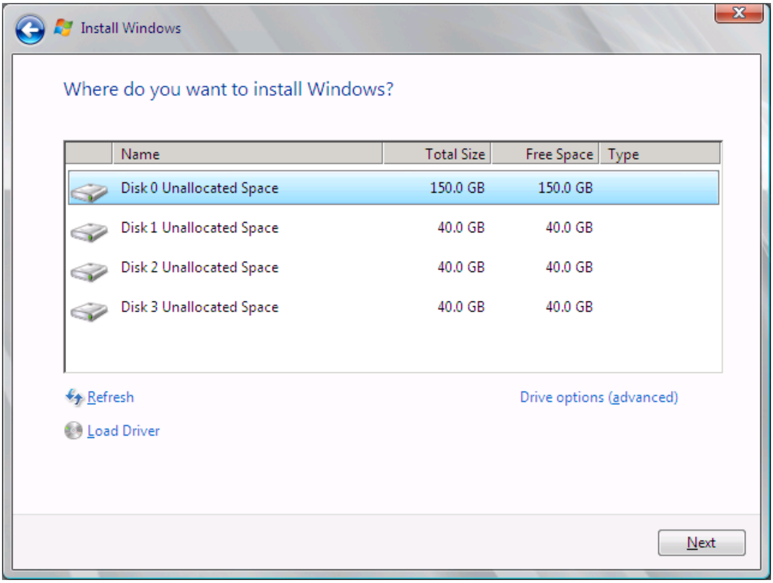
> ***NOTE*** **There is a good deal of vocabulary involved when working with disks in Windows SBS 2011. Terms such as *disk*, *partition*, and *volume* can refer to the same resources at different times, but they are not necessarily interchangeable. Be sure to observe the differences as they are used in the text.**

Working with Disks During Installation

Before you can store data on a Windows SBS 2011 hard disk, you must create at least one volume on it. You create your first volume, which becomes the C drive, during the operating system installation process, and Windows SBS 2011 uses that volume to store all the default system, application, and data files. Although it is possible to create additional simple volumes from within the setup program, many administrators wait until after the installation process is complete. You must also wait if you want to create non-simple volumes, such as mirror sets and RAID-5 arrays.

Loading Disk Drivers During Installation

The first opportunity that you have to manipulate the storage subsystem on a server running Windows SBS 2011 is during the installation of the Windows Server 2008 R2 operating system. When the Where Do You Want To Install Windows? page appears, as shown in Figure 7-1, it displays all the disks that the setup program was able to locate using the device drivers supplied with Windows.



Where do you want to install Windows?

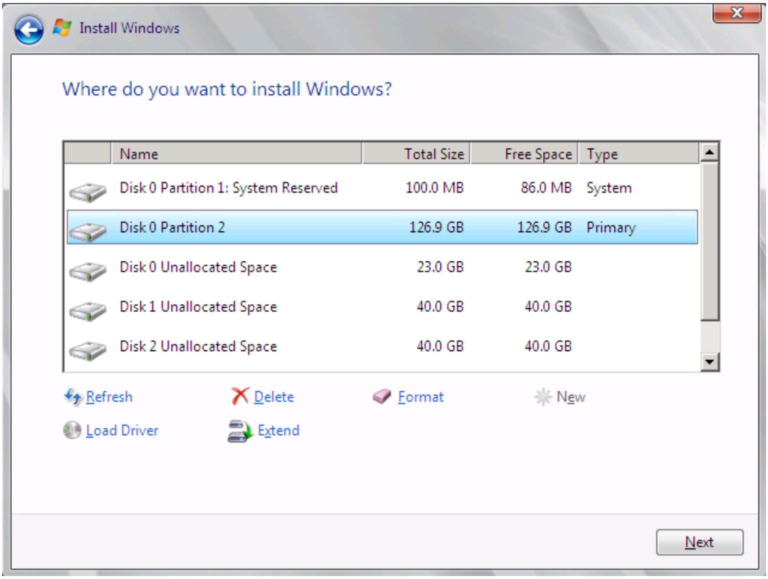
Name	Total Size	Free Space	Type
Disk 0 Unallocated Space	150.0 GB	150.0 GB	
Disk 1 Unallocated Space	40.0 GB	40.0 GB	
Disk 2 Unallocated Space	40.0 GB	40.0 GB	
Disk 3 Unallocated Space	40.0 GB	40.0 GB	

FIGURE 7-1 The Where Do You Want To Install Windows? page of the Windows Server 2008 R2 setup program.

Windows Server 2008 R2 ships with a large collection of disk drivers, and if you purchase an original equipment manufacturer (OEM) version of Windows SBS 2011, that collection might be augmented with drivers for the specific hardware included in the computer. The result, in the majority of cases, is that you can see the disks in the computer during the installation without any special manipulation.

There are times when this is not the case, however. If the Where Do You Want To Install Windows? page should appear with some or all of the computer's disks missing, this means that the system lacks the drivers it needs to access some or all of the storage subsystem.

If your computer has a drive or array that Windows does not support with its included drivers, you can at this point load additional drivers yourself by clicking the *Drive options (advanced)* link. The additional controls that appear, as shown in Figure 7-2, include a *Load driver* link that enables you to supply a CD, DVD, or flash drive containing driver files that you have obtained from the manufacturer of your hardware.



Name	Total Size	Free Space	Type
Disk 0 Partition 1: System Reserved	100.0 MB	86.0 MB	System
Disk 0 Partition 2	126.9 GB	126.9 GB	Primary
Disk 0 Unallocated Space	23.0 GB	23.0 GB	
Disk 1 Unallocated Space	40.0 GB	40.0 GB	
Disk 2 Unallocated Space	40.0 GB	40.0 GB	

FIGURE 7-2 The additional controls on the Where Do You Want To Install Windows? page of the Windows Server 2008 R2 setup program.

Creating Volumes During Installation

By default, selecting a disk during the Windows Server 2008 R2 setup process causes the program to utilize the entire disk to create a small system volume and a C volume, on which it installs the entire Windows SBS 2011 environment.

However, the additional controls on the Where Do You Want To Install Windows? page also enable you to create your own volume for the installation, using only part of an existing disk. If, for example, your server has a single 500 gigabyte (GB) disk drive in it, you might want to create a 150 GB volume for the Windows SBS installation and save the rest for data storage you might need at a later time.

The main restriction on these volume controls is that you cannot create anything other than a simple volume during the Windows Server 2008 R2 installation. Therefore, you cannot create a mirrored, spanned, striped, or redundant array of independent disks (RAID) volume and use it for your Windows SBS 2011 installation. If you want to use these advanced volume types to protect your data, you must wait until the installation is complete, create the volume using the Disk Management snap-in or the Diskpart.exe utility, and then move your data to the protected volume.

MORE INFO **For more information on creating fault tolerant volumes, see "Creating Volumes," later in this chapter.**

Managing Disk Storage

You must create at least one volume during the Windows SBS 2011 installation, but after the installation is complete, you can create as many additional volumes as you need. You might have additional space to work with on the disk containing your C drive, and you might have additional disks already installed in the computer. You can also install additional disk storage on your server by adding internal disk drives, connecting external drives, or deploying network-based storage devices. Once your server recognizes the new storage devices, you can create and manage volumes using the tools and procedures discussed in the following sections.

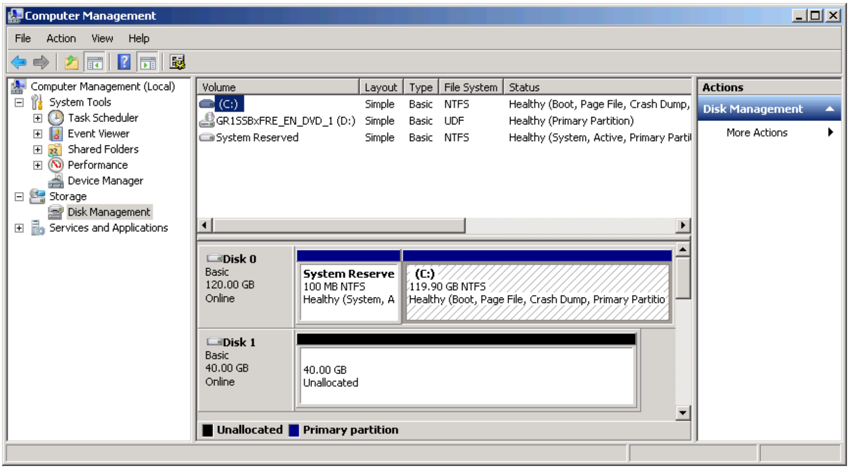
Using the Disk Management Interface

The primary Windows tool for managing disk partitions and volumes is the Disk Management snap-in for Microsoft Management Console (MMC). Disk Management is not a Windows SBS 2011 tool; all Windows versions include it as part of the Computer Management Console. As with all MMC snap-ins, however, you can create a custom MMC Console that combines Disk Management with any other snap-ins you use regularly.

To access the Disk Management snap-in, you can use any of the following procedures:

- Click *Start* > *Administrative Tools* > *Computer Management* and select the *Storage/Disk management* node.
- Click *Start* > *Administrative Tools* > *Server Manager* and select the *Storage/Disk management* node.
- Click *Start*. Then click *Run* and execute the Diskmgmt.msc file.
- Click *Start*. Then click *Run* and execute the Mmc.exe file. Select *File* > *Add/Remove Snap-in* and add *Disk management* to the console.

When you open the Disk Management snap-in, you see the default interface shown in Figure 7-3.

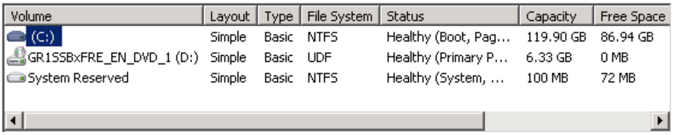


Volume	Layout	Type	File System	Status
(C:)	Simple	Basic	NTFS	Healthy (Boot, Page File, Crash Dump,
GR1SSBxFRE_EN_DVD_1 (D:)	Simple	Basic	UDF	Healthy (Primary Partition)
System Reserved	Simple	Basic	NTFS	Healthy (System, Active, Primary Parti

FIGURE 7-3 The Disk Management snap-in.

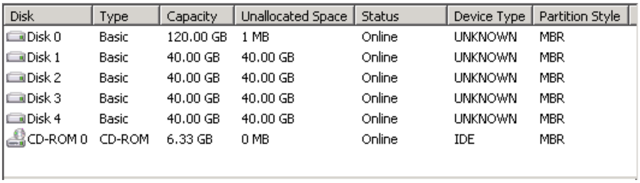
The two center panes in the console, called Top and Bottom, can each display one of the following three views:

- **Disk list** Lists the physical drives installed in the computer and displays the disk number; disk type, such as Basic or DVD; disk capacity; unallocated space; current status, such as online, offline, or no media; the device type, such as SCSI or IDE; and the partition style, such as MBR or GPT.



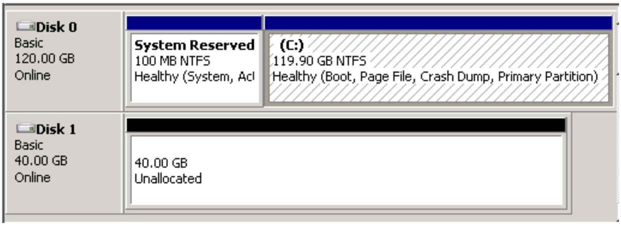
Volume	Layout	Type	File System	Status	Capacity	Free Space
(C:)	Simple	Basic	NTFS	Healthy (Boot, Pag...	119.90 GB	86.94 GB
GR1SSBxFRE_EN_DVD_1 (D:)	Simple	Basic	UDF	Healthy (Primary P...	6.33 GB	0 MB
System Reserved	Simple	Basic	NTFS	Healthy (System, ...	100 MB	72 MB

- **Volume list** Lists the volumes on all the computer's disks and displays the volume name; layout, such as Simple, Spanned, or Striped; the disk type, such as Basic or Dynamic; the file system, such as NTFS or Compact Disk File System (CDFS); the disk status, such as Healthy, Failed, or Formatting; and information about the disk's capacity and its current free space.



Disk	Type	Capacity	Unallocated Space	Status	Device Type	Partition Style
Disk 0	Basic	120.00 GB	1 MB	Online	UNKNOWN	MBR
Disk 1	Basic	40.00 GB	40.00 GB	Online	UNKNOWN	MBR
Disk 2	Basic	40.00 GB	40.00 GB	Online	UNKNOWN	MBR
Disk 3	Basic	40.00 GB	40.00 GB	Online	UNKNOWN	MBR
Disk 4	Basic	40.00 GB	40.00 GB	Online	UNKNOWN	MBR
CD-ROM 0	CD-ROM	6.33 GB	0 MB	Online	IDE	MBR

- **Graphical view** Contains a graphical representation of the computer's physical disks, partitions, volumes, and logical drives. The disk status column (on the left) displays the disk number plus its type, capacity, and status. The volume status column (on the right) displays the name, size, file system, and current status for each volume on the disk.



Disk 0
Basic
120.00 GB
Online

System Reserved
100 MB NTFS
Healthy (System, Act

(C:)
119.90 GB NTFS
Healthy (Boot, Page File, Crash Dump, Primary Partition)

Disk 1
Basic
40.00 GB
Online

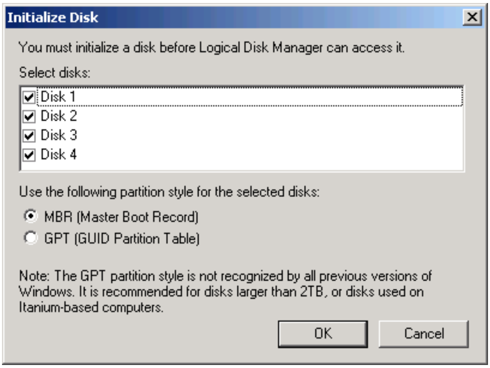
40.00 GB
Unallocated

The default interface contains the volume list in the top pane and the graphical view in the bottom. You can modify these defaults as desired. Right-clicking an element in any of the three panes displays a context menu containing commands for managing the selected element.

Initializing a Disk

When you install a new hard disk in your server, or access one for the first time, the first thing you must do is initialize it by selecting a partition style. To initialize a disk, perform the following procedure:

1. Click *Start*. Then click *Administrative Tools* > *Computer Management*. The Computer Management Console appears.
2. In the Scope (left) pane, select the *Disk management* node. The Initialize Disk dialog box appears.



Initialize Disk

You must initialize a disk before Logical Disk Manager can access it.

Select disks:

☑ Disk 1
☑ Disk 2
☑ Disk 3
☑ Disk 4

Use the following partition style for the selected disks:

● MBR (Master Boot Record)
○ GPT (GUID Partition Table)

Note: The GPT partition style is not recognized by all previous versions of Windows. It is recommended for disks larger than 2TB, or disks used on Itanium-based computers.

3. Select one of the following partition styles for the new disk:
   - **MBR (Master Boot Record)** The default partition style, supporting up to four partitions and volumes up to 2 terabytes (TB) in size
   - **GPT (GUID Partition Table)** Supports up to 128 partitions and volumes as large as 18 exabytes (18 x 260 bytes)
4. Click *OK*. The Disk Management interface appears, with the new disk appearing as unallocated space.

Once you have initialized the disk, you can proceed to create volumes on it.

Creating Volumes

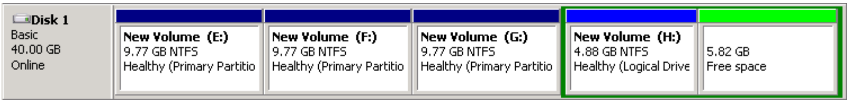
Windows SBS 2011 supports five volume types, as described in Table 7-1. These volume types provide varying amounts of fault tolerance and performance enhancement. The volumes you created during the Windows SBS 2011 installation are simple volumes, and because the volumes contain the computer's boot and system files, they must remain that way. However, you can use any unallocated space on the system disk, plus the space on your other disks, to create volumes of any type.

TABLE 7-1 Volume Types Supported by Windows SBS 2011

VOLUME TYPE	NUMBER OF DISKS REQUIRED	FAULT TOLERANCE	DESCRIPTION
Simple	1	None.	Consists of space from a single disk.
Spanned	2 to 32	None. The loss of one disk destroys the volume.	Consists of space from multiple dynamic disks, combined to create a single volume.
Striped	2 to 32	None. The loss of one disk destroys the volume.	Consists of space from multiple dynamic disks, combined to create a single volume. The system writes data one stripe at a time to each successive disk in the volume, increasing input/output (I/O) efficiency.
Mirrored	2	Yes. The volume survives the loss of one disk.	Consists of an identical amount of space on two disks. The system writes duplicate copies of all data to both of the disks, so that all the data remains available if one disk fails. The volume size therefore equals half of the total disk space.

VOLUME TYPE	NUMBER OF DISKS REQUIRED	FAULT TOLERANCE	DESCRIPTION
RAID-5	3 or more	Yes. The volume survives the loss of one disk.	Consists of space on at least three disks. The system stripes data, along with parity information, across the disks. If one disk should fail, the system can reconstruct the missing data using the parity information on the other disks.

In addition to the volume types, Windows SBS 2011 supports two disk types: basic disks and dynamic disks. When you first initialize a disk, it appears as a basic disk. A *basic disk* can have up to four partitions: three primary partitions and one extended partition, with the extended partition hosting multiple logical drives. As long as you create only simple volumes on a disk, it remains a basic disk. The first three simple volumes you create on a basic disk are the primary partitions. When you create a fourth simple volume, the Disk Management snap-in creates an extended partition using all the remaining unallocated space on the disk, and a logical drive of the size you specified for the simple volume, as shown in Figure 7-4.



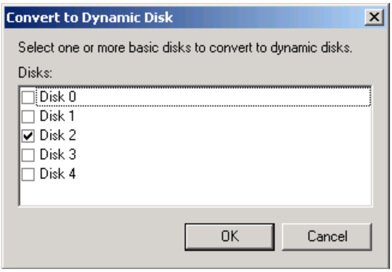
Disk 1 Basic 40.00 GB Online	New Volume (E:) 9.77 GB NTFS Healthy (Primary Partitio	New Volume (F:) 9.77 GB NTFS Healthy (Primary Partitio	New Volume (G:) 9.77 GB NTFS Healthy (Primary Partitio	New Volume (H:) 4.88 GB NTFS Healthy (Logical Drive	5.82 GB Free space

FIGURE 7-4 An extended partition and logical drive in the Disk Management snap-in.

> ***TIP*** **It is possible to create a fourth primary partition on a basic disk, but you cannot do it using the Disk Management snap-in. Instead, you must use the Diskpart.exe tool from the command prompt.**

To create volumes other than simple volumes, you must convert the disks into dynamic disks. Technically, a *dynamic disk* has one partition that uses all its available space. You can then create multiple volumes within that single partition. When you use basic disks to create a spanned, striped, mirrored, or RAID-5 volume using the Disk Management snap-in, the tool converts the disks from basic to dynamic automatically. If you delete all the volumes on a dynamic disk (erasing the data on them), Disk Management automatically converts it back to a basic disk.

The Disk Management snap-in enables you to convert a basic disk into a dynamic disk manually, by right-clicking a disk and using the interface shown in Figure 7-5, although this usually is not necessary.



Convert to Dynamic Disk

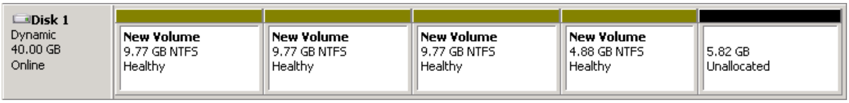
Select one or more basic disks to convert to dynamic disks.

Disks:

- □ Disk 0
- □ Disk 1
- ☑ Disk 2
- □ Disk 3
- □ Disk 4

FIGURE 7-5 The Convert To Dynamic Disk dialog box.

When you convert a basic disk with partitions on it to a dynamic disk, the snap-in converts each partition to a simple volume, as shown in Figure 7-6. There is a corresponding command to convert a dynamic disk back to a basic disk, but it only appears when there are no volumes on the dynamic disk. Therefore, the only way to convert a dynamic disk to a basic disk is to delete all its data.



Disk 1
Dynamic
40.00 GB
Online

New Volume 9.77 GB NTFS Healthy	New Volume 9.77 GB NTFS Healthy	New Volume 9.77 GB NTFS Healthy	New Volume 4.88 GB NTFS Healthy	5.82 GB Unallocated

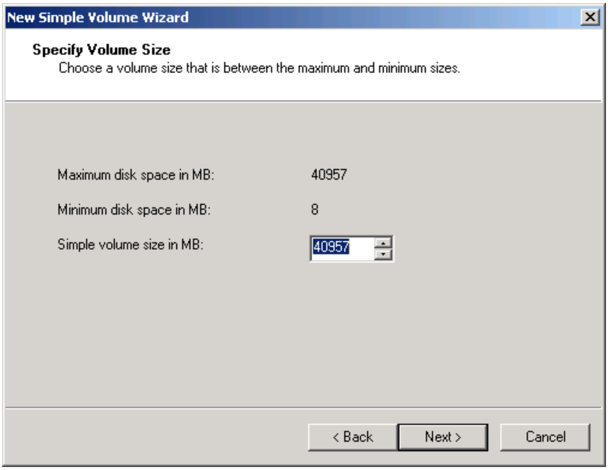
FIGURE 7-6 Basic disk partitions become dynamic disk volumes.

> ***CAUTION*** **The only drawback to using dynamic disks is that you cannot boot the computer from any volume on a dynamic disk other than the current boot volume. This prevents you from using a technique called *dual-booting* to run two operating systems on the same computer. This is not a serious problem for most users, as virtualization technology has rendered dual-booting obsolete in most cases.**

Creating a Simple Volume

To create a simple volume with the Disk Management snap-in, perform the following procedure:

1. Click *Start*. Then click *Administrative Tools > Computer Management*. The Computer Management Console appears.
2. In the Scope (left) pane, select the *Disk management* node.
3. In the graphical view, right-click the unallocated space on any of your disks; from the context menu, select *New simple volume*. The New Simple Volume Wizard appears.
4. Click *Next* to bypass the Welcome page. The Specify Volume Size page appears.



New Simple Volume Wizard

Specify Volume Size

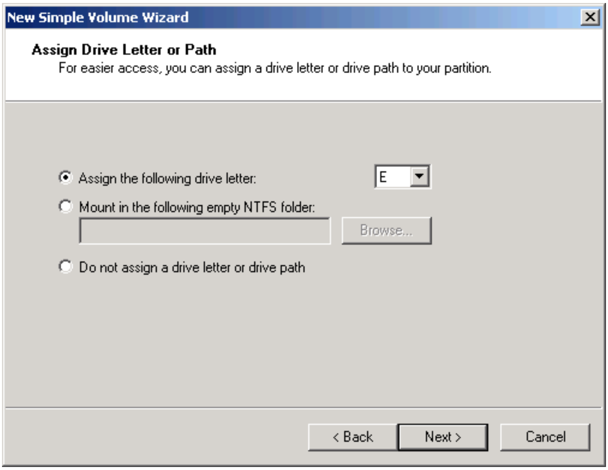
Choose a volume size that is between the maximum and minimum sizes.

Maximum disk space in MB: 40957

Minimum disk space in MB: 8

Simple volume size in MB: 40957

5. In the *Simple volume size in MB* box, specify the size of the volume you want to create and click *Next*. The Assign Drive Letter Or Path page appears.



New Simple Volume Wizard

Assign Drive Letter or Path

For easier access, you can assign a drive letter or drive path to your partition.

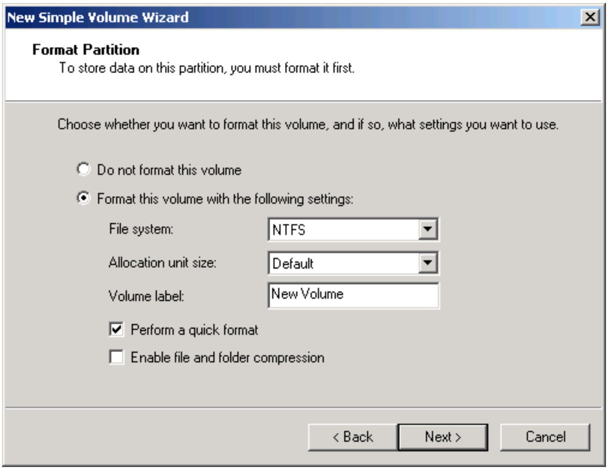
● Assign the following drive letter: E

○ Mount in the following empty NTFS folder:

○ Do not assign a drive letter or drive path

6. Select one of the following options and configure its properties:
   - **Assign the following drive letter** Enables you to select the available drive letter you want to use to access the volume.
   - **Mount in the following empty NTFS folder** Enables you to access the new volume from within a folder on another existing volume. This makes the new volume appear in the specified folder, as though it is part of the existing volume.
   - **Do not assign a drive letter or drive path** Enables you to create the new volume without any means of accessing it. You can assign a drive letter or mount the volume to a folder at a later time.

7. Click *Next*. The Format Partition page appears.


New Simple Volume Wizard

Format Partition

To store data on this partition, you must format it first.

Choose whether you want to format this volume, and if so, what settings you want to use.

○ Do not format this volume

● Format this volume with the following settings:

File system: NTFS

Allocation unit size: Default

Volume label: New Volume

☑ Perform a quick format

□ Enable file and folder compression

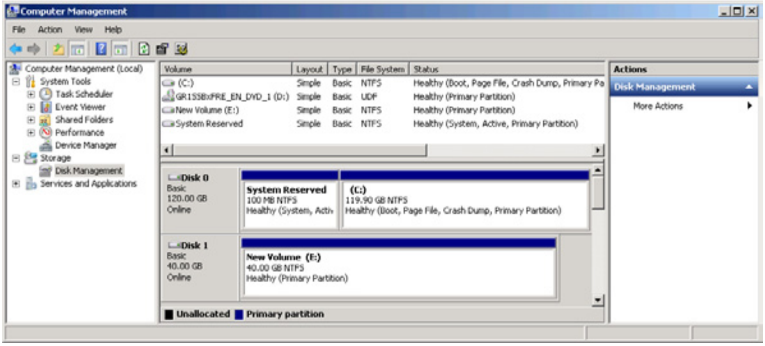
8. To format the volume, leave the *Format the volume with the following settings* option selected and configure the following properties:

   - **File system** Specifies whether you want to format the volume using the NTFS, FAT, FAT32, or exFAT file system. NTFS provides many more features than any of the file allocation table (FAT) options, including access control, compression, and encryption. The only compelling reason to use FAT or FAT32 is if you must access the volume using an operating system that does not support NTFS. The exFAT file system is a new, 64-bit version designed for use on USB flash drives.
   - **Allocation unit size** Specifies the size of the individual clusters the system uses when allocating space on the volume. For a volume that stores a great many small files, a smaller value provides more efficient use of disk space; for a volume that stores extremely large files, a greater value provides better performance. For most applications, however, the default setting is preferable.
   - **Volume label** Specifies a name, up to 32 characters long, that the system uses to identify the volume.
   - **Perform a quick format** Selecting this check box causes the wizard to format the volume without checking for errors. Clearing the check box causes the wizard to check the disk for errors as it formats the volume and mark bad sectors as inaccessible. The time required for the error checking depends on the size of the drive. For large drives, it can be a lengthy process.

- **Enable file and folder compression** Selecting this check box along with the NTFS file system causes the computer to store all the data it writes on the volume in a compressed form. This provides additional storage space on the disk, but also places an additional burden on the system processor, which is responsible for performing all of the real-time compressions and decompressions.

NOTE **You can turn compression on and off for a volume at any time, from the *General* tab on the volume's Properties sheet.**

9. Click *Next*. The Completing The New Simple Volume Wizard page appears.
10. Click *Finish*. The wizard closes, and the new volume appears in the unallocated space.



Volume	Layout	Type	File System	Status
(C:)	Simple	Basic	NTFS	Healthy (Boot, Page File, Crash Dump, Primary Pa
GR1SSBxFRE_EN_DVD_1 (D:)	Simple	Basic	UDF	Healthy (Primary Partition)
New Volume (E:)	Simple	Basic	NTFS	Healthy (Primary Partition)
System Reserved	Simple	Basic	NTFS	Healthy (System, Active, Primary Partition)

Disk 0
Basic
120.00 GB
Online

System Reserved
100 MB NTFS
Healthy (System, Activ

(C:)
119.90 GB NTFS
Healthy (Boot, Page File, Crash Dump, Primary Partition)

Disk 1
Basic
40.00 GB
Online

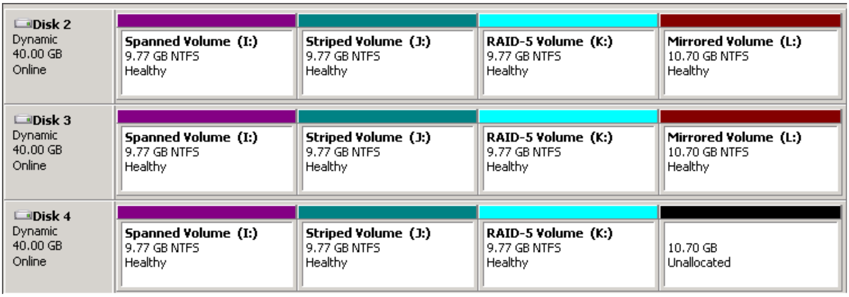
New Volume (E:)
40.00 GB NTFS
Healthy (Primary Partition)

Depending on the computer's hardware, the size of the volume, and the settings you selected, it might take several minutes for the formatting to finish.

Creating Other Volume Types

The Disk Management snap-in also includes wizards for creating spanned, striped, mirrored, and RAID-5 volumes. These wizards are identical to the New Simple Volume Wizard, except for the addition of a Select Disks page. This page enables you to select the disks you want to use to create the volume and specify the amount of space you want to use on each disk.

When the wizard finishes creating a volume, the allocated space on all of the disks involved changes color to reflect the properties of the new volume, as shown in Figure 7-7.

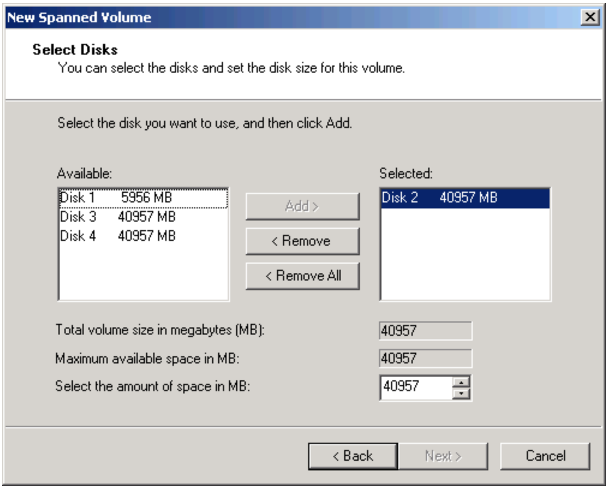


Disk 2 Dynamic 40.00 GB Online	Spanned Volume (I:) 9.77 GB NTFS Healthy	Striped Volume (J:) 9.77 GB NTFS Healthy	RAID-5 Volume (K:) 9.77 GB NTFS Healthy	Mirrored Volume (L:) 10.70 GB NTFS Healthy
Disk 3 Dynamic 40.00 GB Online	Spanned Volume (I:) 9.77 GB NTFS Healthy	Striped Volume (J:) 9.77 GB NTFS Healthy	RAID-5 Volume (K:) 9.77 GB NTFS Healthy	Mirrored Volume (L:) 10.70 GB NTFS Healthy
Disk 4 Dynamic 40.00 GB Online	Spanned Volume (I:) 9.77 GB NTFS Healthy	Striped Volume (J:) 9.77 GB NTFS Healthy	RAID-5 Volume (K:) 9.77 GB NTFS Healthy	10.70 GB Unallocated

FIGURE 7-7 New spanned, striped, mirrored, and RAID-5 volumes in the Disk Management snap-in.

Creating Spanned Volumes

When creating a spanned disk, as shown in Figure 7-8, you must select at least 2 and no more than 32 disks, and you can specify any amount of space on each disk.



New Spanned Volume

Select Disks

You can select the disks and set the disk size for this volume.

Select the disk you want to use, and then click Add.

Available:

Disk 1	5956 MB
Disk 3	40957 MB
Disk 4	40957 MB

Selected:

Disk 2	40957 MB

Total volume size in megabytes (MB): 40957

Maximum available space in MB: 40957

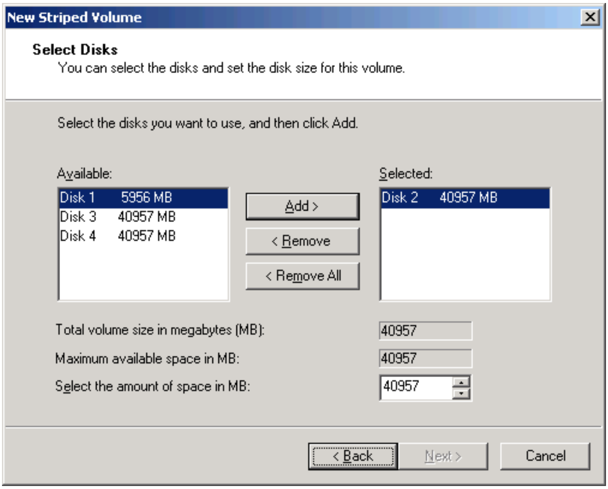
Select the amount of space in MB: 40957

FIGURE 7-8 The Select Disks page in the New Spanned Volume Wizard.

The disk you selected when creating the volume appears already in the *Selected* list, with all its available disk space allocated. You can modify the amount of space you want to devote to the drive as needed. The *Available* list contains all the other disks in the system with available space. After selecting one or more disks and clicking the *Add* button, you can modify the amount of space allocated from each additional disk as well. The *Total volume size in megabytes (MB)* indicator specifies the total amount of space on all the disks you selected.

Creating Striped Volumes

When creating a striped volume, as shown in Figure 7-9, you must select at least 2 and no more than 32 disks, and you must specify the same amount of space on each disk.



New Striped Volume

Select Disks

You can select the disks and set the disk size for this volume.

Select the disks you want to use, and then click Add.

Available:

Disk 1	5956 MB
Disk 3	40957 MB
Disk 4	40957 MB

Selected:

Disk 2	40957 MB

Total volume size in megabytes (MB): 40957

Maximum available space in MB: 40957

Select the amount of space in MB: 40957

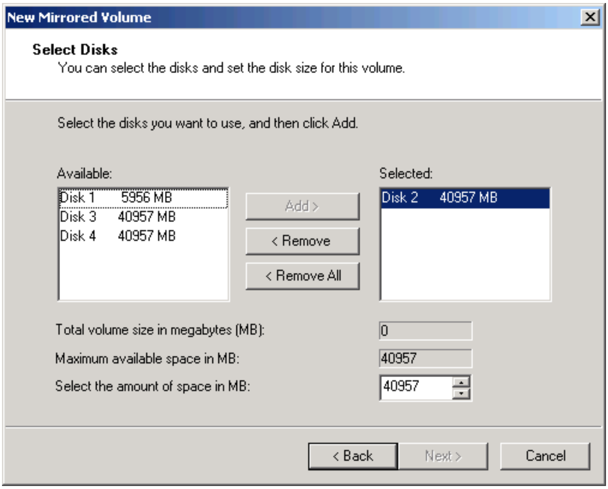
FIGURE 7-9 The Select Disks page in the New Striped Volume Wizard.

The process of selecting disks for a striped volume is essentially the same as that for a spanned volume, except that the amounts of space allocated on each disk automatically adjust themselves as needed. For example, if the disk you selected when creating the volume has 40,000 MB free, and you add a disk that has only 20,000 MB free, the wizard automatically adjusts the configuration to use 20,000 MB from both disks because all the selected disks must contribute the same amount of space. As with a spanned drive, the *Total volume size in megabytes (MB)* indicator specifies the combined allocated space in all the selected disks.

> ***CAUTION*** **As mentioned earlier, it is critical to understand that spanned and striped volumes do not add fault tolerance, and are, in fact, less fault tolerant than the other volume types. The loss of one disk in a spanned or striped volume causes the entire volume to be lost, including the data on other undamaged disks.**

Creating Mirrored Volumes

When creating a mirrored volume, as shown in Figure 7-10, you can select only two disks, and you must specify the same amount of space on each disk.


New Mirrored Volume

Select Disks

You can select the disks and set the disk size for this volume.

Select the disks you want to use, and then click Add.

Available:	Selected:
Disk 1 5956 MB	Disk 2 40957 MB
Disk 3 40957 MB	
Disk 4 40957 MB	

Total volume size in megabytes (MB):	0
Maximum available space in MB:	40957
Select the amount of space in MB:	40957

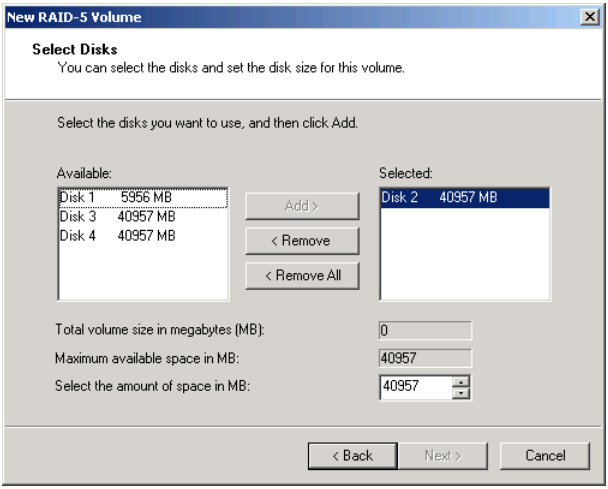
FIGURE 7-10 The Select Disks page in the New Mirrored Volume Wizard.

The Select Disks page in the New Mirrored Volume Wizard functions just as when you created a striped volume, except that you can select only two disks, and the *Total volume size in megabytes (MB)* indicator specifies the amount of space allocated on each disk, not the sum of both. A mirrored volume stores two copies of each file, thereby realizing a volume size that is half of the total allocated space.

> ***NOTE*** **A mirrored disk array enables the computer to survive the failure of one disk with service interruption or data loss. Another variation on this technology is to create a mirrored array using two disks that are connected to different host adapters. This technique, called disk duplexing, enables the computer to survive the failure of a disk or a host adapter.**

Creating RAID-5 Volumes

When creating a RAID-5 volume, as shown in Figure 7-11, you must select three or more disks, and you must specify the same amount of space on each disk.



New RAID-5 Volume

Select Disks
You can select the disks and set the disk size for this volume.

Select the disks you want to use, and then click Add.

Available:

Disk 1	5956 MB
Disk 3	40957 MB
Disk 4	40957 MB

Selected:

Disk 2	40957 MB

Total volume size in megabytes (MB): 0

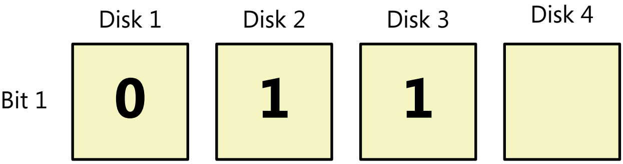
Maximum available space in MB: 40957

Select the amount of space in MB: 40957

FIGURE 7-11 The Select Disks page in the New RAID-5 Volume Wizard.

The system provides fault tolerance by calculating a parity value for each bit in the array. A *parity value* is a sum of the corresponding bits on each disk in the array. Every bit has a binary value of 0 or 1, so the sum of all the bits in a particular location on the array must be 0 or 1. (This is why all the disks in the array must have the same amount of space.) If one of the disks in the array is lost, the system can use the parity information to recalculate the value of the missing bits.

For example, in a 4-disk array, the values of the first bit in each of the first 3 disks might be 0, 1, and 1, as shown in Figure 7-12.



	Disk 1	Disk 2	Disk 3	Disk 4
Bit 1	0	1	1	

FIGURE 7-12 Bit 1 values on a four-disk RAID-5 array (before parity).

Adding them together (in binary) gives you a parity value of 1, which the system writes to the first bit in the fourth disk, as shown in Figure 7-13.

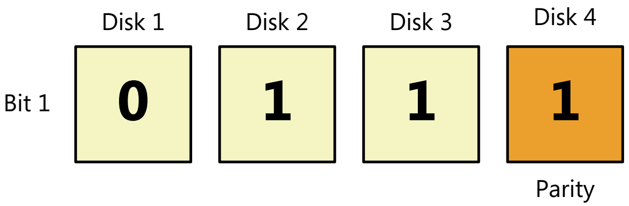


FIGURE 7-13 Bit 1 values on a four-disk RAID-5 array (with parity).

If the second disk in the array fails, as shown in Figure 7-14, one of the four corresponding bits is lost.

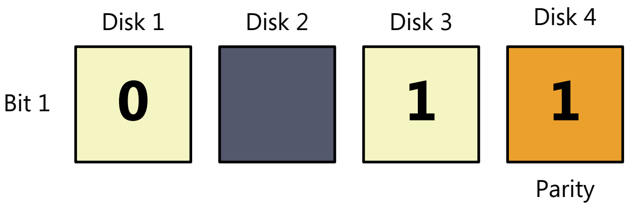


FIGURE 7-14 Bit 1 values on a four-disk RAID-5 array, after disk failure.

When this occurs, the system can look at the values of the first bit in the remaining disks (0 and 1) and the value of the parity bit (1), and know that the value of the missing bit must be 1, as shown in Figure 7-15. (If the parity bit were 0, the missing bit would have to be 0.) When the malfunctioning drive is replaced, the system calculates the value of each missing bit and reconstructs the data on the new disk.

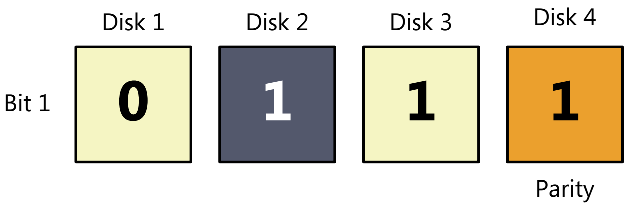


FIGURE 7-15 Bit 1 values on a 4-disk RAID-5 array, after disk reconstruction.

In this way, a RAID-5 array can yield a greater amount of available storage space than a mirrored array. On a RAID-5 volume, the size of the volume specified by the *Total volume size in megabytes (MB)* indicator is based on the size of the disks, multiplied by the number of disks in the array, minus 1. Thus, a RAID-5 array that consists of four 100 GB drives will have a volume size of 300 GB.

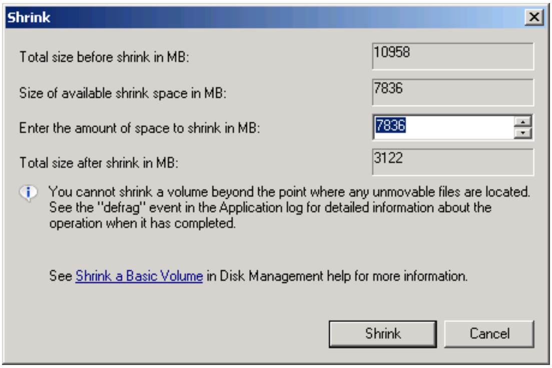
100 × (4 – 1) = 300

A RAID-5 volume can suffer the failure of any one disk without data loss. When a disk fails, overall performance of the array suffers, more so while the array is reconstructing the data on a newly installed disk.

The RAID-5 capability provided by Windows Server 2008 R2 is known as *software-based RAID* because the system processor is responsible for performing all of the bit parity calculations. Administrators who are serious about RAID data protection might want to consider a *hardware-based RAID* solution, instead. Hardware-based RAID uses a separate host adapter with its own processor to offload the bit parity calculations from the system processor. This provides greater efficiency without overburdening the computer's main processor.

Shrinking and Extending Volumes

With certain limitations, Windows SBS 2011 also enables you to shrink and extend volumes after you have created them, with no loss of data. When you right-click a volume and select Shrink Volume, a Shrink dialog box appears, as shown in Figure 7-16.



Shrink

Total size before shrink in MB: 10958

Size of available shrink space in MB: 7836

Enter the amount of space to shrink in MB: 7836

Total size after shrink in MB: 3122

You cannot shrink a volume beyond the point where any unmovable files are located. See the "defrag" event in the Application log for detailed information about the operation when it has completed.

See Shrink a Basic Volume in Disk Management help for more information.

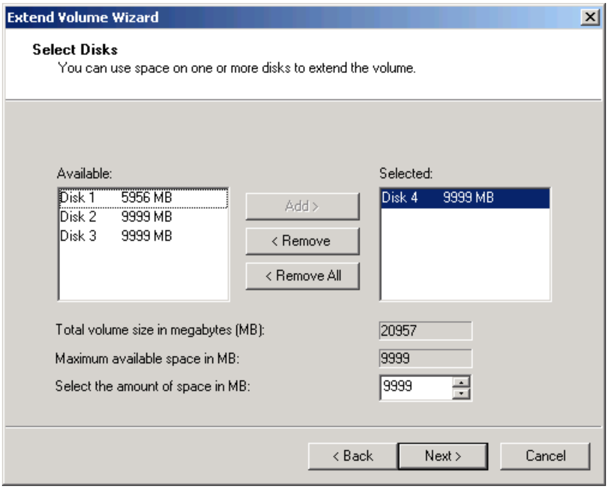
FIGURE 7-16 The Shrink dialog box.

The dialog box enables you to specify how much disk space you want to free up by shrinking the volume, based on the amount of data currently stored there. The space freed by the shrink process is added to any contiguous unallocated space located just after the shrinked drive.

Volume shrinking is subject to the following limitations:

- You cannot shrink volumes formatted with any of the FAT file systems; you can shrink only NTFS volumes.
- You cannot shrink striped, mirrored, or RAID-5 volumes.
- To shrink a volume, the amount of free space on the volume must be at least equal to the amount of space you want to reclaim.

When you right-click a volume and select *Extend volume*, the Extend Volume Wizard appears. The wizard consists of a Select Disks page (see Figure 7-17), just like the one you see when creating a non-simple volume. This is because you can conceivably extend a simple volume onto one or more additional disks, creating a spanned volume in the process.



Extend Volume Wizard

Select Disks

You can use space on one or more disks to extend the volume.

Available:

```
Disk 1    5956 MB
Disk 2    9999 MB
Disk 3    9999 MB
```

Selected:

```
Disk 4    9999 MB
```

Total volume size in megabytes (MB): 20957

Maximum available space in MB: 9999

Select the amount of space in MB: 9999

FIGURE 7-17 The Select Disks page from the Extend Volume Wizard.

The ability to extend volumes is subject to the following limitations:

- You cannot extend volumes formatted with any of the FAT file systems; you can only shrink NTFS volumes.
- To extend a volume on a basic disk into noncontiguous space on the same disk, you must convert it to a dynamic disk.
- You cannot extend mirror or RAID-5 volumes.
- You can extend a boot volume or system volume only into contiguous space on the same disk; you cannot extend them onto other disks.

NOTE **In this context, the term *contiguous space* refers to unallocated space immediately following the volume you want to extend.**

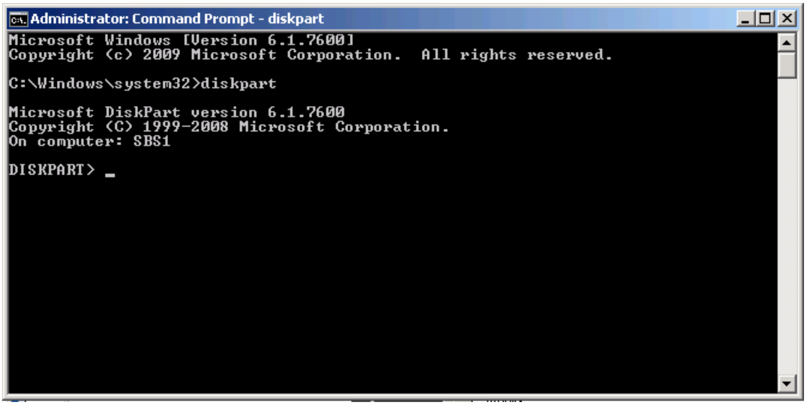
Using Diskpart.exe

In addition to the graphical interface that the Disk Management snap-in provides, Windows Server 2008 R2 also includes a command-line utility called Diskpart.exe that can perform all the same tasks, and a few that Disk Management cannot, such as creating a fourth primary partition on a basic disk.

Diskpart.exe has two operational modes: a script mode and an interactive mode. To use script mode, you create scripts containing multiple Diskpart commands and execute them from the command line using the following syntax:

```
diskpart /s scriptfile
```

To use interactive mode, you run Diskpart.exe from the command line without any parameters. This runs the program and generates a DISKPART> prompt, as shown in Figure 7-18.

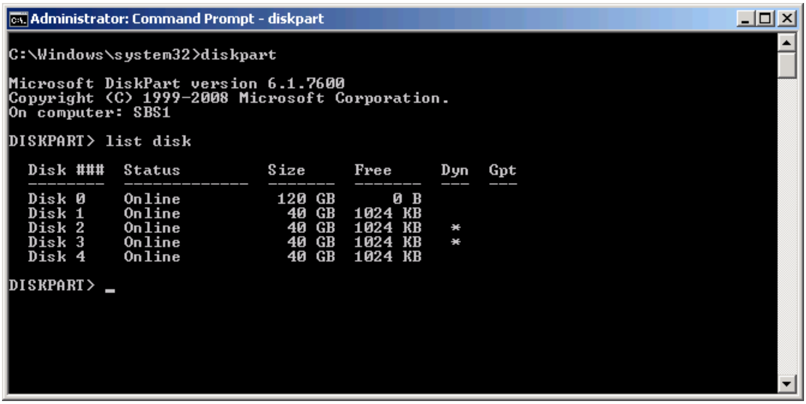


```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>diskpart

Microsoft DiskPart version 6.1.7600
Copyright (C) 1999-2008 Microsoft Corporation.
On computer: SBS1

DISKPART> _
```

FIGURE 7-18 The *DISKPART>* prompt generated by Diskpart.exe in interactive mode.

To use Diskpart in interactive mode, you execute commands from the *DISKPART>* prompt. Typically, you use various commands to specify what storage resource you want to manage and then use other commands to work with that resource.

For example, to create a new partition on a basic disk, you must first specify the disk where you want to create the partition. The *list disk* command displays a list of the disks on the system, as shown in Figure 7-19.



```
C:\Windows\system32>diskpart

Microsoft DiskPart version 6.1.7600
Copyright (C) 1999-2008 Microsoft Corporation.
On computer: SBS1

DISKPART> list disk

  Disk ###  Status         Size     Free     Dyn  Gpt
  --------  -------------  -------  -------  ---  ---
  Disk 0    Online          120 GB      0 B
  Disk 1    Online           40 GB  1024 KB
  Disk 2    Online           40 GB  1024 KB   *
  Disk 3    Online           40 GB  1024 KB   *
  Disk 4    Online           40 GB  1024 KB

DISKPART> _
```

FIGURE 7-19 Output of the Diskpart.exe *list disk* command.

To work with a particular disk, you use a command like *select disk 4*, which shifts the focus of the program to that disk. It executes all your commands from this point on disk 4, until you change the focus. In the same way, you can change the focus of the program to a specific partition or volume on the current disk.

Once you have selected a disk, you can create a partition using a command like the following:

```
create partition primary size=10000
```

This command creates a 10 GB primary partition on the currently selected disk. Using other commands, such as *add*, *convert*, *delete*, *extend*, *format*, and *shrink*, you can manipulate disks, partitions, and volumes, just as you can from the Disk Management snap-in.

> ***NOTE*** **The Disk Management snap-in is somewhat informal about disk terminology, often confusing the terms *partition* and *volume*. Diskpart.exe is more precise. You cannot create a volume on a basic disk using Diskpart, nor can you create a partition on a dynamic disk.**

CHAPTER 8

Working with Permissions

Security is one of the primary concerns of any network administrator, of course, and Windows Small Business Server (SBS) 2011 is designed to help administrators keep their networks safe without the need for extensive training in security principles. As mentioned in previous chapters, Windows SBS 2011 is based on the open architecture of Windows Server 2008 R2 and other Microsoft products, but instead of leaving the user to design an effective and secure configuration, the product arrives preconfigured. The designers of Windows SBS have made many of the decisions that are ordinarily left up to administrators, and in doing so, they have created a networking environment that takes advantage of the software's security capabilities.

Network security is not just a matter of design and deployment, however. It is an ongoing concern, and administrators must be aware of the Windows SBS security architecture and the tools they can use to maintain and enhance it.

Understanding Windows SBS Security Principles

Security is essentially a matter of controlling access to network resources. In theory, one can create a perfectly secure system simply by denying everyone access to it, but this is hardly a feasible solution for a data network. Some of the basic security principles for the small business network administrator to consider are as follows:

- Allow users to access the network resources they need to perform their jobs.

- Prevent unauthorized network users from accessing administrative tools and settings.
- Allow network users to access the Internet without providing Internet users unrestricted access to the network.

The following sections examine the primary mechanisms and design decisions in Windows SBS 2011 that enable administrators to realize these goals.

Authenticating Users

Authentication, one of the two fundamental security functions, is the process of verifying a user's identity in preparation for granting that user access to a protected resource. To authenticate a user, a system requires at least one of the following:

- **Something the user *knows*** The most common form of authentication requires users to supply a piece of information, such as a password, which the system already possesses. The complicating factor in this type of authentication is the security of the passwords, which can conceivably be intercepted during transmission or compromised by the user. Windows SBS 2011 uses password-based authentication by default, with authentication protocols that protect the passwords from capture during network transmission.
- **Something the user *has*** Some security systems require users to possess a smart card or other identifying device that they must supply to the computer before they can access protected resources. Windows SBS 2011 supports smart card authentication, but it is not configured to do so by default. The main drawback of this authentication method is the additional cost for the cards and the card reader hardware. Smart cards can also be easily lost or stolen, so users are nearly always required to provide a password as well.
- **Something the user *is*** Some security systems require users to confirm their identities by scanning physiological characteristics, such as fingerprints. This technology is known as *biometrics*. Biometrical authentication is one of the most secure systems available because fingerprints and other physiological characteristics are difficult to spoof or steal. Windows Server 2008 R2 does not include direct support for biometrical authentication (although Windows 7 now does, in the form of the Windows Biometric framework), but it does support modular authentication protocols that enable the system to interact with third-party hardware and software authentication solutions.

Active Directory Domain Services (AD DS) is responsible for authenticating network users in Windows SBS 2011. When you create user accounts, you specify passwords for them, which AD DS stores in its database. When users log on from their workstations, they type their passwords as part of the authentication process.

The biggest problem with password-based authentication is the tendency of the passwords to be compromised. There are two potential avenues of compromise: the network and the users themselves. If client applications transmit passwords over the network in clear text, it is possible for someone to capture the network packets and read the passwords inside them. Even if a client application encrypts the passwords before transmitting them, a potential intruder can often identify the data string that contains the encrypted password and use it to create an illicit logon by replaying it back to a server, still in its encrypted form.

To protect the user passwords, AD DS uses *Kerberos*, an advanced authentication protocol that enables clients to log on without transmitting passwords over the network in any form, clear or encrypted. Named for the three-headed dog of Greek mythology that guards the entrance to Hades, Kerberos is a highly complex protocol that requires three elements to function: the client attempting to access a protected resource, the server hosting the protected resource, and an authentication provider. In Windows SBS 2011, the AD DS domain controller is the authentication provider, and it is involved in every security transaction, even when a user accesses a resource on another server. To avoid transmitting passwords over the network, Kerberos uses cryptographic values derived from the passwords to create unique *tickets* that clients and servers exchange to gain access to protected resources. Because the tickets are generated for a specific use at a specific time, intruders capturing the packets cannot replay them or derive user passwords from them.

Passwords are also vulnerable to low-tech forms of compromise, typically resulting from users' sloppy or naive security habits. Users often write passwords down, give them to coworkers for the sake of convenience, or are duped into supplying them through social engineering. To address these problems, Windows SBS 2011 uses Group Policy settings to compel users to change their passwords at regular intervals. You can modify these settings to suit the security needs of your organization.

> ***NOTE*** ***Social engineering*** **is the term used to define the process by which intruders gain access to protected resources by manipulating users into providing their credentials or other information. For example, a friendly stranger claiming to be from the company's IT department calls a user on the phone and says that he has been instructed to upgrade the user's account, but he needs the user's password to do so. The user, without verifying the caller's identity, supplies the password and thinks no more of it. In many cases, social engineering is a far easier and more effective tactic for penetrating a network's security than other high-tech alternatives.**

Authorizing Users

The other fundamental security function is *authorization*, which is defined as the process of specifying which protected resources an authenticated user is permitted to access. Authentication confirms the user's identity, but authorization actually provides access to the network resources. In Windows SBS 2011, various permission systems authorize users to access protected resources.

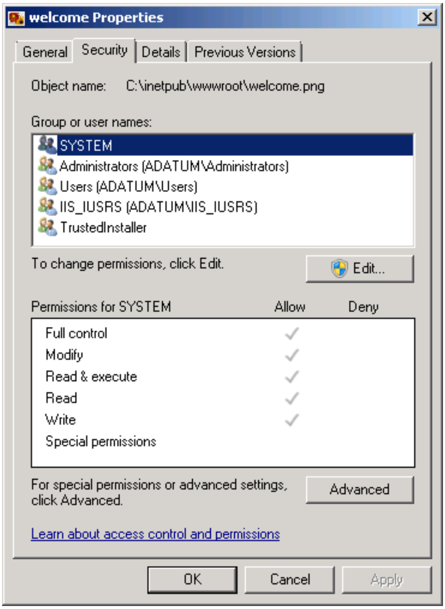
Although they function in much the same way, Windows SBS 2011 has separate permission systems for each of the following resources:

- NTFS files and folders
- Folder shares

- Printer shares
- AD DS objects
- Registry keys

Permissions are flags that enable a particular user or group of users to perform specific actions on a specific resource. For example, a user who possesses the Read permission for an NTFS file is allowed to read the contents of the file, but the user cannot modify the file nor do anything other than read it without additional permissions.

Windows stores permissions as a part of the objects they protect. Each protected element has an *access control list (ACL)* that consists of individual *access control entries (ACEs)*. Each ACE consists of a *security principal* (the user, group, or computer receiving access) and the permissions assigned to that security principal. In Windows SBS 2011, when you open the Properties sheet for a file, the *Security* tab contains the interface you can use to modify the file's ACL, as shown in Figure 8-1. Other elements, such as folder and printer shares, AD DS objects, and registry keys, have different types of permissions, but you use the same interface to manage them.


welcome Properties
General
Security
Details
Previous Versions
To change permissions, click Edit.
Edit...
For special permissions or advanced settings, click Advanced.
Advanced
Learn about access control and permissions
OK
Cancel
Apply

Object name: C:\inetpub\wwwroot\welcome.png

Group or user names:

SYSTEM
Administrators (ADATUM\Administrators)
Users (ADATUM\Users)
IIS_IUSRS (ADATUM\IIS_IUSRS)
TrustedInstaller

Permissions for SYSTEM	Allow	Deny
Full control	✓	
Modify	✓	
Read & execute	✓	
Read	✓	
Write	✓	
Special permissions		

FIGURE 8-1 The *Security* tab on a file's Properties sheet.

In Windows SBS 2011, as with all the other Windows operating systems, permissions are always a part of the protected element, not the entity receiving access to that element. Each file on an NTFS volume, for example, has an ACL specifying the users and groups that can access it. If you move the file to another NTFS drive, the ACL goes with it. However, user and group objects in the AD DS database do not have a list of the files and other resources they are permitted to access.

Combining Permissions

Access control—the process of regulating who can use specific system resources—is one of the fundamental tasks of the network administrator. Windows SBS 2011, like all of the Windows operating systems, uses permissions to control access to shares, file systems, printers, and many other resources.

Shared folders have their own independent set of permissions, completely separate from the other Windows permission systems, such as the NTFS permissions you use to control access to files and folders. The main difference between share permissions and NTFS permissions is that share permissions apply only when a user attempts to access a protected resource over the network. NTFS permissions apply both over the network and on the local console.

For example, users who have the NTFS permissions needed to access a server folder, but who lack share permissions for that same folder, can access it from the server console, but not over the network. Users that have share permissions but lack NTFS permissions cannot access the folder at all.

> ***NOTE*** **The FAT file systems that Windows Server 2008 R2 supports have no built-in access control capabilities. Therefore, a computer with FAT volumes must rely on share permissions, as they are the only form of access control available. However, in today's computing environment, there are few—if any—compelling reasons to use the FAT file systems, so the need to rely on share permissions for access control is now a rarity.**

Because users must have both share and NTFS permissions to access a particular resource from the network, many administrators choose to avoid confusion by using only one of the available permission systems. NTFS permissions are the logical choice because they provide more comprehensive and flexible protection. In fact, this is the approach that Windows SBS 2011 takes in its default shares. All three of the default shares that Windows SBS 2011 creates for user access have the Allow Full Control permission assigned to the Everyone special identity, which means that all network users can connect to them without restriction. To control access to the shares on a granular level, Windows SBS 2011 assigns NTFS permissions.

> ***NOTE*** **A *special identity* is a Windows element that stands for all objects sharing a specific trait or condition. For example, assigning permissions to the Authenticated Users special identity causes all users that are logged on to the domain to receive those permissions.**

Establishing Permission Policies

One of the key elements of network administration is making sure that all the people sharing responsibility for a specific function are on the same page with regard to how they should use that function. In small businesses, this is sometimes not a big problem because there are only a few administrators (or maybe only one) who need to receive the word. On the other hand, administration on small business networks is often more informal than it is on larger ones, and administrators are less likely to establish policies and see to it that everyone follows them.

With regard to share and NTFS permission systems, it is important for someone to decide early on how administrators should use them on this particular network and see to it that those decisions are enforced. In some cases, this might simply be a matter of one person declaring that administrators should leave all share permissions wide open and use only NTFS permissions to secure resources. Other permission policies might dictate that administrators use Allow permissions, but not Deny permissions, and specify when and if administrators can block or otherwise control permission inheritance.

It is certainly not required that administrators of small business networks avoid using share permissions for access control, but it is recommended. Using share permissions and NTFS permissions is like having two locked doors that require two different keys to get into your house. Sure, it's safer, but consider carefully whether it is really necessary.

Whichever combination of permissions you choose to employ on your network, failure to create explicit policies in these matters can lead to chaos in the future when a user cannot gain access to a resource. If one administrator prefers to use share instead of NTFS permissions, or Deny instead of Allow permissions, or explicit permissions on every folder instead of inherited ones, troubleshooting becomes a nightmare, with everyone trying to maintain their own standards at the same time.

Working with Permissions

In Chapter 9, "Managing Storage," you learn how to create a new shared folder using the Provision A Shared Folder Wizard supplied with Windows SBS 2011 and configure both the NTFS and the share permissions for that folder in the process. The wizard provides some simple preset combinations of share permissions and also full access to the permission editing interface for both systems. It's a good idea for administrators to have a basic idea of how these permission systems work before they start using them, so the rest of this chapter is devoted to an introduction to the share and NTFS permission systems, as well as an explanation of the permission editing interfaces for each one.

Using Share Permissions

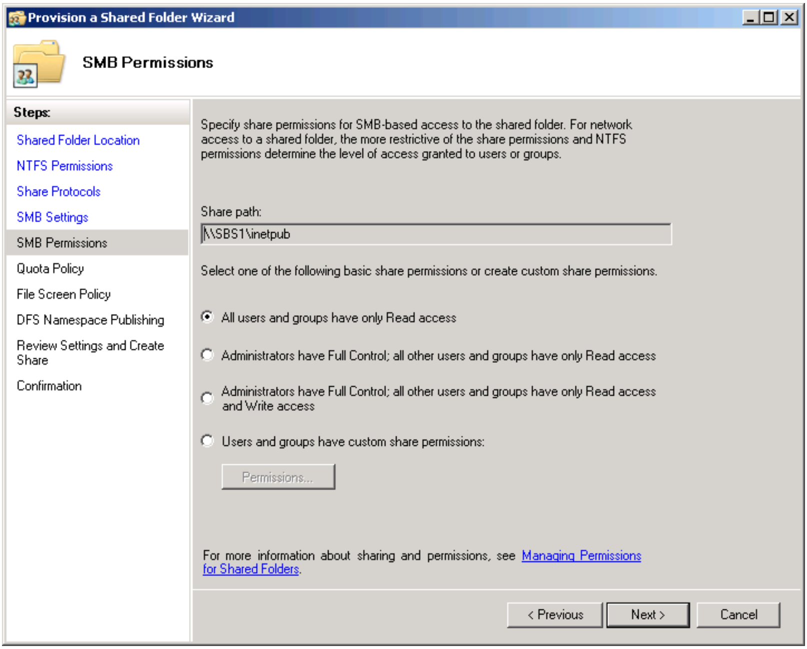
The share permission system is the simplest of the permission systems in Windows Server 2008 R2. It functions just like the NTFS and other permission systems in Windows, except that there are only three permissions you can assign. As with the other permission systems, you can allow or deny each of the permissions to any security principal available on the system or in the domain. Table 8-1 lists the three share permissions and the tasks they enable users to perform.

TABLE 8-1 Share Permissions and Associated Tasks

SHARE PERMISSION	ALLOWS OR DENIES SECURITY PRINCIPALS THE ABILITY TO:
Full Control	■ Change file permissions ■ Take ownership of files ■ Perform all tasks allowed by the Change permission
Change	■ Create folders ■ Add files to folders ■ Change data in files ■ Append data to files ■ Change file attributes ■ Delete folders and files ■ Perform all actions permitted by the Read permission
Read	■ Display folder names, file names, file data, and attributes ■ Execute program files ■ Access other folders within the shared folder

Assigning the Allow Full Control share permission to everyone is a simple solution that, on a small business network, is typically successful in removing the share permission system from everyone's consideration. There are certain inconveniences that are possible as a result—someone could conceivably take ownership of a share and deny everyone else all permissions to it—but this is a futile gesture because there is nothing to stop you, or anyone else, from taking ownership back and revoking those permissions.

When you create a new share using the Provision A Shared Folder Wizard, the SMB Permissions page, shown in Figure 8-2, enables you to select from three preconfigured share permission assignments, none of which is equivalent to the Allow Full Control for Everyone assignment that Windows SBS 2011 uses for its default shares. However, when you select the *Users and groups have custom share permissions* option and click *Permissions*, a Permissions dialog box for the share appears, enabling you to assign any permissions you want.



Specify share permissions for SMB-based access to the shared folder. For network access to a shared folder, the more restrictive of the share permissions and NTFS permissions determine the level of access granted to users or groups.

Share path: \\SBS1\inetpub

Select one of the following basic share permissions or create custom share permissions.

● All users and groups have only Read access

○ Administrators have Full Control; all other users and groups have only Read access

○ Administrators have Full Control; all other users and groups have only Read access and Write access

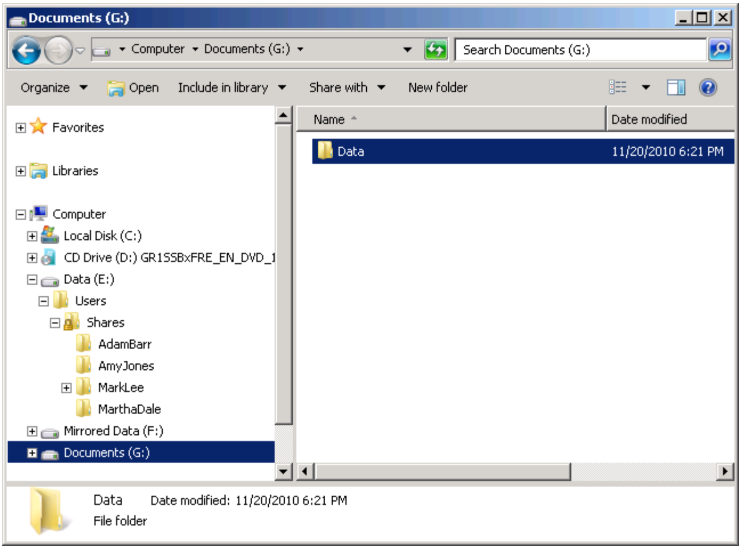
○ Users and groups have custom share permissions:

For more information about sharing and permissions, see Managing Permissions for Shared Folders.

FIGURE 8-2 The SMB Permissions page of the Provision A Shared Folder Wizard.

This same Permissions interface is accessible from the shared folder's Properties sheet. To assign the Allow Full Control permission to a folder share that you have already created, use the following procedure:

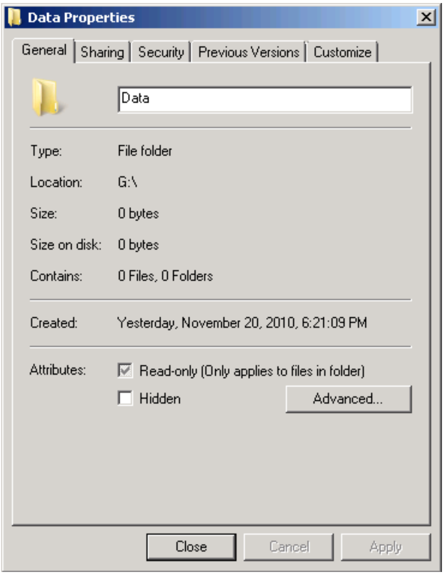
1. Log on to your Windows SBS 2011 server using a domain account with administrative privileges.
2. Open Windows Explorer and browse to the shared folder you want to manage.



Name	Date modified
Data	11/20/2010 6:21 PM

Data Date modified: 11/20/2010 6:21 PM
File folder

3. Right-click the shared folder and, from the context menu, select *Properties*. The Properties sheet for the folder appears.



Data

Type: File folder

Location: G:\

Size: 0 bytes

Size on disk: 0 bytes

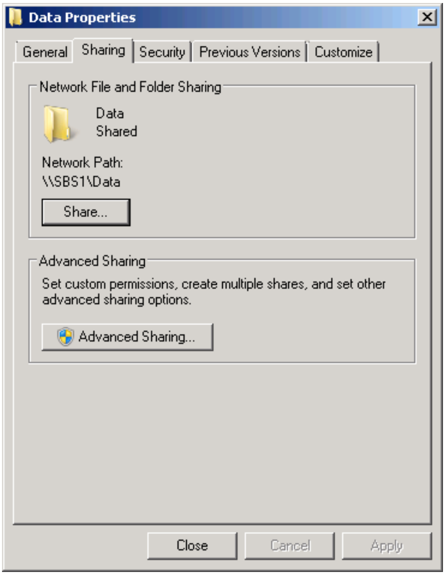
Contains: 0 Files, 0 Folders

Created: Yesterday, November 20, 2010, 6:21:09 PM

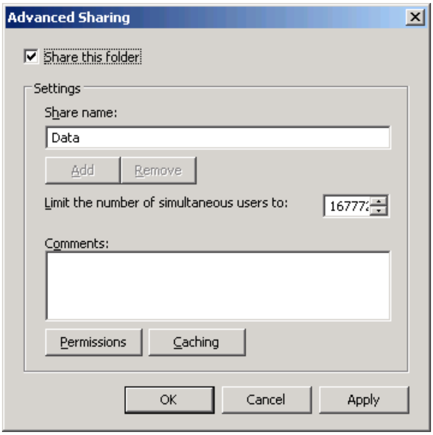
Attributes: ☑ Read-only (Only applies to files in folder)

□ Hidden

4. Click the *Sharing* tab.



5. Click *Advanced sharing*. The Advanced Sharing dialog box appears.

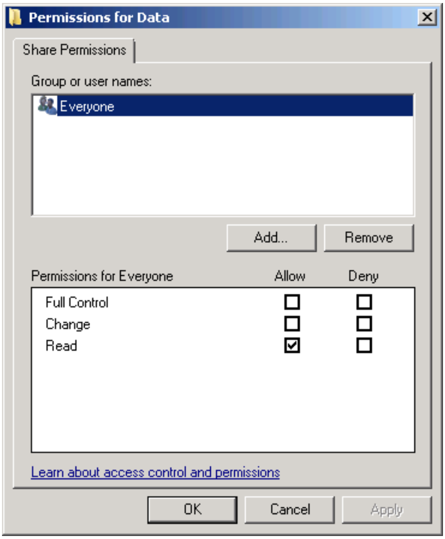


☑ Share this folder

Share name: Data

Limit the number of simultaneous users to: 16777

6. Click *Permissions*. The Permissions dialog box for the share appears.



Permissions for Data

Share Permissions

Group or user names:

Everyone

Permissions for Everyone	Allow	Deny
Full Control	□	□
Change	□	□
Read	☑	□

Learn about access control and permissions

NOTE **This is the same Permissions dialog box that appears when you select the *Users and groups have custom share permissions* option in the Provision A Shared Folder Wizard.**

7. In the *Group or user names* list, select *Everyone*.
8. In the *Permissions for everyone* box, select the *Allow full control* check box and click *OK*.
9. Click *OK* to close the Advanced Sharing dialog box.
10. Click *OK* to close the Properties sheet.
11. Close Windows Explorer.

Using NTFS Permissions

Once you grant to the Everyone special identity the Allow Full Control share permission, anyone can access the shared folder over the network. However, users cannot access the files in the shared folder unless they have appropriate NTFS permissions. NTFS permissions apply whether the user is accessing the files over the network or is seated at the computer where the files are stored.

Unlike the relatively simple share permissions system, NTFS permissions provide much more detailed control over the access granted to a specific security principal. You might want to limit some users to reading a file while granting others permission to modify the contents of the same file. Still others might be able to create new files in the same folder.

Standard Permissions and Special Permissions

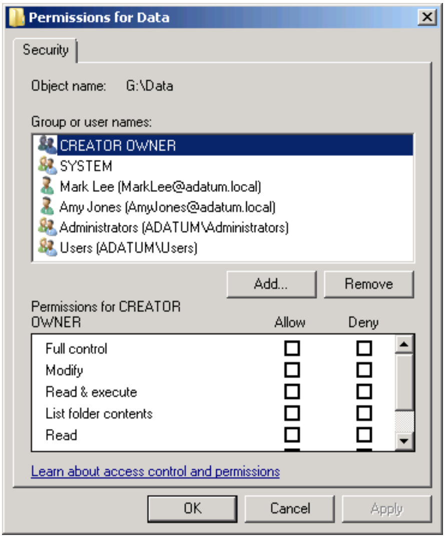
The NTFS file system includes two types of permissions: standard permissions and special permissions. *Standard permissions* are the ones that most administrators use on an everyday basis. The six NTFS standard permissions and the privileges they provide when you apply them to files and folders are listed in Table 8-2.

TABLE 8-2 NTFS Standard Permissions

STANDARD PERMISSION	WHEN APPLIED TO A FOLDER, ENABLES A SECURITY PRINCIPAL TO	WHEN APPLIED TO A FILE, ENABLES A SECURITY PRINCIPAL TO
Full Control	■ Modify the folder permissions ■ Take ownership of the folder ■ Delete subfolders and files contained in the folder ■ Perform all actions associated with all the other NTFS folder permissions	■ Modify the file permissions ■ Take ownership of the file ■ Perform all actions associated with all the other NTFS file permissions
Modify	■ Delete the folder ■ Perform all actions associated with the Write and the Read & Execute permissions	■ Modify the file ■ Delete the file ■ Perform all actions associated with the Write and the Read & Execute permissions
Read & Execute	■ Navigate through restricted folders to reach other files and folders ■ Perform all actions associated with the Read and List Folder Contents permissions	■ Perform all actions associated with the Read permission ■ Run applications
List Folder Contents	■ View the names of the files and subfolders contained in the folder	■ Not applicable
Read	■ See the files and subfolders contained in the folder ■ View the ownership, permissions, and attributes of the folder	■ Read the contents of the file ■ View the ownership, permissions, and attributes of the file

STANDARD PERMISSION	WHEN APPLIED TO A FOLDER, ENABLES A SECURITY PRINCIPAL TO	WHEN APPLIED TO A FILE, ENABLES A SECURITY PRINCIPAL TO
Write	■ Create new files and subfolders inside the folder ■ Modify the folder attributes ■ View the ownership and permissions of the folder	■ Overwrite the file ■ Modify the file attributes ■ View the ownership and permissions of the file

When you open the Properties dialog box for an NTFS file or folder, select the *Security* tab, and click *Edit*, you see the interface shown in Figure 8-3, which is quite similar to the share permission interface you worked with earlier. In fact, all the Windows Server 2008 R2 permission systems use the same basic interface, the differences being the names of the permissions you can select and the number of available permissions.



Object name: G:\Data

Group or user names:

CREATOR OWNER
SYSTEM
Mark Lee (MarkLee@adatum.local)
Amy Jones (AmyJones@adatum.local)
Administrators (ADATUM\Administrators)
Users (ADATUM\Users)

Permissions for CREATOR OWNER	Allow	Deny
Full control	□	□
Modify	□	□
Read & execute	□	□
List folder contents	□	□
Read	□	□

FIGURE 8-3 The *Security* tab of an NTFS file.

Standard permissions are easy to use, but they are not the most detailed form of permissions available on NTFS volumes. In actuality, standard permissions are preconfigured combinations of special permissions. *Special permissions* provide the finest possible control over your NTFS files and folders. There are 14 special permissions, as listed in Table 8-3.

TABLE 8-3 NTFS Special Permissions

SPECIAL PERMISSION	FUNCTIONS
Traverse Folder/ Execute File	■ The Traverse Folder permission allows or denies security principals the ability to move through folders that they do not have permission to access so they can reach files or folders that they do have permission to access. This permission applies to folders only. ■ The Execute File permission allows or denies security principals the ability to run program files. This permission applies to files only.
List Folder/ Read Data	■ The List Folder permission allows or denies security principals the ability to view the file and subfolder names within a folder. This permission applies to folders only. ■ The Read Data permission allows or denies security principals the ability to view the contents of a file. This permission applies to files only.
Read Attributes	■ Allows or denies security principals the ability to view the NTFS attributes of a file or folder.
Read Extended Attributes	■ Allows or denies security principals the ability to view the extended attributes of a file or folder.
Create Files/Write Data	■ The Create Files permission allows or denies security principals the ability to create files within the folder. This permission applies to folders only. ■ The Write Data permission allows or denies security principals the ability to modify the file and overwrite existing content. This permission applies to files only.
Create Folders/ Append Data	■ The Create Folders permission allows or denies security principals the ability to create subfolders within a folder. This permission applies to folders only. ■ The Append Data permission allows or denies security principals the ability to add data to the end of the file but not to modify, delete, or overwrite existing data in the file. This permission applies to files only.
Write Attributes	■ Allows or denies security principals the ability to modify the NTFS attributes of a file or folder.
Write Extended Attributes	■ Allows or denies security principals the ability to modify the extended attributes of a file or folder.

SPECIAL PERMISSION	FUNCTIONS
Delete Subfolders and Files	■ Allows or denies security principals the ability to delete subfolders and files, even if the Delete permission has not been granted on the subfolder or file.
Delete	■ Allows or denies security principals the ability to delete the file or folder.
Read Permissions	■ Allows or denies security principals the ability to read the permissions for the file or folder.
Change Permissions	■ Allows or denies security principals the ability to modify the permissions for the file or folder.
Take Ownership	■ Allows or denies security principals the ability to take ownership of the file or folder.
Synchronize	■ Allows or denies different threads of multithreaded, multiprocessor programs to wait on the handle for the file or folder, and synchronize with another thread that might signal it.

When you assign a standard permission to a security principal, you are actually assigning a combination of special permissions. The standard permissions and their corresponding special permissions are listed in Table 8-4. However, it is also possible to work with special permissions directly.

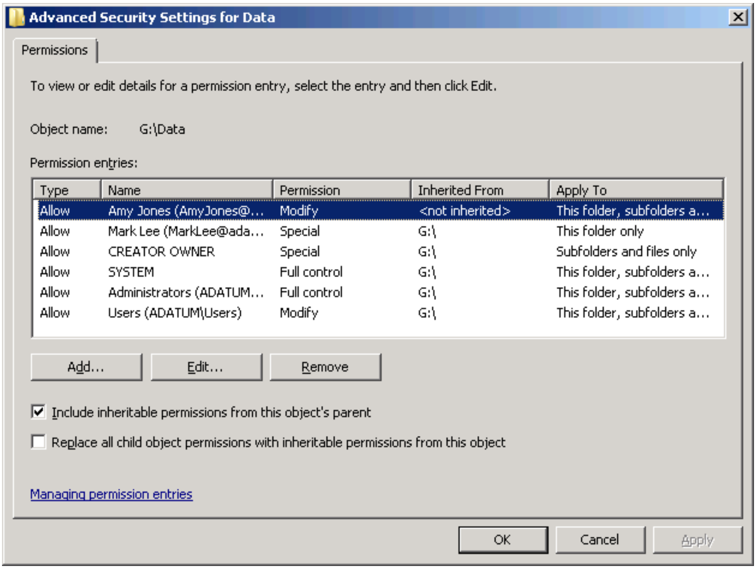
TABLE 8-4 NTFS Standard Permissions and their Special Permission Equivalents

STANDARD PERMISSIONS	SPECIAL PERMISSIONS
Read	■ List Folder/Read Data ■ Read Attributes ■ Read Extended Attributes ■ Read Permissions ■ Synchronize
Read & Execute	■ List Folder/Read Data ■ Read Attributes ■ Read Extended Attributes ■ Read Permissions ■ Synchronize ■ Traverse Folder/Execute File

STANDARD PERMISSIONS	SPECIAL PERMISSIONS
Modify	■ Create Files/Write Data ■ Create Folders/Append Data ■ Delete ■ List Folder/Read Data ■ Read Attributes ■ Read Extended Attributes ■ Read Permissions ■ Synchronize ■ Write Attributes ■ Write Extended Attributes
Write	■ Create Files/Write Data ■ Create Folders/Append Data ■ Read Permissions ■ Synchronize ■ Write Attributes ■ Write Extended Attributes
List Folder Contents	■ List Folder/Read Data ■ Read Attributes ■ Read Extended Attributes ■ Read Permissions ■ Synchronize ■ Traverse Folder/Execute File

STANDARD PERMISSIONS	SPECIAL PERMISSIONS
Full Control	■ Change Permissions ■ Create Files/Write Data ■ Create Folders/Append Data ■ Delete ■ Delete Subfolders and Files ■ List Folder/Read Data ■ Read Attributes ■ Read Extended Attributes ■ Read Permissions ■ Synchronize ■ Take Ownership ■ Write Attributes ■ Write Extended Attributes

When you open the Properties sheet for an NTFS file or folder, click *Advanced* on the *Security* tab, and then click *Edit*, the Advanced Security Settings For Data dialog box appears, as shown in Figure 8-4. This dialog box is the closest you can come to working directly with the ACEs in the file or folder's ACL.



To view or edit details for a permission entry, select the entry and then click Edit.

Object name: G:\Data

Permission entries:

Type	Name	Permission	Inherited From	Apply To
Allow	Amy Jones (AmyJones@...	Modify	<not inherited>	This folder, subfolders a...
Allow	Mark Lee (MarkLee@ada...	Special	G:\	This folder only
Allow	CREATOR OWNER	Special	G:\	Subfolders and files only
Allow	SYSTEM	Full control	G:\	This folder, subfolders a...
Allow	Administrators (ADATUM...	Full control	G:\	This folder, subfolders a...
Allow	Users (ADATUM\Users)	Modify	G:\	This folder, subfolders a...

☑ Include inheritable permissions from this object's parent

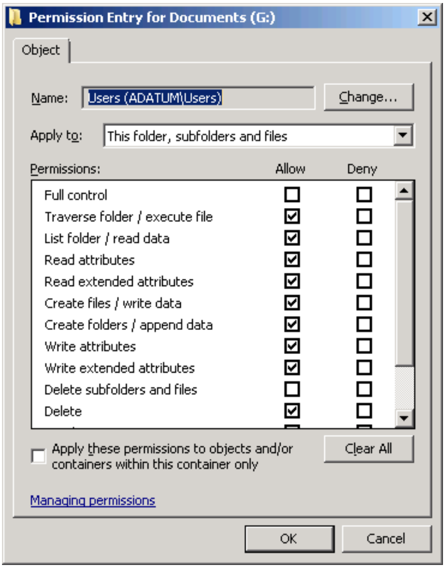
□ Replace all child object permissions with inheritable permissions from this object

FIGURE 8-4 The Advanced Security Settings For Data dialog box for an NTFS file or folder.

In this interface, you can see each of the ACEs that apply to the file or folder you selected when opening the dialog box. For each entry, the interface displays the following information:

- **Type** Specifies whether the entry contains an Allow or Deny permission. You cannot change this field on an existing entry.
- **Name** Specifies the security principal that will receive the permissions. By editing an entry, you can change the security principal as needed.
- **Permission** Specifies the permissions the security principal will receive. If the special permissions the entry assigns combine to form a standard permission, the name of that standard permission appears in this field. In the case of a nonstandard combination of special permissions, the word Special appears here. By editing an entry, you can change the permissions as needed.
- **Inherited from** Specifies the name of the parent folder from which the entry received the specified permissions. If the entry is applied directly to the selected file or folder, then a *<not inherited>* indicator appears here. You cannot change this field on an existing entry.
- **Apply to** Specifies whether the entry should apply the specified permissions to the selected folder only, or to specific subordinate elements in the folder. By editing an entry, you can change this field to specify virtually any combination of subordinate folders and files.

To modify an entry, you click *Change permissions*, select the entry, and click *Edit* to open a Permission Entry dialog box for the selected folder, as shown in Figure 8-5.



Name: Users (ADATUM\Users)

Apply to: This folder, subfolders and files

Permissions:	Allow	Deny
Full control	□	□
Traverse folder / execute file	☑	□
List folder / read data	☑	□
Read attributes	☑	□
Read extended attributes	☑	□
Create files / write data	☑	□
Create folders / append data	☑	□
Write attributes	☑	□
Write extended attributes	☑	□
Delete subfolders and files	□	□
Delete	☑	□

□ Apply these permissions to objects and/or containers within this container only

FIGURE 8-5 A Permission Entry dialog box.

In this dialog box, you can choose the special permissions you want to apply, change the security principal, and specify that you want to apply the permissions to any of the following combinations of files and folders:

- This folder only
- This folder, subfolders, and files
- This folder and subfolders
- This folder and files
- Subfolders and files only
- Subfolders only
- Files only

Using Group Permissions

Although it is possible to assign permissions to individual users, the general rule of thumb for network administrators is to assign permissions to groups instead. You can then grant permissions to users simply by adding them to a group. This way, when creating accounts for new users, or when a user changes jobs within the organization, you only have to manage group memberships instead of assigning and revoking a large number of permissions to different resources.

Understanding Permission Inheritance

Permissions always flow downward through a tree hierarchy by default. In the case of an NTFS volume, the permissions you assign to a folder are inherited by all the files and subfolders in that folder. Therefore, if you grant a user permission to access the root of a disk, that user receives the same permission for all the subordinate files and folders on that disk.

As a general rule, administrators design the directory structures of their disks to accommodate this phenomenon by placing the more restricted folders lower in the directory tree. For example, Windows SBS 2011 creates a Users folder on the C drive during the operating system installation and grants the Users group the following NTFS permissions to it:

- Allow Read & Execute
- Allow List folder Contents
- Allow Read

These permissions enable all members of the Users group to look at the contents of the folder, but they can't modify or delete the files there. Beneath the Users folder are individual subfolders, named for each person who has logged onto the system. These folders contain the user profiles, with each user receiving the Allow Full Control permission for his or her profile folder. Thus, the permissions become more specific as you move downward through the tree.

It is possible to prevent folders from inheriting permissions from their parent folders, if necessary. One way to do this is to assign Deny permissions for a particular folder to a particular user or group. As you can see in the permission interfaces shown earlier, Windows SBS 2011 enables you to allow permissions or deny them. Deny permissions always override Allow permissions, so even if a user inherits permissions to a particular folder from a parent, an explicit Deny permission for that folder takes precedence. Another way to prevent permission inheritance is to open the Advanced Security Settings dialog box and clear the *Include inheritable permissions from this object's parent* check box.

Both of these methods are effective ways of controlling permission inheritance, but they can complicate the access control process enormously, particularly if you have multiple administrators with different philosophies managing permissions for your network. Most administrators avoid using Deny permissions entirely and leave the default permission inheritance policies in place.

Understanding Effective Permissions

As you have seen, Windows SBS 2011 users can receive NTFS permissions for a particular file or folder in a variety of ways, including these:

- From explicit user assignments
- Inherited from parent folders
- Through group memberships

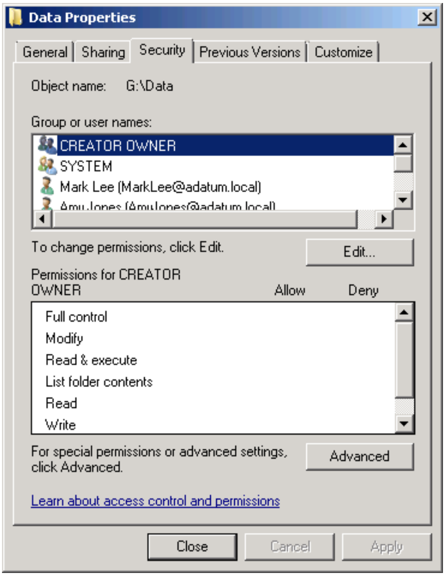
In many cases, users receive permissions for a specific file or folder from multiple sources, and those permissions can sometimes conflict. In a case like this, it is important for administrators to understand how Windows SBS resolves these permission conflicts. The combination of Allow and Deny permissions for a file or folder that a security principal receives from all possible sources is called its *effective permissions* for that resource. The three basic rules to remember when evaluating permission combinations are as follows:

- **Allow permissions are cumulative.** When a security principal receives different Allow permissions from various sources, the system combines them to form the effective permissions. For example, if a user inherits the Allow Read and Allow List Folder Contents permissions for a file from its parent folder, and receives the Allow Write and Allow Modify permissions for the same file from a group membership, the user's effective permissions for the file is the combination of all four permissions.
- **Deny permissions override Allow permissions.** When a security principal receives both Allow and Deny permissions from any single source, the Deny permissions take precedence over the Allow permissions. For example, if a user receives the Allow Full Control permission for a file from one group membership and the Deny Full Control permission for the same file from another group membership, then the Deny Full Control permission overrides the Allow Full Control permission, preventing the user from accessing the file in any way.

- **Explicit permissions take precedence over inherited permissions.** When you explicitly assign a security principal permissions to a file or folder, these permissions override any permissions that the security principal inherits from a parent folder or receives from group memberships. For example, if a user inherits the Deny Full Control permission for a file from its parent folder, assigning the user the Allow Full Control permission for that file overrides the inherited permission and provides the user with full access.

Because the interactions of the various permission sources can sometimes be difficult to evaluate, the Advanced Security Settings dialog box for an NTFS file or folder enables you to view the effective permissions for a specific user or group. To view effective permissions, use the following procedure:

1. Log on to your Windows SBS 2011 server using a domain account with administrative privileges.
2. Open Windows Explorer and browse to the parent folder of the folder you want to access.
3. Right-click the file or folder whose effective permissions you want to view. From the context menu, select Properties. The Properties sheet for the file or folder appears.
4. Click the *Security* tab.


Data Properties

Object name: G:\Data

Group or user names:

CREATOR OWNER
SYSTEM
Mark Lee (MarkLee@adatum.local)
Amy Jones (AmyJones@adatum.local)

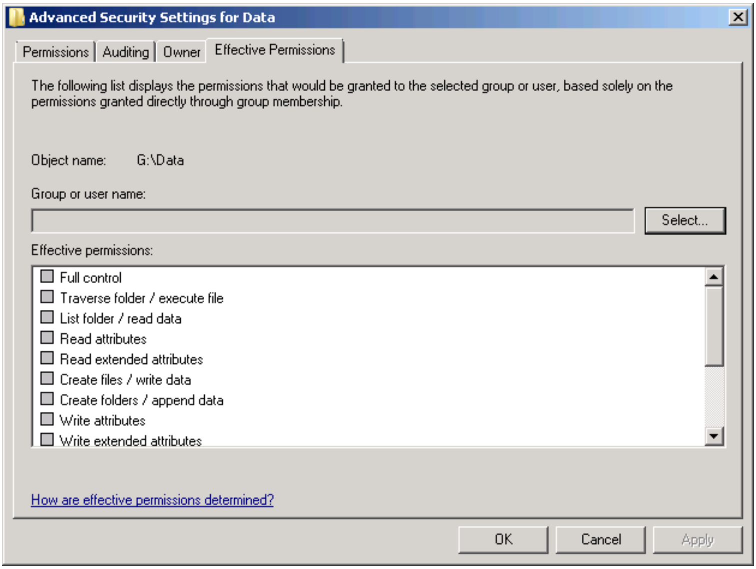
To change permissions, click Edit.

Permissions for CREATOR OWNER

	Allow	Deny
Full control		
Modify		
Read & execute		
List folder contents		
Read		
Write		

For special permissions or advanced settings, click Advanced.

5. Click *Advanced*. The Advanced Security Settings dialog box for the file or folder appears.
6. Click the *Effective permissions* tab.


Advanced Security Settings for Data
Permissions
Auditing
Owner
Effective Permissions
Select...
How are effective permissions determined?
OK
Cancel
Apply

The following list displays the permissions that would be granted to the selected group or user, based solely on the permissions granted directly through group membership.

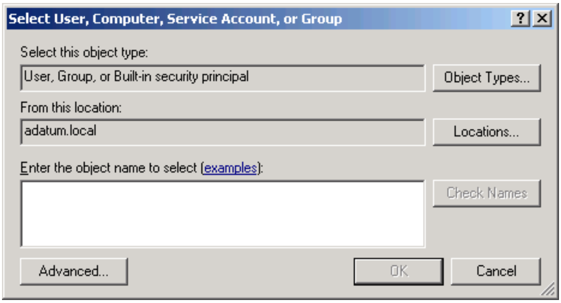
Object name: G:\Data

Group or user name:

Effective permissions:

- □ Full control
- □ Traverse folder / execute file
- □ List folder / read data
- □ Read attributes
- □ Read extended attributes
- □ Create files / write data
- □ Create folders / append data
- □ Write attributes
- □ Write extended attributes

7. Click *Select*. The Select User, Computer, Service Account, Or Group dialog box appears.

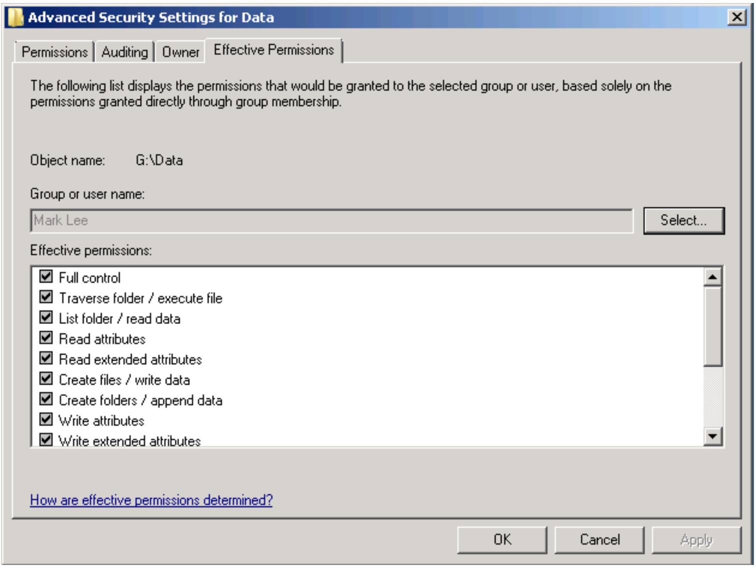


Select this object type: User, Group, or Built-in security principal

From this location: adatum.local

Enter the object name to select (examples):

8. In the *Enter the object name to select* text box, type the name of the security principal whose effective permissions you want to view and click *OK*. The security principal appears in the *Group or user name* text box and the *Effective permissions* box displays the permissions that the security principal currently possesses.


Advanced Security Settings for Data

The following list displays the permissions that would be granted to the selected group or user, based solely on the permissions granted directly through group membership.

Object name: G:\Data

Group or user name:

Mark Lee

Effective permissions:

☑ Full control
☑ Traverse folder / execute file
☑ List folder / read data
☑ Read attributes
☑ Read extended attributes
☑ Create files / write data
☑ Create folders / append data
☑ Write attributes
☑ Write extended attributes

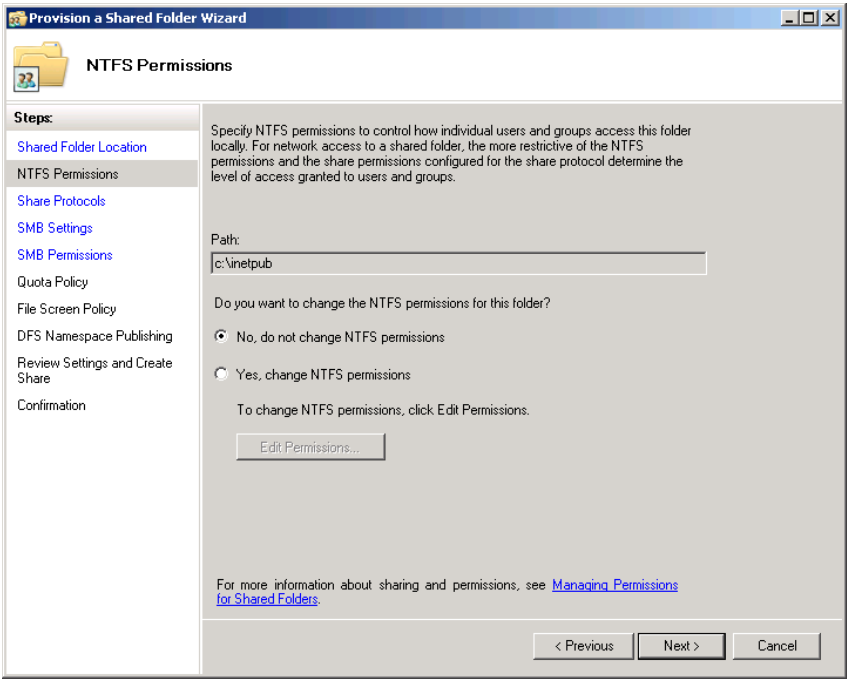
How are effective permissions determined?

NOTE **Selected gray check boxes indicate permissions that the security principal has inherited from a parent folder. Selected white check boxes indicate permissions explicitly assigned to the security principal.**

9. Click *OK* to close the Advanced Security Settings dialog box.
10. Click *OK* again to close the Properties sheet.
11. Close Windows Explorer.

Assigning NTFS Permissions

When you create a new share using the Provision A Shared Folder Wizard, the NTFS Permissions page, shown in Figure 8-6, provides access to the Permissions dialog box for the folder you intend to share. You can also modify the NTFS permissions for any file or folder using its Properties sheet.



Specify NTFS permissions to control how individual users and groups access this folder locally. For network access to a shared folder, the more restrictive of the NTFS permissions and the share permissions configured for the share protocol determine the level of access granted to users and groups.

Path:
c:\inetpub

Do you want to change the NTFS permissions for this folder?

● No, do not change NTFS permissions

○ Yes, change NTFS permissions

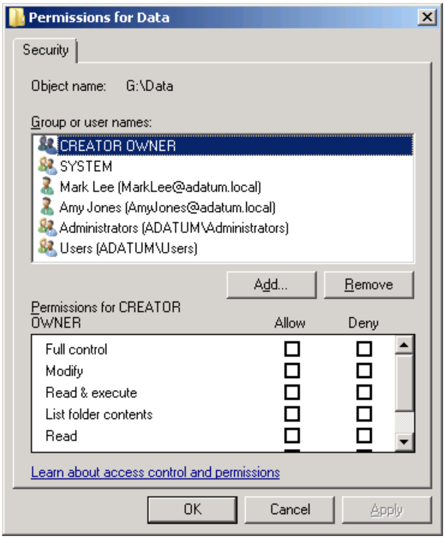
To change NTFS permissions, click Edit Permissions.

For more information about sharing and permissions, see Managing Permissions for Shared Folders.

FIGURE 8-6 The NTFS Permissions page in the Provision A Shared Folder Wizard.

To assign NTFS permissions to a folder, use the following procedure:

1. Log on to your Windows SBS 2011 server using a domain account with administrative privileges.
2. Open Windows Explorer and browse to the parent folder of the folder you want to manage.
3. Right-click the folder whose NTFS permissions you want to manage and, from the context menu, select *Properties*. The Properties sheet for the folder appears.
4. Click the *Security* tab.
5. Click *Edit*. The Permissions dialog box for the folder appears.



Permissions for Data

Security

Object name: G:\Data

Group or user names:

- CREATOR OWNER
- SYSTEM
- Mark Lee (MarkLee@adatum.local)
- Amy Jones (AmyJones@adatum.local)
- Administrators (ADATUM\Administrators)
- Users (ADATUM\Users)

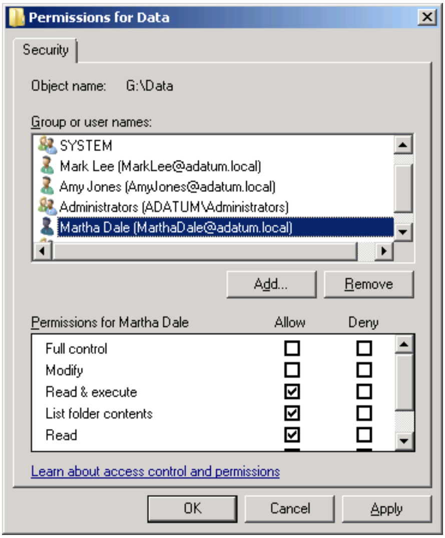
Add... Remove

Permissions for CREATOR OWNER	Allow	Deny
Full control	□	□
Modify	□	□
Read & execute	□	□
List folder contents	□	□
Read	□	□

Learn about access control and permissions

OK Cancel Apply

6. Click *Add*. The Select users, computers, service accounts, or groups dialog box appears.
7. In the *Enter object names to select* text box, type the name of the security principal to which you want to assign permissions and click *OK*. The security principal appears in the *Group or user names* list.



Permissions for Data

Security

Object name: G:\Data

Group or user names:

- SYSTEM
- Mark Lee (MarkLee@adatum.local)
- Amy Jones (AmyJones@adatum.local)
- Administrators (ADATUM\Administrators)
- Martha Dale (MarthaDale@adatum.local)

Add... Remove

Permissions for Martha Dale	Allow	Deny
Full control	□	□
Modify	□	□
Read & execute	☑	□
List folder contents	☑	□
Read	☑	□

Learn about access control and permissions

OK Cancel Apply

8. With the security principal you added selected, select the check boxes for the permissions you want to allow or deny. Then click *OK*.
9. Click *OK* again to close the Properties sheet.
10. Close Windows Explorer.

Understanding Resource Ownership

One of the peculiarities of the NTFS permission system is that it is possible to revoke all permissions from all users, leaving no one with the ability to access a particular file or folder. To prevent files and folders from being so orphaned, every NTFS element has an owner. The owner of a file or folder always has the ability to modify the permissions for that file or folder, even if the owner does not possess any permissions himself or herself. By default, the owner of a file or folder is the user who created it. However, any user who possesses the Allow Take Ownership special permission or the Allow Full Control standard permission can assume ownership of a file or folder.

CHAPTER 9

Managing Storage

Shared storage is one of the primary reasons for the invention of the local area network (LAN), and Windows Small Business Server (SBS) 2011 creates a number of shared folders as part of its default configuration. Once you have installed Windows SBS 2011, you can add more storage to your server and create as many shares as needed to support your users. You can also deploy additional servers on the network to provide even more file services.

Understanding the Default Windows SBS 2011 Storage Configuration

One of the main features of Windows SBS 2011 is the comprehensive setup procedure, which prevents new administrators from having to perform complex component installations and configurations. As discussed in Chapter 3, “Installing Windows Small Business Server (SBS) 2011,” and elsewhere, the Windows SBS setup process makes many configuration and administration decisions for you, and this necessarily entails a certain amount of compromise.

One of the areas in which compromise is necessary is in the server’s storage configuration. One of the traditional rules of server administration is to keep your operating system and application files on one volume and your data on another. This simplifies the process of locating specific files and facilitates proper backup procedures.

Windows SBS cannot comply with this rule because the setup program cannot realistically modify the installation of applications such as Microsoft Exchange or Windows Server Update Services (WSUS) to accommodate the additional volumes that might be present in the computer. The decision the product designers had to make was between keeping the installation procedure as simple as possible and providing additional flexibility. They chose the former.

As a result, the Windows SBS setup program places all the operating system files, application files, and data files on the same C drive that the program creates during the installation process. Once the server installation is complete, as discussed in Chapter 7, "Managing Disks," you are free to create as many additional volumes as you need, using advanced storage technologies such as spanning, striping, mirroring, and RAID-5, if desired.

Moving Data Stores

The concession that Windows SBS 2011 makes to the "separate disks" rule described earlier is to make it a simple matter to move your application from its default location on the C drive. After you create additional volumes on your disks, you can use the Windows SBS Console to move your Exchange, SharePoint, and Windows Server Update Services (WSUS) data stores to a volume on another disk.

This capability enables administrators to move data stores for several reasons, including the following:

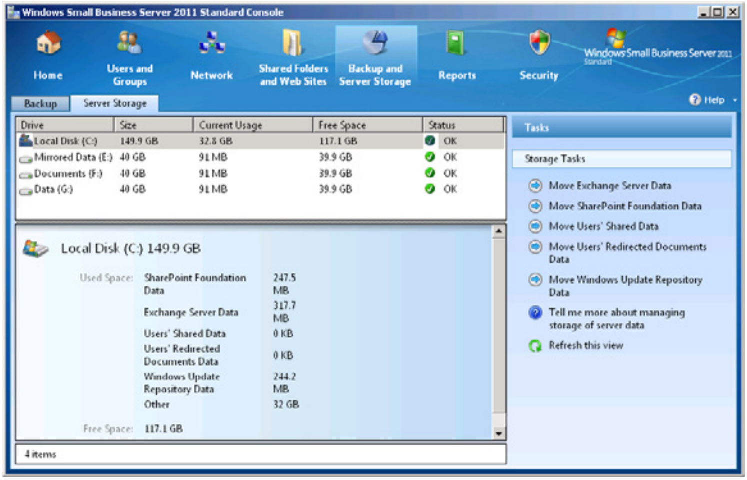
- To separate your data from the operating system files
- To optimize system performance by separating data read operations from programming reads
- To allocate additional storage space to a data store that is running out of space on the C drive.
- To store application data on a fault tolerant volume, such as one using mirroring or RAID-5

Before you actually move your data to a new location, consider the following prerequisites:

- **Destination volumes are ready** You must install the new disks and any drivers they might need, create the new volumes, and format them using the NTFS file system.
- **Sufficient space is available** Make sure that the destination volume has sufficient free space to hold the application data, including room for future expansion.
- **Users are not accessing the data** Perform the move during off hours, when users are not logged on to the network, or make sure that users are not accessing the data while you perform the move.

To move Windows SBS application data to another location, follow these steps:

1. Log on to your Windows SBS 2011 server, using an account with network Administrator privileges. The Windows SBS Console appears.
2. Click *Backup and server storage*, and then click the *Server storage* tab.
3. Select the *Local disk (C:)* drive. The console displays how much data for each of the Windows SBS–installed applications is stored on the disk.


Windows Small Business Server 2011 Standard Console
Home
Users and Groups
Network
Shared Folders and Web Sites
Backup and Server Storage
Reports
Security
Windows Small Business Server 2011 Standard
Backup
Server Storage
Help
Tasks
Storage Tasks

Drive	Size	Current Usage	Free Space	Status
Local Disk (C:)	149.9 GB	32.8 GB	117.1 GB	✓ OK
Mirrored Data (E:)	40 GB	91 MB	39.9 GB	✓ OK
Documents (F:)	40 GB	91 MB	39.9 GB	✓ OK
Data (G:)	40 GB	91 MB	39.9 GB	✓ OK

Local Disk (C:) 149.9 GB

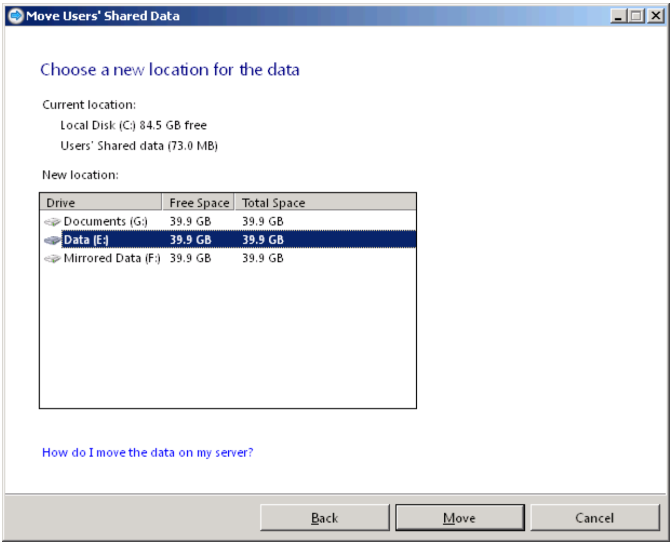
Used Space:	SharePoint Foundation Data	247.5 MB
	Exchange Server Data	317.7 MB
	Users' Shared Data	0 KB
	Users' Redirected Documents Data	0 KB
	Windows Update Repository Data	244.2 MB
	Other	32 GB
Free Space:	117.1 GB	

4 items

- Move Exchange Server Data
- Move SharePoint Foundation Data
- Move Users' Shared Data
- Move Users' Redirected Documents Data
- Move Windows Update Repository Data
- Tell me more about managing storage of server data
- Refresh this view

4. In the Tasks pane, click one of these tasks:
   - *Move Exchange Server data*
   - *Move SharePoint Foundation data*
   - *Move users' shared data*
   - *Move users' redirected documents data*
   - *Move Windows Update repository data*

   The Move Data Wizard for the task you selected appears, displaying the Getting Started page.
5. Click *Next*. The Choose A New Location For The Data page appears.



Choose a new location for the data

Current location:

Local Disk (C:) 84.5 GB free

Users' Shared data (73.0 MB)

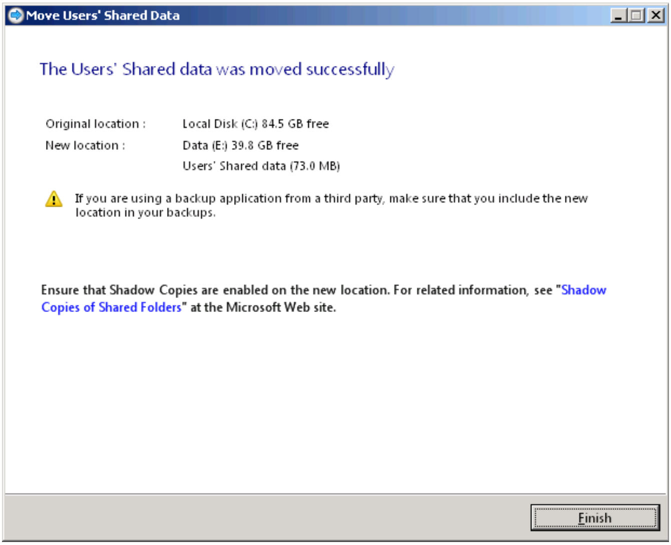
New location:

Drive	Free Space	Total Space
Documents (G:)	39.9 GB	39.9 GB
Data (E:)	39.9 GB	39.9 GB
Mirrored Data (F:)	39.9 GB	39.9 GB

How do I move the data on my server?

NOTE **If you have not configured a backup job yet or if you are using a product other than Windows Server Backup to perform your backups, a message box appears, warning you to back up your data before you attempt to move it.**

6. In the *New location* list, select the volume where you want to store the data and click *Move*. The wizard moves the data to the selected volume and reconfigures Windows SBS 2011 to access the data from its new location. A page appears, indicating that the data was moved successfully.



The Users' Shared data was moved successfully

Original location :	Local Disk (C:) 84.5 GB free
New location :	Data (E:) 39.8 GB free
	Users' Shared data (73.0 MB)

⚠ If you are using a backup application from a third party, make sure that you include the new location in your backups.

Ensure that Shadow Copies are enabled on the new location. For related information, see "Shadow Copies of Shared Folders" at the Microsoft Web site.

7. Click *Finish*.

NOTE **Once you have moved data to a new location, be sure to enable shadow copies on the new folder and reconfigure your backup software to find the data on its new volume.**

There is no wizard to move shares that you have created yourself. To move manually created shares, you must stop sharing them, move the folders to the new location, re-create the NTFS permissions, if necessary, and then share the folders again.

Using the Default Shares

As you have learned in previous chapters, creating volumes makes a hard disk accessible to the operating system, but to make the volumes accessible to users on the network, you must create shared folders on them. Windows SBS 2011 creates a number of shared folders, commonly called *shares*, during the installation process. Some of these shares are intended for use by applications, such as Microsoft Exchange Server and WSUS, but the following three shares are meant for direct access by users:

- **Public** Contains folders accessible to everyone, for the purpose of storing files that individuals want to share with other users on the network
- **RedirectedFolders** Contains the user profile folders for each account that has folder redirection enabled
- **UserShares** Contains a subfolder for each user on the network, to which only that user has access permissions

You can also create as many additional shares on your server as you need to support your users.

NOTE **To create shares, you can use the Provision A Shared Folder Wizard, accessible from the Windows SBS Console or the Share And Storage Management Console. You can also create shares directly from a folder's Properties sheet.**

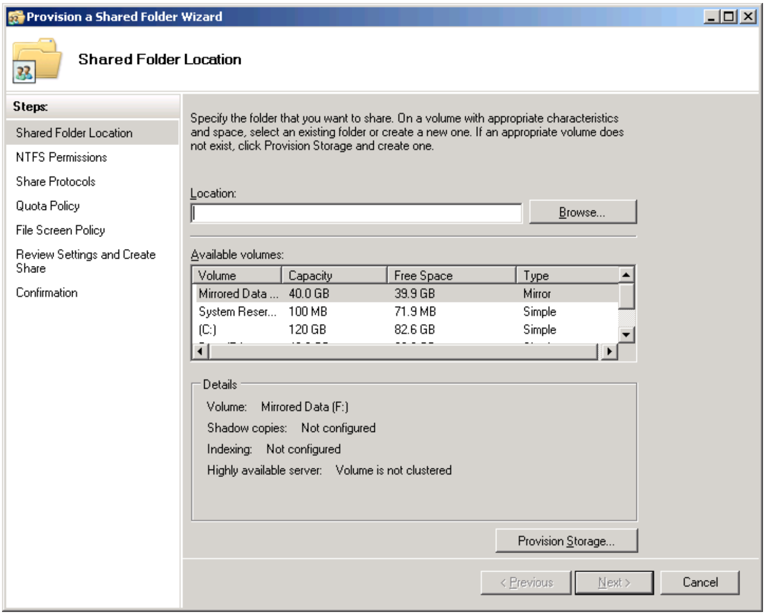
Working with Shares

Once you have created volumes on your server disks, you are ready to create shares. The Windows SBS Console provides access to the Provision A Shared Folder Wizard, which is the same tool you can use to create shares in the Share And Storage Management Console, a tool included with Windows Server 2008 R2. Once you have created shares, you can manage their basic properties from within the Windows SBS Console as well.

Creating a New Share Using Windows SBS Console

To create a new shared folder or volume with the Windows SBS Console, use the following procedure:

1. Log on to your Windows SBS 2011 server, using an account with network Administrator privileges. The Windows SBS Console appears.
2. Click *Shared folders and web sites* and then select the *Shared folders* tab.
3. In the *Tasks* list, click *Add a new shared folder*. The Provision A Shared Folder Wizard appears, displaying the Shared Folder Location page.



Provision a Shared Folder Wizard

Shared Folder Location

Specify the folder that you want to share. On a volume with appropriate characteristics and space, select an existing folder or create a new one. If an appropriate volume does not exist, click Provision Storage and create one.

Location:

Available volumes:

Volume	Capacity	Free Space	Type
Mirrored Data ...	40.0 GB	39.9 GB	Mirror
System Reser...	100 MB	71.9 MB	Simple
(C:)	120 GB	82.6 GB	Simple

Details

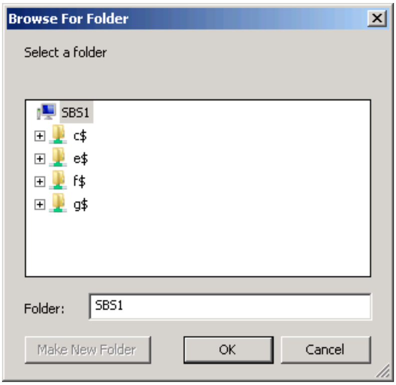
Volume: Mirrored Data (F:)

Shadow copies: Not configured

Indexing: Not configured

Highly available server: Volume is not clustered

4. Click *Browse*. The Browse For Folder dialog box appears.



Browse For Folder

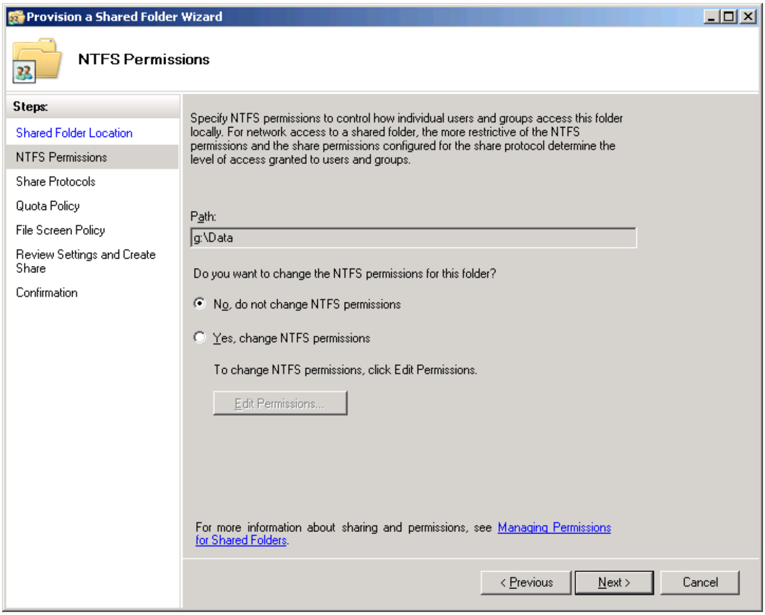
Select a folder

Folder: SBS1

5. Select the volume on which you want to create the share. If you want to share a folder on the volume, browse to the folder and select it. You can also click *Make new folder* to create and share a folder on the selected volume. Then click *OK*.

   MORE INFO You can click *Provision storage* to start the Provision Storage Wizard, which enables you to create new volumes. However, this wizard can create only simple volumes. To create a striped, spanned, mirrored, or RAID-5 volume, use the Disk Management snap-in or the Diskpart.exe command line utility, as described in Chapter 7.

6. Click *Next*. The NTFS Permissions page appears.



Specify NTFS permissions to control how individual users and groups access this folder locally. For network access to a shared folder, the more restrictive of the NTFS permissions and the share permissions configured for the share protocol determine the level of access granted to users and groups.

Path:
g:\Data

Do you want to change the NTFS permissions for this folder?

● No, do not change NTFS permissions

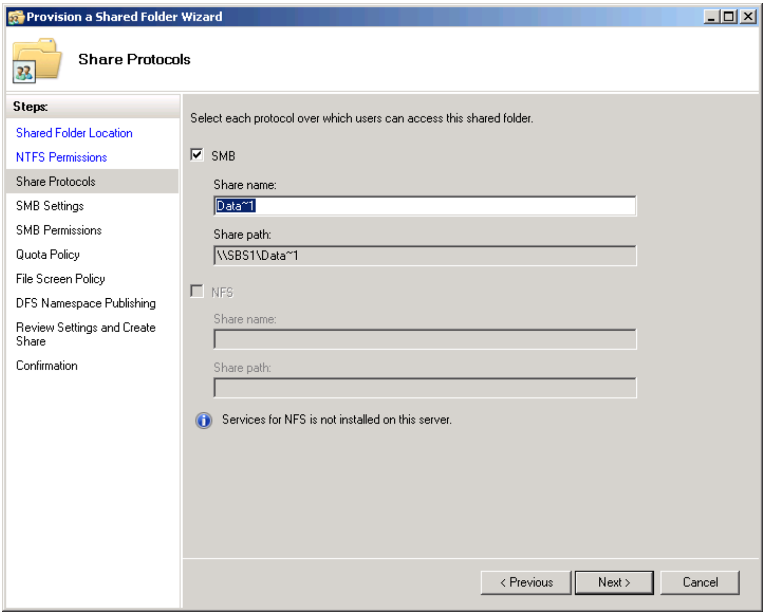
○ Yes, change NTFS permissions

To change NTFS permissions, click Edit Permissions.

For more information about sharing and permissions, see Managing Permissions for Shared Folders.

   MORE INFO For more information on using NTFS permissions, see Chapter 8, "Working with Permissions."

7. Leave the default *No, do not change NTFS permissions* option selected and click *Next*. The Share Protocols page appears.



Select each protocol over which users can access this shared folder.

☑ SMB

Share name: Data~1

Share path: \\SBS1\Data~1

□ NFS

Share name:

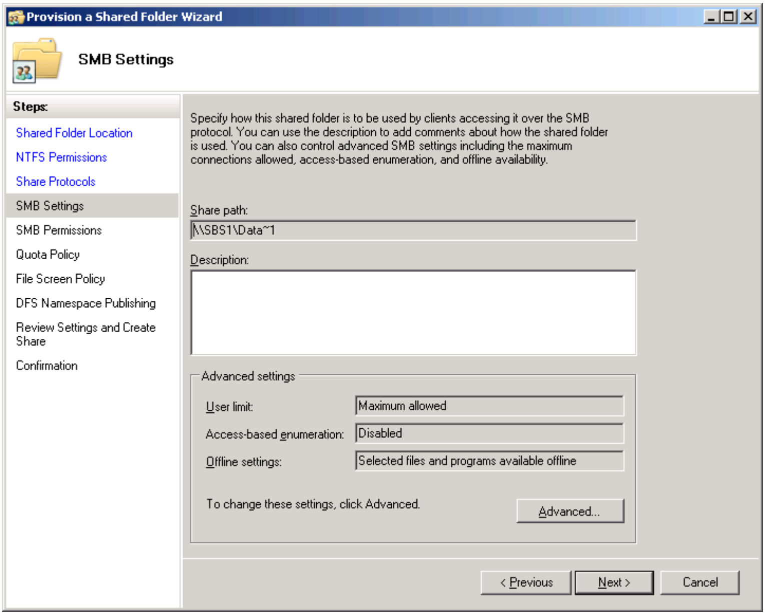
Share path:

Services for NFS is not installed on this server.

8. Leave the *SMB* check box selected and in the *Share name* text box, type the name under which the share will appear on the network.

   NOTE **The *NFS* option is dimmed because the Services for Network File System role service is not installed on the server running Windows SBS 2011 by default. Network File System (NFS) is a file sharing protocol used by most UNIX and Linux distributions. If you have UNIX or Linux clients that need access to your Windows shares, you can install the role service and configure your shares to use NFS as well as Server Message Block (SMB) file sharing.**

9. Click *Next*. The SMB Settings page appears.


Provision a Shared Folder Wizard

SMB Settings

Steps:
- Shared Folder Location
- NTFS Permissions
- Share Protocols
- SMB Settings
- SMB Permissions
- Quota Policy
- File Screen Policy
- DFS Namespace Publishing
- Review Settings and Create Share
- Confirmation

Specify how this shared folder is to be used by clients accessing it over the SMB protocol. You can use the description to add comments about how the shared folder is used. You can also control advanced SMB settings including the maximum connections allowed, access-based enumeration, and offline availability.

Share path: \\SBS1\Data~1

Description:

Advanced settings

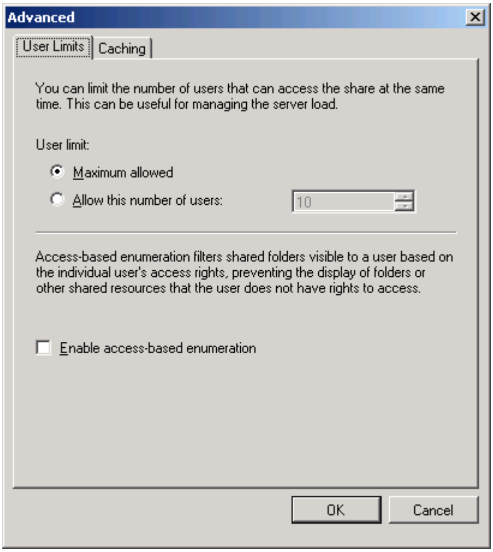
User limit: Maximum allowed

Access-based enumeration: Disabled

Offline settings: Selected files and programs available offline

To change these settings, click Advanced.

10. Click *Advanced* to open the Advanced dialog box, in which you can configure the following SBS settings:
    - **User limits** Specifies the maximum number of users allowed to access the share at one time.


Advanced

You can limit the number of users that can access the share at the same time. This can be useful for managing the server load.

User limit:

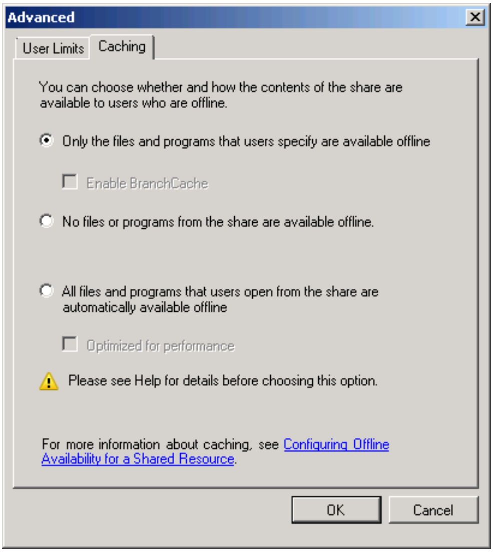
● Maximum allowed

○ Allow this number of users: 10

Access-based enumeration filters shared folders visible to a user based on the individual user's access rights, preventing the display of folders or other shared resources that the user does not have rights to access.

□ Enable access-based enumeration

- **Access-based enumeration** When enabled, allows only the users with access permissions to see the share on the network.
- **Offline settings** Specifies whether users can save copies of the files in the share to local drives using Offline Files.



You can choose whether and how the contents of the share are available to users who are offline.

● Only the files and programs that users specify are available offline

□ Enable BranchCache

○ No files or programs from the share are available offline.

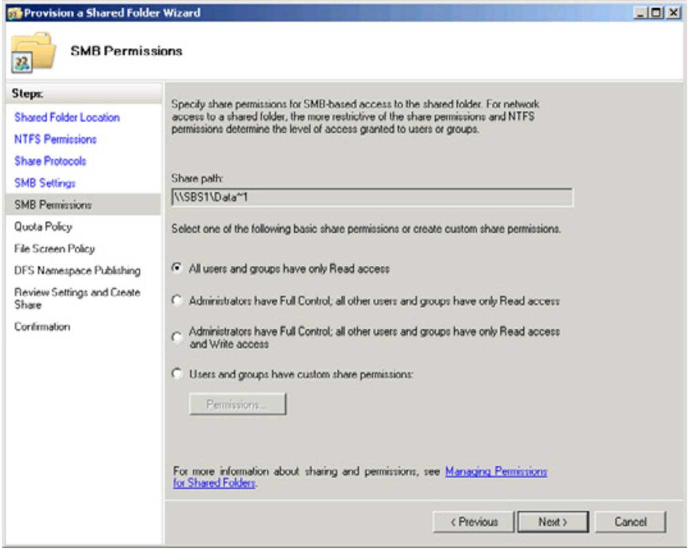
○ All files and programs that users open from the share are automatically available offline

□ Optimized for performance

Please see Help for details before choosing this option.

For more information about caching, see Configuring Offline Availability for a Shared Resource.

11. Click *OK* to close the Advanced dialog box.
12. Click *Next*. The SMB Permissions page appears.



Specify share permissions for SMB-based access to the shared folder. For network access to a shared folder, the more restrictive of the share permissions and NTFS permissions determine the level of access granted to users or groups.

Share path:
\\SBS1\Data~1

Select one of the following basic share permissions or create custom share permissions.

● All users and groups have only Read access

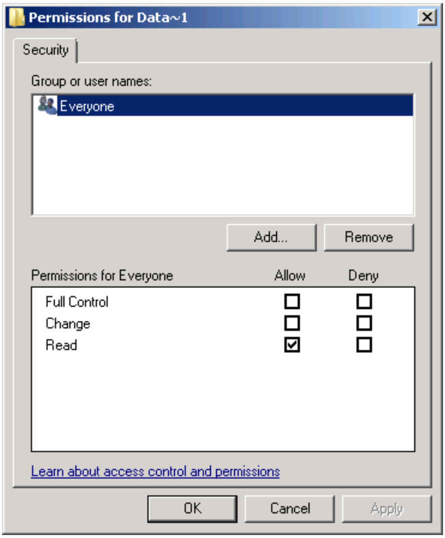
○ Administrators have Full Control; all other users and groups have only Read access

○ Administrators have Full Control; all other users and groups have only Read access and Write access

○ Users and groups have custom share permissions:

For more information about sharing and permissions, see Managing Permissions for Shared Folders.

13. Select one of the preset permission options or click *Permissions* to open a Permissions dialog box, in which you can specify the share permissions you want to assign to your users.

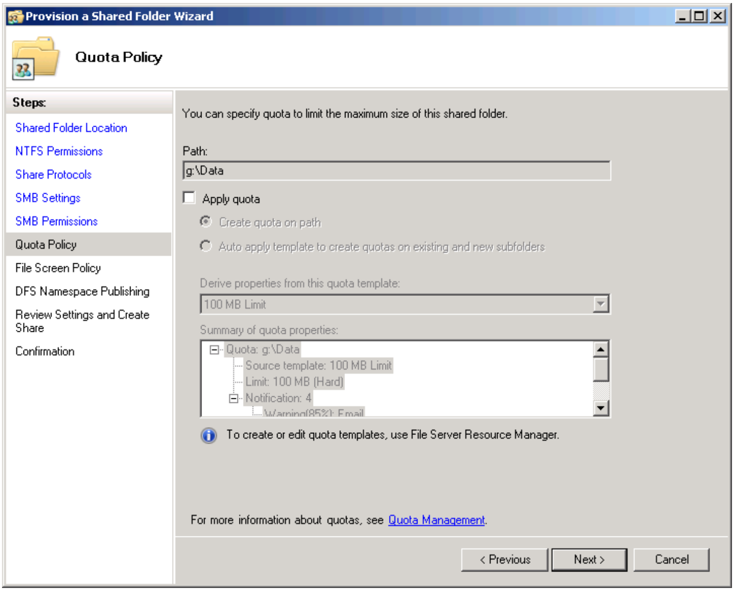


Group or user names:

Everyone

Permissions for Everyone	Allow	Deny
Full Control	□	□
Change	□	□
Read	☑	□

14. Click *Next*. The Quota Policy page appears.



You can specify quota to limit the maximum size of this shared folder.

Path: g:\Data

□ Apply quota

● Create quota on path

○ Auto apply template to create quotas on existing and new subfolders

Derive properties from this quota template: 100 MB Limit

Summary of quota properties:

```
⊟ Quota: g:\Data
   Source template: 100 MB Limit
   Limit: 100 MB (Hard)
  ⊟ Notification: 4
     Warning(85%): Email
```

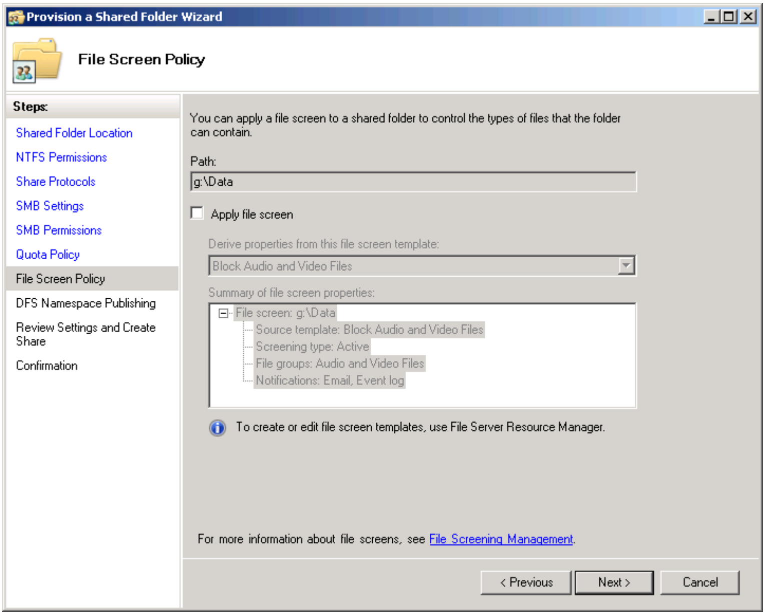
To create or edit quota templates, use File Server Resource Manager.

For more information about quotas, see Quota Management.

To set a quota on disk space consumption for each user, select the *Apply quota* check box and then select *Quota* options and a quota template.

MORE INFO **For more information on using quotas, see the section entitled "Enforcing Quotas," later in this chapter.**

15. Click *Next*. The File Screen Policy page appears.



You can apply a file screen to a shared folder to control the types of files that the folder can contain.

Path: g:\Data

☐ Apply file screen

Derive properties from this file screen template: Block Audio and Video Files

Summary of file screen properties:

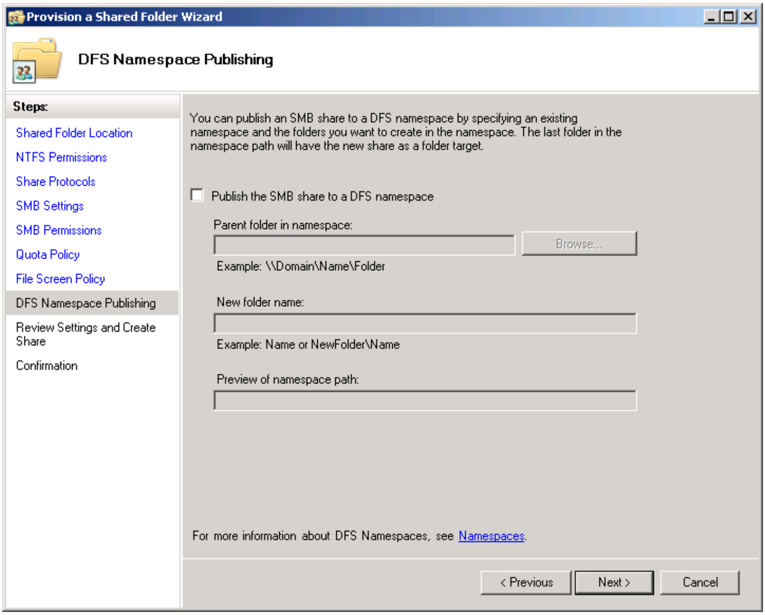
- File screen: g:\Data
  - Source template: Block Audio and Video Files
  - Screening type: Active
  - File groups: Audio and Video Files
  - Notifications: Email, Event log

To create or edit file screen templates, use File Server Resource Manager.

For more information about file screens, see File Screening Management.

To use file screening, select the *Apply file screen* check box and then select a file screen template.

16. Click *Next*. The DFS Namespace Publishing page appears.



You can publish an SMB share to a DFS namespace by specifying an existing namespace and the folders you want to create in the namespace. The last folder in the namespace path will have the new share as a folder target.

□ Publish the SMB share to a DFS namespace

Parent folder in namespace:

Example: \\Domain\Name\Folder

New folder name:

Example: Name or NewFolder\Name

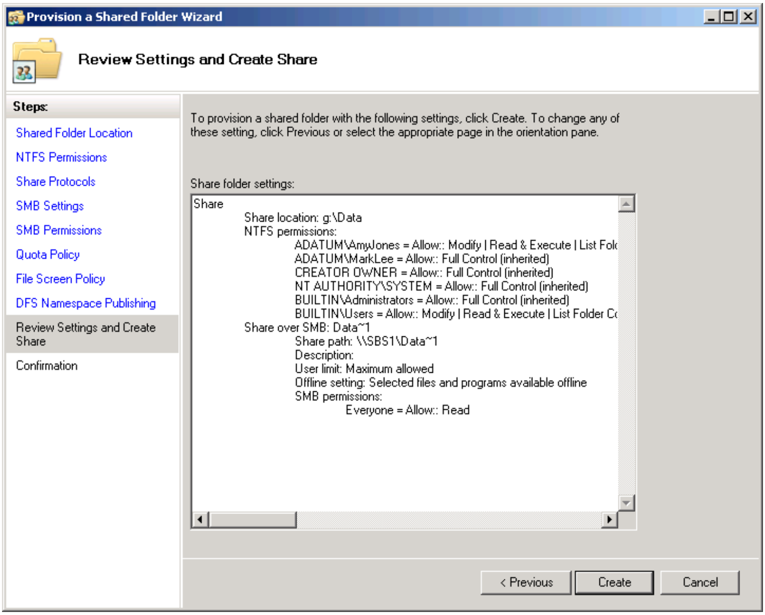
Preview of namespace path:

For more information about DFS Namespaces, see Namespaces.

To add the share to a DFS namespace, select the *Publish the SMB share to a DFS namespace* check box and specify a namespace location and a folder name.

NOTE **The Distributed File System (DFS) is a feature of Windows Server 2008 R2 that enables you to combine shares from various locations into a single virtual namespace. To use DFS, you must install the File Services\Distributed File Services role service using the Server Manager Console and then create and configure a DFS namespace.**

17. Click *Next*. The Review Settings And Create Share page appears.

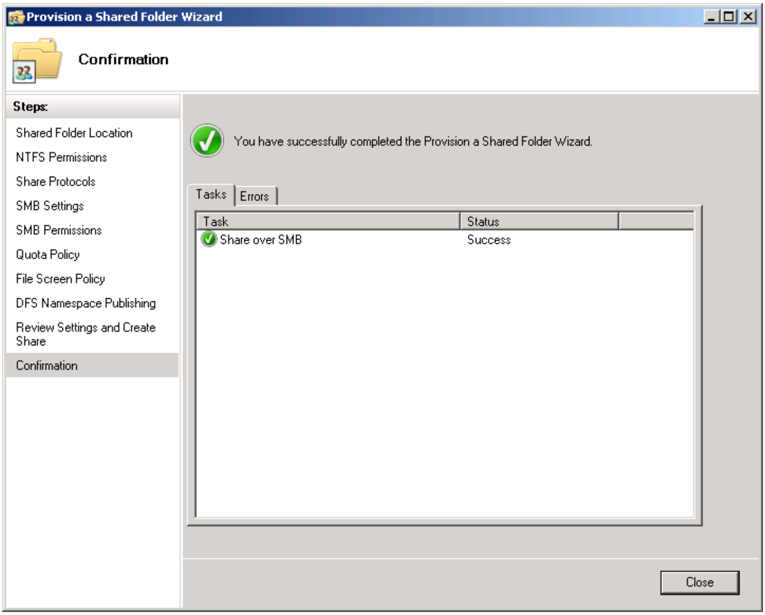


To provision a shared folder with the following settings, click Create. To change any of these setting, click Previous or select the appropriate page in the orientation pane.

Share folder settings:

```
Share
        Share location: g:\Data
        NTFS permissions:
                ADATUM\AmyJones = Allow:: Modify | Read & Execute | List Folc
                ADATUM\MarkLee = Allow:: Full Control (inherited)
                CREATOR OWNER = Allow:: Full Control (inherited)
                NT AUTHORITY\SYSTEM = Allow:: Full Control (inherited)
                BUILTIN\Administrators = Allow:: Full Control (inherited)
                BUILTIN\Users = Allow:: Modify | Read & Execute | List Folder Cc
        Share over SMB: Data~1
                Share path: \\SBS1\Data~1
                Description:
                User limit: Maximum allowed
                Offline setting: Selected files and programs available offline
                SMB permissions:
                        Everyone = Allow:: Read
```

18. Click *Create*. The wizard creates the share and the Confirmation page appears.



You have successfully completed the Provision a Shared Folder Wizard.

Task	Status
✓ Share over SMB	Success

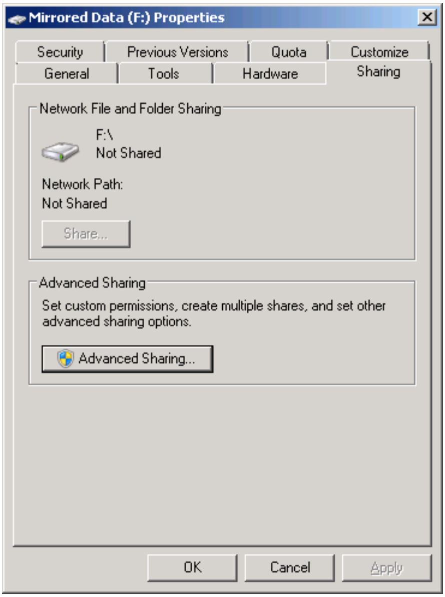
19. Click *Close*. The wizard closes.

Creating a New Share Using Windows Explorer

It is also possible to create a share outside of the Windows SBS Console, by accessing the folder itself in the Windows Explorer interface. These two share creation methods are interchangeable; shares you create in the Windows SBS Console appear as shared in Windows Explorer, and shares you create in Windows Explorer appear on the Shared Folders tab in Windows SBS Console. The main difference between the two methods is that the Windows SBS Console provides more comprehensive control over the share and all the necessary permissions, but for most administrators, which tool you use is a matter of personal preference.

To create a share in Windows Explorer, do the following:

1. Log on to your Windows SBS 2011 Server, using an account with network Administrator privileges.
2. Click *Start*. Then click *All Programs* > *Accessories* > *Windows Explorer*. The Windows Explorer window appears.
3. Browse to the folder you want to share, right-click it, and from the context menu, select *Properties*. The Properties sheet for the share appears.
4. Click the *Sharing* tab.



Network File and Folder Sharing

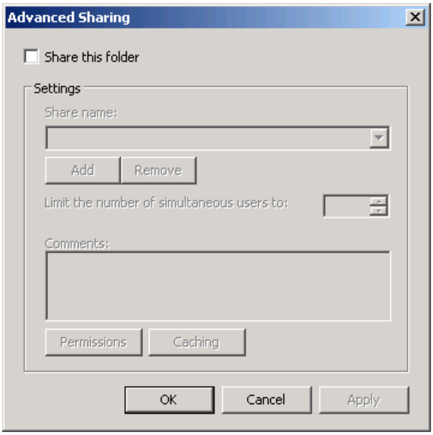
F:\
Not Shared

Network Path:
Not Shared

Advanced Sharing

Set custom permissions, create multiple shares, and set other advanced sharing options.

5. Click *Advanced sharing*. The Advanced Sharing dialog box appears.


Advanced Sharing

□ Share this folder

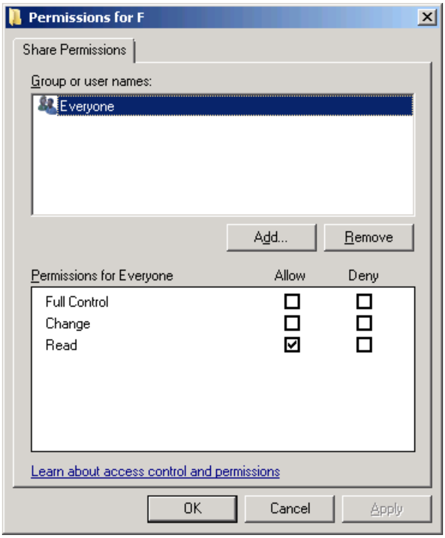
Settings

Share name:

Limit the number of simultaneous users to:

Comments:

6. Select the *Share this folder* check box.
7. In the *Share name* text box, type the name under which the share will appear on the network.
8. Click *Permissions*. The Permissions dialog box for the share appears.


Permissions for F

Share Permissions

Group or user names:

Everyone

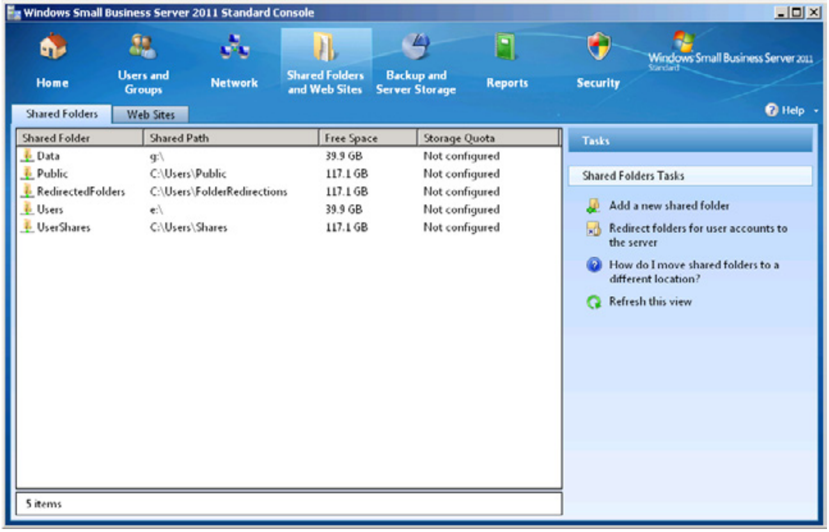
Permissions for Everyone	Allow	Deny
Full Control	□	□
Change	□	□
Read	☑	□

9. Specify the permissions you want to assign to the share and click *OK*.
10. Click *OK* to close the Advanced Sharing dialog box.
11. Click *Close* to close the Properties sheet.

NOTE Unlike the Provision A Shared Folder Wizard, the Advanced Sharing dialog box does not provide the ability to set NTFS permissions or configure SMB settings, file quotas, file screen policies, or DFS namespace settings as you create the share. You can, however, configure these settings after you have created the share, using the various tools available in Windows Server 2008 R2.

Managing Shares

Using the Windows SBS Console, you can view all the shared folders on your server, both the default shares and any new ones you have created. To view the shares, open the Shared Folders And Web Sites page, and then click the *Shared folders* tab, as shown in Figure 9-1. By selecting a share and using the controls in the *Tasks* list, you can stop sharing the folder or modify its properties, as described in the following sections.


Windows Small Business Server 2011 Standard Console
Home
Users and Groups
Network
Shared Folders and Web Sites
Backup and Server Storage
Reports
Security
Windows Small Business Server 2011 Standard
Help
Shared Folders
Web Sites

Shared Folder	Shared Path	Free Space	Storage Quota
Data	g:\	39.9 GB	Not configured
Public	C:\Users\Public	117.1 GB	Not configured
RedirectedFolders	C:\Users\FolderRedirections	117.1 GB	Not configured
Users	e:\	39.9 GB	Not configured
UserShares	C:\Users\Shares	117.1 GB	Not configured

5 items

Tasks

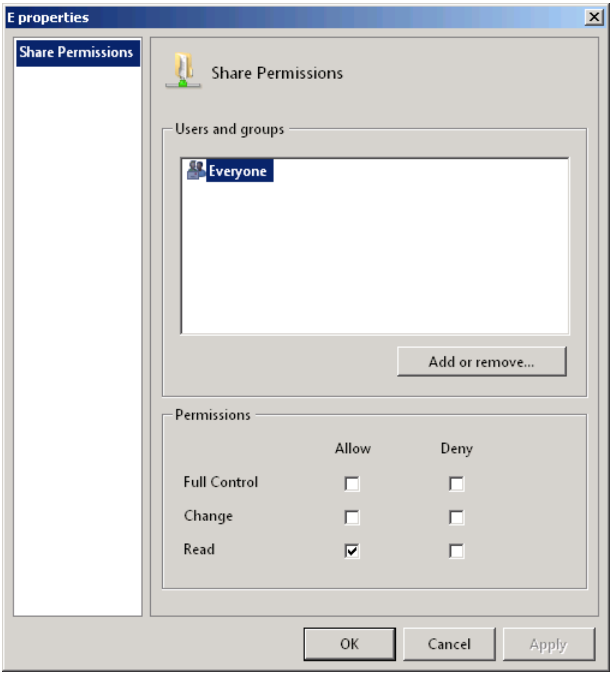
Shared Folders Tasks

- Add a new shared folder
- Redirect folders for user accounts to the server
- How do I move shared folders to a different location?
- Refresh this view

FIGURE 9-1 The *Shared folders* tab in the Windows SBS Console.

Configuring Share Permissions Using Windows SBS Console

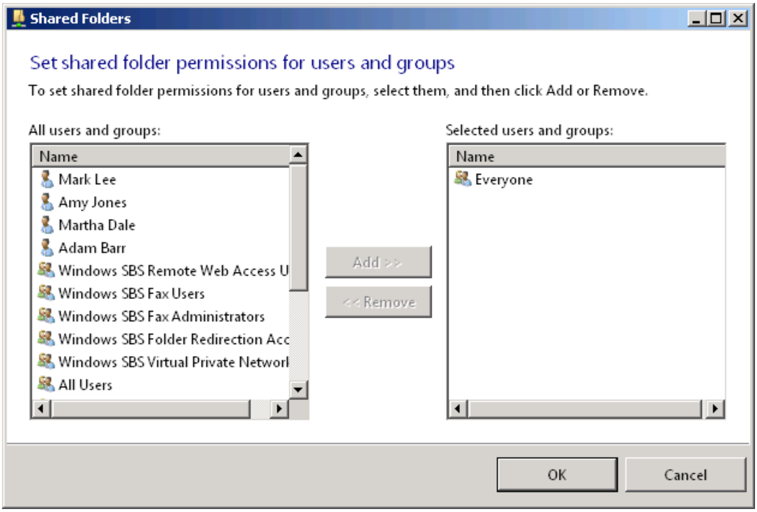
To change a share's permissions, you must first open its Properties sheet. Select the share and then select *Change folder permissions* from the *Tasks* list to open the share's Properties sheet. Then select an entry in the *Users and groups* list to see the share permissions assigned to that entry. For example, Figure 9-2 shows that *Everyone* has the *Allow read* permission.



	Allow	Deny
Full Control	□	□
Change	□	□
Read	☑	□

FIGURE 9-2 The Properties sheet for a shared folder in the Windows SBS Console.

For the default shares, Windows SBS 2011 grants the *Allow full control* permission to the *Everyone* special identity. Changing the permissions for the default shares is not recommended. The shares you create yourself receive the permissions that you specify in the Provision A Shared Folder Wizard. You can modify these permissions by selecting an entry in the *Users and groups* list and selecting the check boxes for the permissions you want to assign. To manage the entries in the list, click *Add or remove* to display the Shared Folders dialog box, as shown in Figure 9-3.



Shared Folders

Set shared folder permissions for users and groups

To set shared folder permissions for users and groups, select them, and then click Add or Remove.

All users and groups:

Name
Mark Lee
Amy Jones
Martha Dale
Adam Barr
Windows SBS Remote Web Access U
Windows SBS Fax Users
Windows SBS Fax Administrators
Windows SBS Folder Redirection Acc
Windows SBS Virtual Private Networl
All Users

Selected users and groups:

Name
Everyone

FIGURE 9-3 The Shared Folders dialog box in the Windows SBS Console.

> ***BEST PRACTICES*** **Remember that in addition to share permissions, users must have the appropriate NTFS permissions to access a shared folder. To simplify the administration of your shares, the recommended practice is to always grant *Everyone* the *Allow full control* share permission and use NTFS permissions to control access to the shared folders.**

Configuring Share Permissions Using Windows Explorer

Whether you create a folder share with the Windows SBS Console or with Windows Explorer, you can use either tool to modify its share permission assignments. To manage share permissions using the Windows Explorer interface, you open the Advanced Sharing dialog box and click the *Permissions* button, just as you did earlier when creating a share.

Using Folder Redirection

It is preferable to store user data on server drives rather than local workstation drives for several reasons:

- **Backups** Backing up one or two servers is much faster, easier, and often cheaper than backing up multiple workstations.
- **Mobility** With all data files stored on server drives, users can work from any computer and move to another location as needed.
- **Replacement** Deploying new client computers in the place of older ones is a simple matter of replacing the hardware; no migration of data files is necessary.

Folder redirection is a Windows feature that enables client workstations to store the contents of their data folders on a server drive automatically. The process is completely invisible to the workstation user.

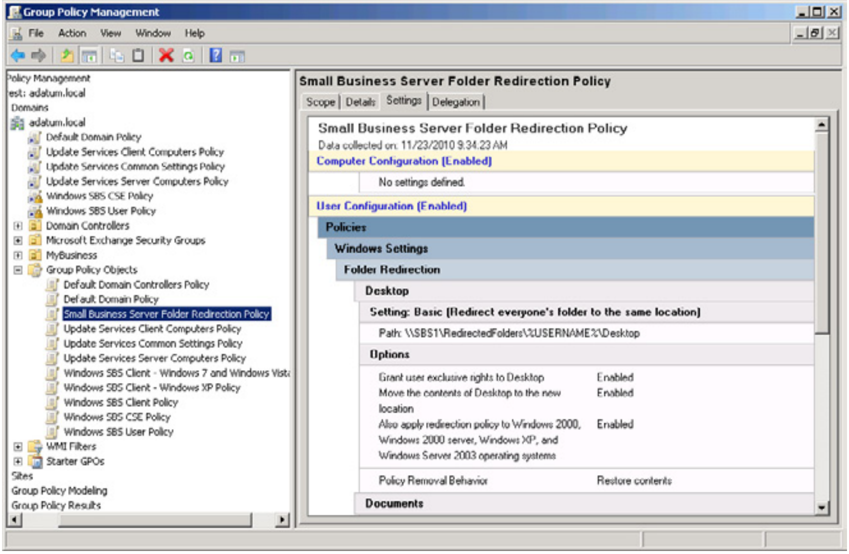
A Windows workstation creates a folder for each person who logs on at the computer in the C:\Users folder. Each of these user folders contains a separate user profile for that person. A *user profile* is a set of folders and registry files that store the documents and configuration settings belonging to a particular user. A typical user profile consists of the folders listed in Table 9-1, some of which are hidden, plus a hidden registry file.

TABLE 9-1 User Profile Folders

VISIBLE FOLDERS	HIDDEN FOLDERS
Contacts	AppData
Desktop	Application Data
Documents	Cookies
Downloads	Local Settings
Favorites	My Documents
Links	NetHood
Music	PrintHood
Pictures	Recent
Saved Games	Send To
Searches	Start Menu
Videos	Templates

To a user viewing his or her own profile, the Documents, Music, Pictures, and Video folders appear as My Documents, My Music, My Pictures, and My Video, respectively. When a user logs on at the workstation using a local or domain account, the system loads that individual's profile and uses it throughout the session until the user logs off. During the session, the My Documents folder in the user's profile becomes the operative My Documents folder for the system, as do all the other folders in the profile. Folder redirection is simply a means of storing a copy of certain user profile folders on another computer, usually a file server. Once the folders are redirected to the server, that user can log on at any computer, and the system copies the redirected folders to the user's local profile on that computer.

Windows SBS 2011 implements folder redirection using Group Policy settings that specify which folders to redirect and where to store them, as shown in Figure 9-4. During the operating system installation, the Windows SBS 2011 setup program creates a Group Policy object (GPO) called Small Business Server Folder Redirection Policy and links it to the *domain*/MyBusiness/Users/SBSUsers organizational unit object. This way, every user on the network loads the GPO during the domain logon process.


Group Policy Management
File
Action
View
Window
Help
Policy Management
est: adatum.local
Domains
adatum.local
Default Domain Policy
Update Services Client Computers Policy
Update Services Common Settings Policy
Update Services Server Computers Policy
Windows SBS CSE Policy
Windows SBS User Policy
Domain Controllers
Microsoft Exchange Security Groups
MyBusiness
Group Policy Objects
Default Domain Controllers Policy
Default Domain Policy
Small Business Server Folder Redirection Policy
Update Services Client Computers Policy
Update Services Common Settings Policy
Update Services Server Computers Policy
Windows SBS Client - Windows 7 and Windows Vist
Windows SBS Client - Windows XP Policy
Windows SBS Client Policy
Windows SBS CSE Policy
Windows SBS User Policy
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
Small Business Server Folder Redirection Policy
Scope
Details
Settings
Delegation

Small Business Server Folder Redirection Policy
Data collected on: 11/23/2010 9:34:23 AM

Computer Configuration (Enabled)

No settings defined.

User Configuration (Enabled)

Policies

Windows Settings

Folder Redirection

Desktop

Setting: Basic (Redirect everyone's folder to the same location)

Path: \\SBS1\RedirectedFolders\%USERNAME%\Desktop

Options

Grant user exclusive rights to Desktop	Enabled
Move the contents of Desktop to the new location	Enabled
Also apply redirection policy to Windows 2000, Windows 2000 server, Windows XP, and Windows Server 2003 operating systems	Enabled
Policy Removal Behavior	Restore contents

Documents

FIGURE 9-4 Policy settings in the Small Business Server Folder Redirection Policy GPO.

Understanding the Folder Redirection Defaults

The Group Policy settings for folder redirection are located in the GPO in the following container: User Configuration\Policies\Windows Settings\Folder Redirection, as shown in Figure 9-5. By default, Windows SBS 2011 redirects only the Desktop and Documents folders, along with the Music, Pictures, and Videos subfolders beneath the Documents folder.

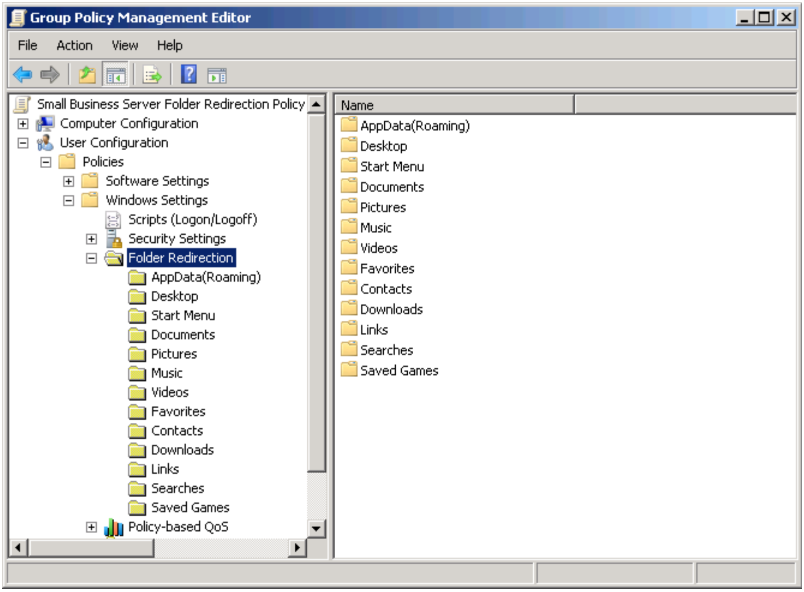
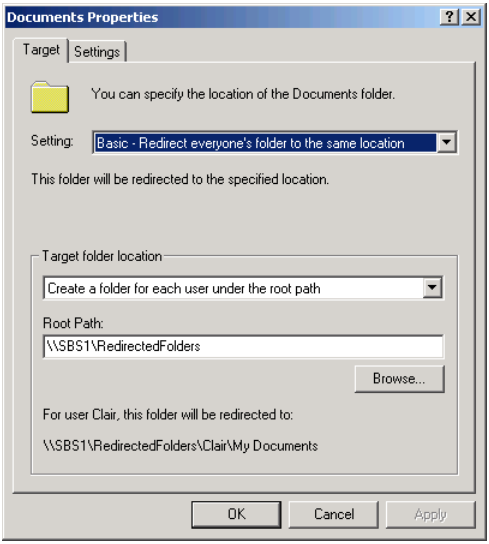


FIGURE 9-5 The Folder Redirection policies in a GPO.

You can modify the settings in the Small Business Server Folder Redirection Policy GPO with the Group Policy Management Editor Console by right-clicking one of the folders under the *Folder redirection* node and opening its Properties sheet, as shown in Figure 9-6. The most common modification that administrators are likely to make is to redirect additional folders, such as Startup and Favorites, to provide users with a more complete server-based environment.



You can specify the location of the Documents folder.

Setting: Basic - Redirect everyone's folder to the same location

This folder will be redirected to the specified location.

Target folder location

Create a folder for each user under the root path

Root Path:

\\SBS1\RedirectedFolders

For user Clair, this folder will be redirected to:

\\SBS1\RedirectedFolders\Clair\My Documents

FIGURE 9-6 The Properties sheet for a Folder Redirection policy.

Table 9-2 lists the default settings for the Desktop and Documents folders and explains their functions. The Music, Pictures, and Videos folders have only one setting: Follow the Documents Folder, which causes the workstation to treat them as subfolders beneath the Documents folder and redirect them using the Documents folder settings.

TABLE 9-2 Default Folder Redirection Group Policy Settings for the Desktop and Documents Folders

SETTING	DEFAULT VALUE	FUNCTION
Setting	Basic—Redirect Everyone's Folder to the Same Location	Causes workstations to redirect the Desktop or Documents folder for all users to the same server share. The alternative is to redirect the folders to different locations based on group memberships.

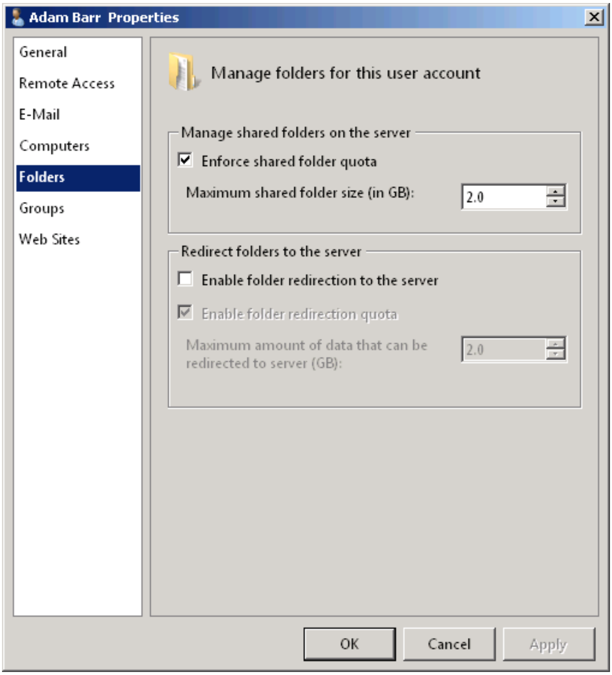
SETTING	DEFAULT VALUE	FUNCTION
Target Folder Location	Create a Folder for Each User Under the Root Path	Causes workstations to create a separate folder for each user on the server share. The alternatives are to redirect the folders to each user's home directory, to a single folder for all users, or to the user's local userprofile location.
Root Path	\\SERVER\Redirectedfolders	Specifies the server share where you want to store the redirected folders.
Grant the User Exclusive Rights to Desktop/Documents	Enabled	Prevents anyone except the user from receiving permission to access the redirected folder.
Move The Contents of Desktop/Documents to the New Location	Enabled	Causes the workstation to copy the contents of the redirected folders on its local drive to the target folder on the server share.
Also Apply Redirection Policy To Windows 2000, Windows 2000 Server, Windows XP, And Windows Server 2003 Operating Systems	Enabled	Provides compatibility with earlier operating systems that use different folder names in their user profiles, such as My Documents.
Policy Removal	Redirect the Folder Back to the Local User-profile Location When Policy Is Removed	Causes the workstation to copy the contents of the redirected folders back to the local drive in the event that an administrator disables the Folder Redirection Group Policy settings. The alternative is to direct the folders back to the local drives without copying their contents from the server, thus rendering those contents inaccessible.

TIP **If you have migrated to Windows SBS 2011 from Windows SBS 2008 or Windows SBS 2003, you will likely have a Small Business Server Folder Redirection GPO on your new server that was migrated from your old server. If this is the case, the Root Path setting in that GPO will contain the UNC name of your old server. Before Folder Operation will function on your network, you must change this setting to point to the name of your new server running Windows SBS 2011.**

Enabling Folder Redirection

Although Windows SBS 2011 creates the Small Business Server Folder Redirection Policy GPO by default, and even creates a folder for each user in the FolderRedirections share, it does not enable folder redirection for each user by default. To enable folder redirection, perform these steps:

1. Log on to your Windows SBS 2011 server, using an account with network Administrator privileges. The Windows SBS Console appears.
2. Click *Users and Groups*, and then select the *Users* tab.
3. Select one of the users in the list and, in the *Tasks* list, select *Edit user account properties*. The Properties sheet for the user account appears.
4. Click the *Folders* tab.



Manage folders for this user account

Manage shared folders on the server

☑ Enforce shared folder quota

Maximum shared folder size (in GB): 2.0

Redirect folders to the server

□ Enable folder redirection to the server

☑ Enable folder redirection quota

Maximum amount of data that can be redirected to server (GB): 2.0

5. Select the *Enable folder redirection to the server* check box.

   Enabling folder redirection also imposes a 2 GB quota on the user's redirection folder by default. To modify this default, clear the *Enable folder redirection quota* check box to disable the quota or modify the value in the *Maximum amount of data that can be redirected to server (GB)* spin box.

6. Click *OK* to close the Properties sheet.

Moving Redirected Folders

Although you can change the location of your users' redirected folders by modifying the Root Path setting in the Small Business Server Folder Redirection Policy GPO, it is far easier to use the Move Users' Redirected Documents Data Wizard in the Windows SBS Console. The wizard not only changes the Group Policy settings but it also modifies the permissions for the target folder and creates the necessary share for you automatically.

To start the Move Users' Redirected Documents Data Wizard, use the procedure in "Moving Data Stores," earlier in this chapter, and select the Move Users' Redirected Documents Data task. The wizard then prompts you for a new location and moves the folders.

Enforcing Quotas

One of the longstanding rules of personal computing is that no matter how much disk space you have in a computer, you eventually end up filling it and needing more. In a server environment, the problem of disk space consumption is compounded by the number of users storing their files on the server drives. Windows SBS 2011 helps administrators to address this problem by establishing quotas that limit the amount of server disk space a user can consume.

For each user account you create, Windows SBS 2011 creates two *quotas*: one for the user's folder in UserShares and one for the user's folder in RedirectedFolders. The user's UserShares folder has a 2 GB hard quota, by default. A *hard quota* is one in which the system prevents the user from consuming more than a specified amount of disk space. When the user's disk space consumption reaches 85 percent of the 2 GB, the system sends a warning email to the user and the administrator, and records an event in the system log. If the user consumes the entire 2 GB, the server stops accepting data. To the user, it appears as if the server has run out of disk space, although in reality, it is only that user's space that has been consumed.

As mentioned in the previous procedure, there is also a 2 GB quota on the user's folder in RedirectedFolders. However, this is a 2 GB soft quota. A *soft quota* generates the same warnings to the user and administrator as a hard quota, but it does not prevent the user from exceeding the allotted amount of disk space. A soft quota, therefore, is only a warning that serves to inform users and administrators of the user's current disk consumption.

The main reason for using a soft quota, in this case, is to prevent applications that store their data in the user's redirected folders from running out of disk space, causing errors that could affect the functionality of the application.

As mentioned earlier, the Add A New User Account Wizard creates the two quotas for each user account, but it is up to you, the administrator, to enable them. You can also modify the default amount of disk space you allot to each user individually. To enable the quotas for an existing user account, use the following procedure:

1. Log on to your Windows SBS 2011 Server, using an account with network Administrator privileges. The Windows SBS Console appears.
2. Click *Users and groups*, and then select the *Users* tab.
3. Select one of the users in the list, and in the *Tasks* list, select *Edit user account properties*. The Properties sheet for the user account appears.
4. Click the *Folders* tab.
5. Select the *Enforce shared folder quota* check box and modify the *Maximum shared folder size* setting, if desired.
6. Select the *Enable folder redirection to the server* check box and modify the *Maximum amount of data that can be redirected to server* setting, if desired.
7. Click *OK*.

TIP **For more detailed administration of quotas, and to create your own additional quotas, you must use the File Server Resource Manager Console, accessible from the Administrative Tools program group. In addition to quotas, the console also enables you to create *file screens*, which specify the types of files that users are permitted to store on the server. For example, you can create file screens that prevent users from storing audio and video files on the server.**

Using File Server Resource Manager

Windows SBS 2011 incorporates simple quota controls into the Windows SBS Console application, but for more detailed administration of quotas, and to create your own additional quotas, you must use the File Server Resource Manager Console.

The File Server Resource Manager Console is part of the File Services role, which Windows SBS 2011 installs automatically. You can launch the console in any one of the following ways:

- Click the *Start* menu. Then click *Administrative Tools > File Server Resource Manager*.
- Launch the Server Manager Console and, in the Scope (left) pane, browse to the *Roles\File Services\Share and Storage Management\File Server Resource manager* node.
- Open the Run dialog box or a Command Prompt window, type **fsrm.msc** and press *Enter*.

The console appears as shown in Figure 9-7.

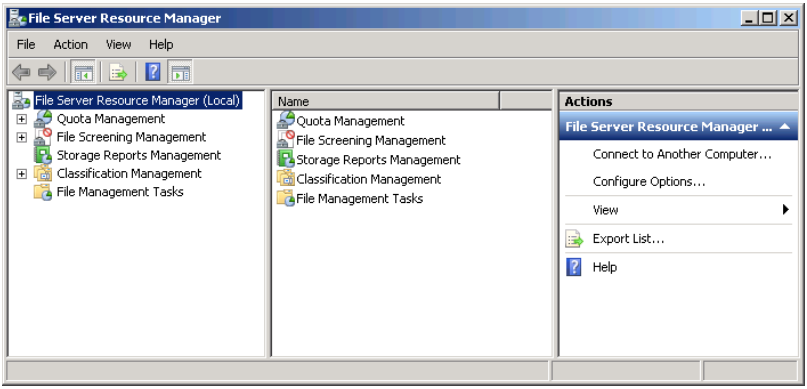

File Server Resource Manager
File
Action
View
Help
File Server Resource Manager (Local)
Quota Management
File Screening Management
Storage Reports Management
Classification Management
File Management Tasks
Name
Quota Management
File Screening Management
Storage Reports Management
Classification Management
File Management Tasks
Actions
File Server Resource Manager ...
Connect to Another Computer...
Configure Options...
View
Export List...
Help

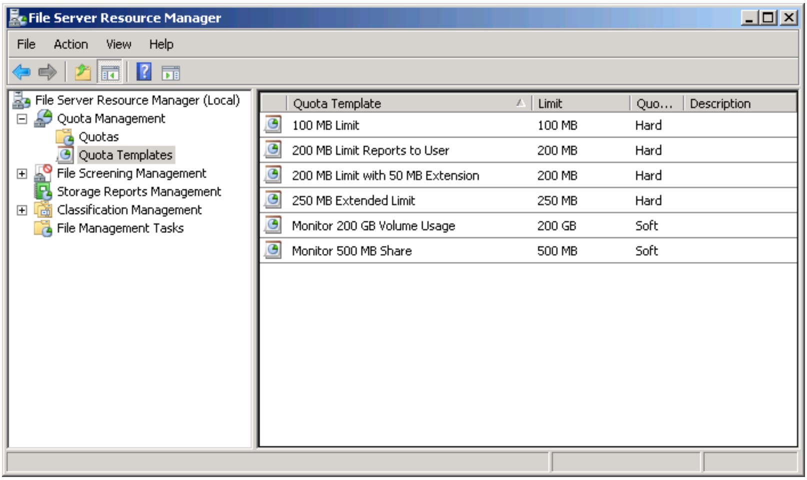
FIGURE 9-7 The File Server Resource Manager Console.

Creating a Quota Template

A *quota template* is a collection of settings that specify whether a quota should be hard or soft, what thresholds the system should apply to a quota, and what actions the system should take when a user reaches a threshold. Using quota templates simplifies the process of creating quotas for multiple users with the same settings.

Quota templates are permanently linked to the quotas created from them. When you use a template to create quotas, you can modify the template at a later time, and the system will apply the changes you made to the template to all the quotas you have created from that template.

The File Server Resource Manager Console includes a number of predefined templates, as shown in Figure 9-8, which you can use as is, or use to create your own templates.

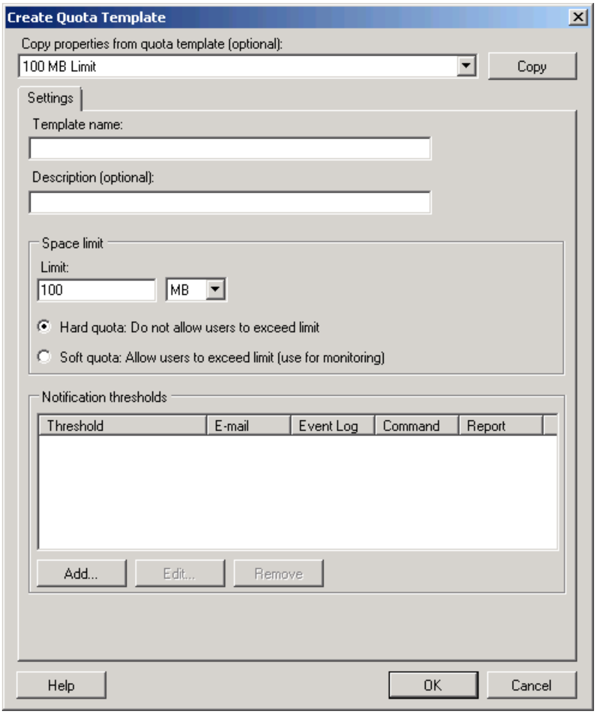

File Server Resource Manager
File
Action
View
Help
File Server Resource Manager (Local)
Quota Management
Quotas
Quota Templates
File Screening Management
Storage Reports Management
Classification Management
File Management Tasks

Quota Template	Limit	Quo...	Description
100 MB Limit	100 MB	Hard	
200 MB Limit Reports to User	200 MB	Hard	
200 MB Limit with 50 MB Extension	200 MB	Hard	
250 MB Extended Limit	250 MB	Hard	
Monitor 200 GB Volume Usage	200 GB	Soft	
Monitor 500 MB Share	500 MB	Soft	

FIGURE 9-8 The default quota templates in the File Server Resource Manager Console.

To create a new quota template, follow this procedure.

1. Log on to your Windows SBS 2011 server, using an account with network Administrator privileges. The Windows SBS Console appears.
2. Click *Start* and then click *Administrative Tools* > *File Server Resource Manager*. The File Server Resource Manager Console appears.
3. Expand the *Quota management* node. Then right-click the *Quota templates* node and, from the context menu, select *Create quota template*. The Create Quota Template dialog box appears.



Create Quota Template

Copy properties from quota template (optional): 100 MB Limit

Settings

Template name:

Description (optional):

Space limit

Limit: 100 MB

● Hard quota: Do not allow users to exceed limit

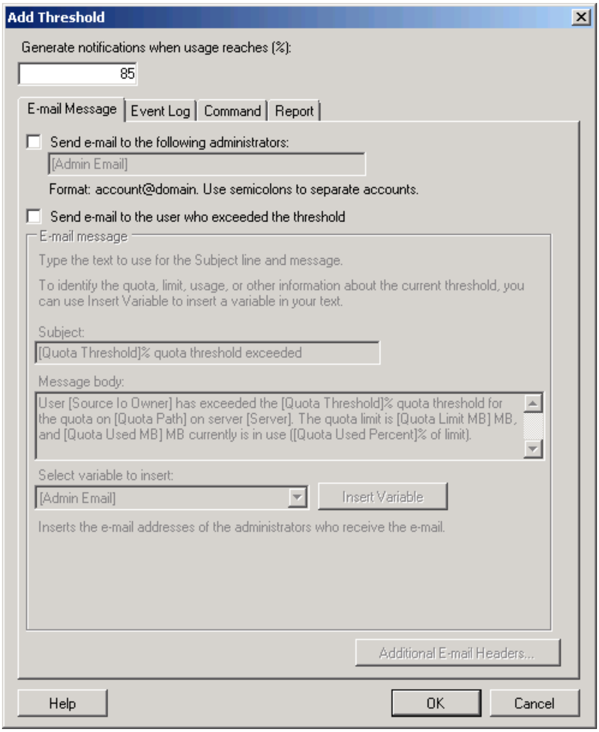
○ Soft quota: Allow users to exceed limit (use for monitoring)

Notification thresholds

Threshold	E-mail	Event Log	Command	Report

To create a new quota template from one of the existing templates, select a template in the *Copy properties from quota template* drop-down list and click *Copy*. The settings from the template appear in the dialog box, so that you can modify them as needed.

4. In the *Template name* text box, type the name you want to use to identify the template. Optionally, in the *Description* text box, type a descriptive string for the template.
5. In the *Space limit* box, specify the amount of storage space you want to allot to each individual user and whether you want to create a hard quota or a soft quota.
6. In the *Notification thresholds* box, click *Add*. The Add Threshold dialog box appears.



Add Threshold

Generate notifications when usage reaches (%): 85

□ Send e-mail to the following administrators: [Admin Email]

Format: account@domain. Use semicolons to separate accounts.

□ Send e-mail to the user who exceeded the threshold

E-mail message

Type the text to use for the Subject line and message.

To identify the quota, limit, usage, or other information about the current threshold, you can use Insert Variable to insert a variable in your text.

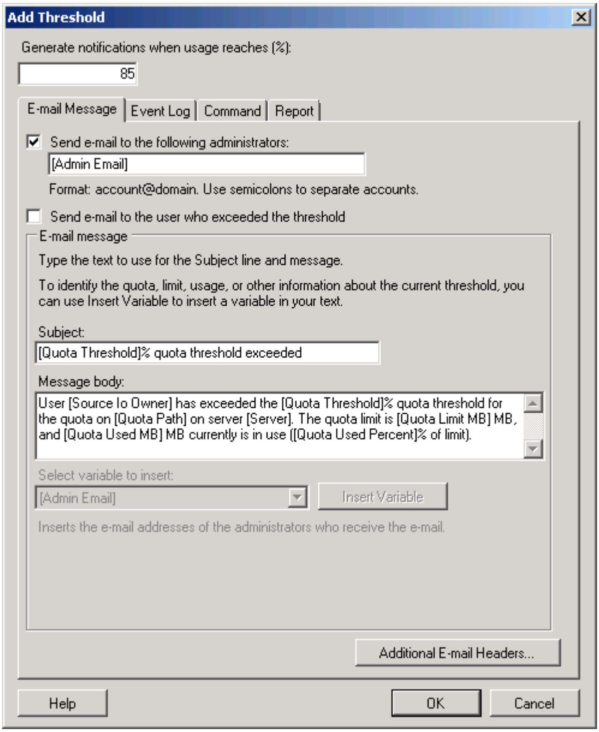
Subject: [Quota Threshold]% quota threshold exceeded

Message body: User [Source Io Owner] has exceeded the [Quota Threshold]% quota threshold for the quota on [Quota Path] on server [Server]. The quota limit is [Quota Limit MB] MB, and [Quota Used MB] MB currently is in use ([Quota Used Percent]% of limit).

Select variable to insert: [Admin Email]

Inserts the e-mail addresses of the administrators who receive the e-mail.

7. In the *Generate notifications when usage reaches (%)* text box, enter a threshold in the form of a percentage of the space limit you specified earlier.
8. Use the controls on the following tabs to specify the actions you want taken when a user reaches the specified threshold:
   - **Email message** Select the appropriate check box to specify whether you want the system to send an email message to an administrator, to the user, or both. For administrators, you can specify the email addresses of one or more persons separated by semicolons. For the user, you can modify the text of the default email message.



Generate notifications when usage reaches (%): 85

☑ Send e-mail to the following administrators: [Admin Email]

Format: account@domain. Use semicolons to separate accounts.

□ Send e-mail to the user who exceeded the threshold

E-mail message

Type the text to use for the Subject line and message.

To identify the quota, limit, usage, or other information about the current threshold, you can use Insert Variable to insert a variable in your text.

Subject: [Quota Threshold]% quota threshold exceeded

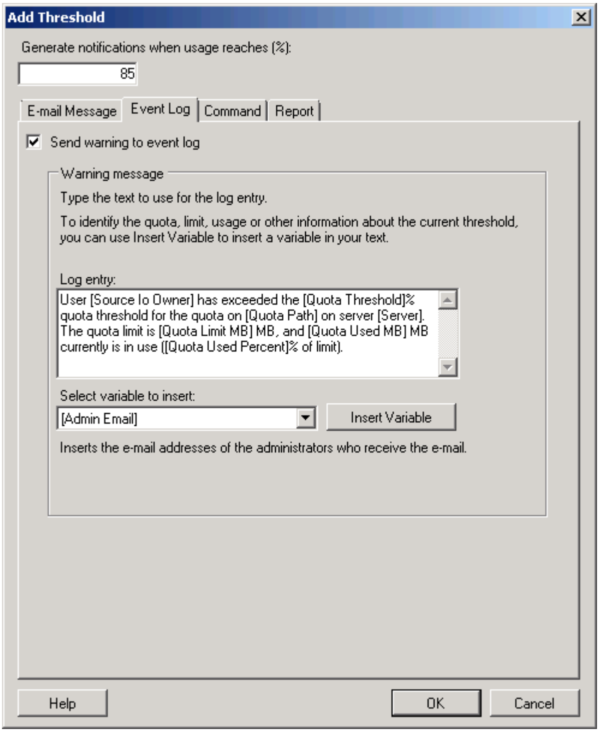
Message body: User [Source Io Owner] has exceeded the [Quota Threshold]% quota threshold for the quota on [Quota Path] on server [Server]. The quota limit is [Quota Limit MB] MB, and [Quota Used MB] MB currently is in use ([Quota Used Percent]% of limit).

Select variable to insert: [Admin Email]

Inserts the e-mail addresses of the administrators who receive the e-mail.

NOTE Windows SBS 2011 must be running the Simple Mail Transfer Protocol (SMTP) service to be able to send email messages. To install SMTP, you must use Server Manager to add the SMTP Server feature.

- **Event log** Select the Send warning to event log check box to create a log entry whenever a user reaches the threshold. You can modify the wording of the log entry in the text box provided.



Generate notifications when usage reaches (%): 85

☑ Send warning to event log

Warning message

Type the text to use for the log entry.

To identify the quota, limit, usage or other information about the current threshold, you can use Insert Variable to insert a variable in your text.

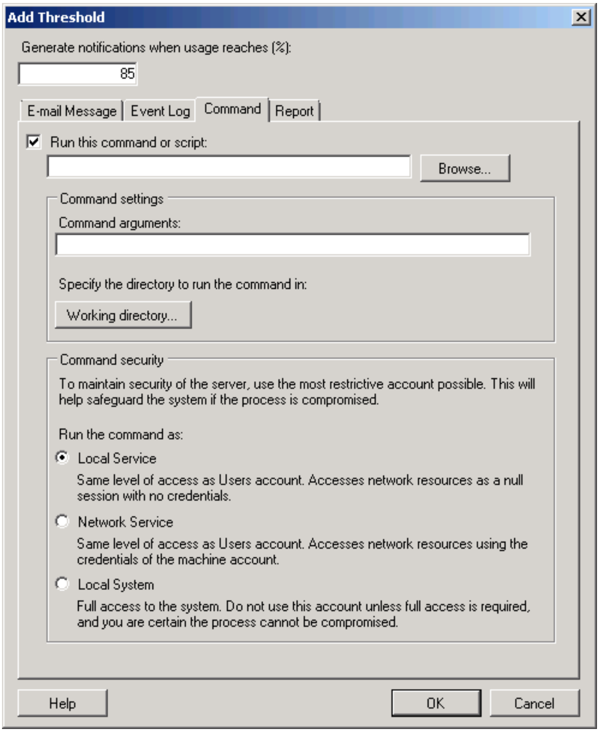
Log entry:

User [Source Io Owner] has exceeded the [Quota Threshold]% quota threshold for the quota on [Quota Path] on server [Server]. The quota limit is [Quota Limit MB] MB, and [Quota Used MB] MB currently is in use ([Quota Used Percent]% of limit).

Select variable to insert: [Admin Email]

Inserts the e-mail addresses of the administrators who receive the e-mail.

- **Command** Select the Run this command or script check box to specify a program or script file that the system should execute whenever a user reaches the threshold. You can also specify command arguments, a working directory, and the type of account the system should use to run the program or script.



Add Threshold

Generate notifications when usage reaches (%):

85

☑ Run this command or script:

Command settings

Command arguments:

Specify the directory to run the command in:

Command security

To maintain security of the server, use the most restrictive account possible. This will help safeguard the system if the process is compromised.

Run the command as:

● Local Service

Same level of access as Users account. Accesses network resources as a null session with no credentials.

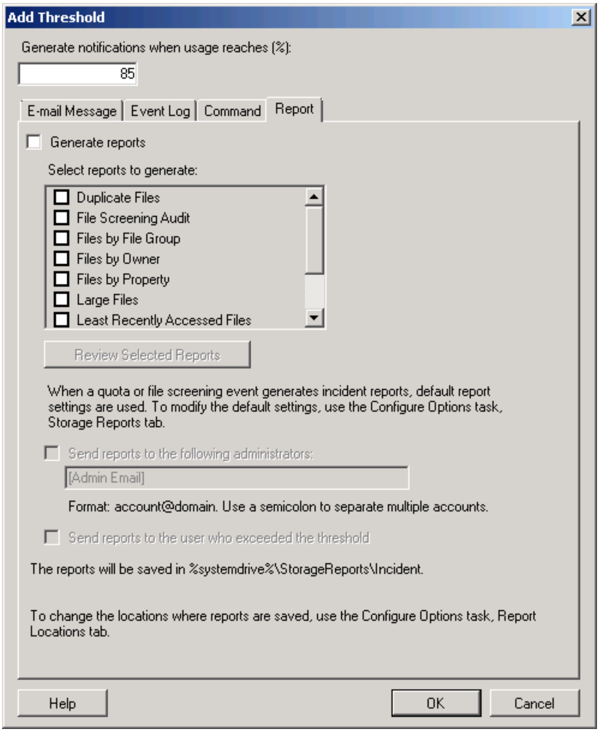
○ Network Service

Same level of access as Users account. Accesses network resources using the credentials of the machine account.

○ Local System

Full access to the system. Do not use this account unless full access is required, and you are certain the process cannot be compromised.

- **Report** Select the Generate reports check box, and then select the check boxes for the reports you want the system to generate. You can also specify that the system email the selected reports to an administrator or to the user that exceeded the threshold.



Add Threshold

Generate notifications when usage reaches (%):

85

□ Generate reports

Select reports to generate:

□ Duplicate Files
□ File Screening Audit
□ Files by File Group
□ Files by Owner
□ Files by Property
□ Large Files
□ Least Recently Accessed Files

When a quota or file screening event generates incident reports, default report settings are used. To modify the default settings, use the Configure Options task, Storage Reports tab.

□ Send reports to the following administrators:

[Admin Email]

Format: account@domain. Use a semicolon to separate multiple accounts.

□ Send reports to the user who exceeded the threshold

The reports will be saved in %systemdrive%\StorageReports\Incident.

To change the locations where reports are saved, use the Configure Options task, Report Locations tab.

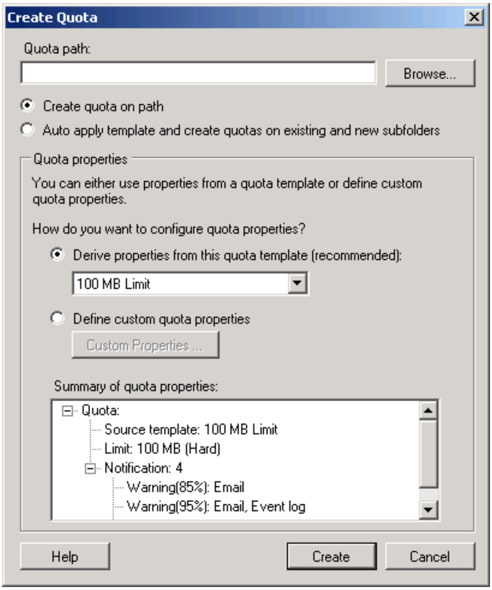
9. Click *OK* to close the Add Threshold dialog box and add the new threshold to the *Notification thresholds* list on the Create Quota Template dialog box.

10. Repeat steps 6 through 9 to create additional thresholds, if desired. When you have created all of the thresholds you need, click *OK* to create the quota template.

Creating a Quota

Once you have created a quota template or if you plan to use the predefined templates without modification, you can proceed to create quotas, using the following procedure.

1. Log on to your Windows SBS 2011 server, using an account with network Administrator privileges. The Windows SBS Console appears.
2. Click *Start*, and then click *Administrative Tools* > *File Server Resource Manager*. The File Server Resource Manager Console appears.
3. Expand the *Quota Management* node, right-click the *Quotas* folder and, from the context menu, select *Create quota*. The Create Quota dialog box appears.



Quota path:

● Create quota on path
○ Auto apply template and create quotas on existing and new subfolders

Quota properties

You can either use properties from a quota template or define custom quota properties.

How do you want to configure quota properties?

● Derive properties from this quota template (recommended):

100 MB Limit

○ Define custom quota properties

Summary of quota properties:

```
⊟ Quota:
    Source template: 100 MB Limit
    Limit: 100 MB (Hard)
  ⊟ Notification: 4
      Warning(85%): Email
      Warning(95%): Email, Event log
```

4. In the *Quota path* text box, type or browse to the name of the volume or folder for which you want to create a quota.
5. Select one of the following application options:
   - **Create quota on path** Creates a single quota for the specified volume or folder
   - **Auto apply template and create quotas on existing and new subfolders** Causes the system to automatically create a quota, based on a template, for each subfolder in the designated path, and for every new subfolder created in that path

6. Select one of the following quota properties options:
   - **Derive properties from this quota template** Configures the quota using the settings of the template you select from the drop-down list
   - **Define custom quota properties** Enables you to specify custom settings for the quota. Clicking the Custom properties button opens a Quota Properties dialog box for the selected volume or folder, which contains the exact same controls as the Create Quota Template dialog box discussed in the previous section.
7. Click *Create*. The new quota appears in the console's Details pane.

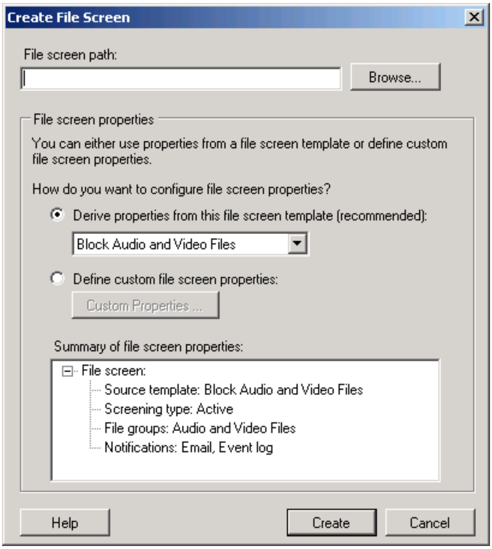
Creating a File Screen

In addition to creating quotas, the File Server Resource Manager Console can also create file screens. A *file screen* is a filter similar to a quota that prevents users from storing particular types of files on a server volume. The most common application for file screens is to prevent users from storing non-work-related—and possibly illegally obtained—files on servers, especially files that consume large amounts of storage space, such as audio and video files.

Windows SBS 2011 does not create any file screens by default, but you can create them yourself. The process of creating a file screen is similar to that of creating a quota: you specify the file types you want to filter and configure the actions you want the server to take when a user attempts to store a file of a forbidden type. As with quotas, you can create file screen templates and configure the server to generate email, log entries, and reports.

To create a file screen, follow these steps:

1. Log on to your Windows SBS 2011 server, using an account with network Administrator privileges. The Windows SBS Console appears.
2. Click *Start* and then click *Administrative Tools > File Server Resource Manager*. The File Server Resource Manager Console appears.
3. Expand the *File screening management node*, right-click the *File screens* folder and, from the context menu, select *Create file screen*. The Create File Screen dialog box appears.



File screen path:

File screen properties

You can either use properties from a file screen template or define custom file screen properties.

How do you want to configure file screen properties?

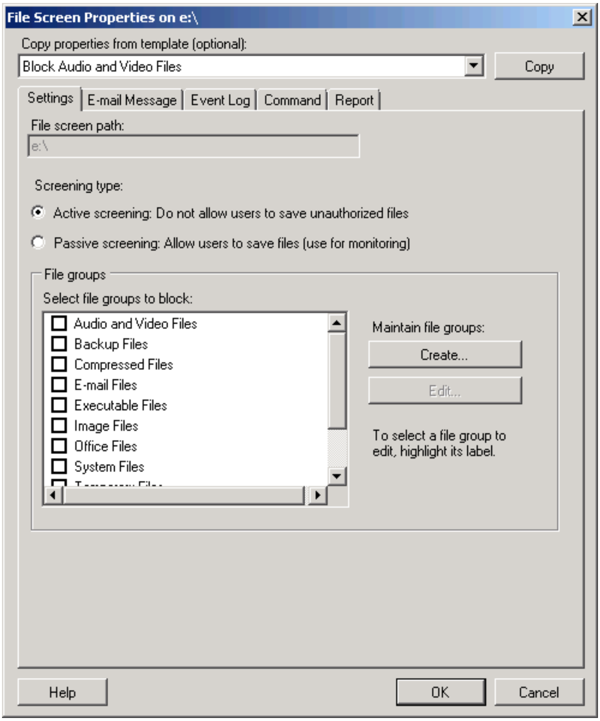
● Derive properties from this file screen template (recommended): Block Audio and Video Files

○ Define custom file screen properties:

Summary of file screen properties:

- File screen:
  - Source template: Block Audio and Video Files
  - Screening type: Active
  - File groups: Audio and Video Files
  - Notifications: Email, Event log

4. In the *File screen path* text box, type or browse to the name of the volume or folder on which you want to screen files.
5. Select one of the following properties options:
   - **Derive properties from the file screen template** Configures the file screen using the settings of the template you select from the drop-down list.
   - **Define custom file screen properties** Enables you to specify custom settings for the file screen. Clicking the Custom properties button opens a File Screen Properties dialog box for the selected volume or folder, which contains the Settings tab shown here, plus the same Email message, Event log, Command, and Report tabs as in the Quota Properties dialog box.



File Screen Properties on e:\

Copy properties from template (optional): Block Audio and Video Files

File screen path: e:\

Screening type:

● Active screening: Do not allow users to save unauthorized files

○ Passive screening: Allow users to save files (use for monitoring)

File groups

Select file groups to block:

- □ Audio and Video Files
- □ Backup Files
- □ Compressed Files
- □ E-mail Files
- □ Executable Files
- □ Image Files
- □ Office Files
- □ System Files

6. Click *Create*. The new file screen appears in the console's Details pane.

In addition to file screens, you can also create *file screen exceptions*, which override the influence of file screens. This way, if you choose to screen out all audio and video files for an entire volume, you can still create an exception for one folder where users are permitted to store legitimate video files.

Generating Storage Reports

Keeping track of usage is an important element of storage management, and File Server Resource Manager is capable of generating a variety of reports to aid administrators in this process.

The reports that the console can create are as follows:

- **Duplicate files** Creates a list of files that are the same size and have the same last modified date.
- **File screening audit** Creates a list of the audit events generated by file screening violations for specific users and during a specific time period.
- **Files by file group** Creates a list of files sorted by selected file groups in the File Server Resource Manager Console.
- **Files by owner** Creates a list of files sorted by selected users who own them.
- **Large files** Creates a list of files conforming to a specified file spec that are a specified size or larger.
- **Least recently accessed files** Creates a list of files conforming to a specified file spec that have not been accessed for a specified number of days.
- **Most recently accessed files** Creates a list of files conforming to a specified file spec that have been accessed within a specified number of days.
- **Quota usage** Creates a list of quotas that are exceeding a specified percentage of the storage limit.

Using the File Server Resource Manager, you can generate reports as needed, on the fly, or configure the console to create them according to a schedule you specify.

CHAPTER 10

Sharing Printers

Printer sharing is one of the original applications for which local area networks (LANs) were invented. The ability to send jobs to printers over the network eliminates the need to purchase multiple, redundant printers and prevents users from having to bother the person who has the printer attached to his or her computer. Windows Small Business Server (SBS) 2011 includes all the printer-sharing capabilities of Windows Server 2008 R2, as well as incorporating basic printer management capabilities into the Windows SBS Console.

This chapter explains how you can adapt the printing capabilities of Windows to your network environment. Once you understand the basic structure of the Windows printing architecture, you can easily provide your users with controlled access to the printers on your network and manage access to those printers as needed.

Understanding Windows Printing

In addition to the hardware that actually does the printing, Windows computers have a number of other components devoted to their print architecture. The main components of a shared printer solution in the Windows environment are as follows:

- **Print device** In Windows, the term *print device* refers to the actual hardware that produces the hard copy output from a print job. Windows enables you to share a print device that is connected to any computer on the network using a universal serial bus (USB), IEEE 1394 (FireWire), or other port; or connected directly to the network.

- **Printer** Although the term is commonly used to refer to the hardware, the term *printer*, in Windows, actually refers to the logical representation of a print device that appears in the operating system and on the network. You can create a printer in Windows without there being an actual print device connected to the computer or the network, and it will appear in the Devices And Printers Control panel just as if the hardware were present. A Windows printer tells the system which port, or interface, it must use to connect to the print device, as well as the printer driver the system must use to process its print jobs and communicate with the print device.
- **Print server** A *print server* is the component responsible for holding print jobs in a queue and sending them, one at a time, to the print device. A print server can be a dedicated hardware component that connects the print device to the network, but more often, one (or more) of the computers on the network functions as the print server. In Windows printing, you can create a single print server that receives jobs from all the clients on the network and feeds them to the print device, or each client can function as its own print server, sending jobs directly to the print device.
- **Printer driver** The *printer driver* is the software component that receives output from applications generating print jobs and converts it into a data stream using a *page description language (PDL)*, which consists of commands that the print device understands. Windows printer drivers generate print jobs using an interim format called *Enhanced Metafile (EMF)*. The EMF data is then converted into a device-specific RAW format, either by the client or the print server, depending on the printer configuration. The print server then stores the RAW data in the print queue until the print device is ready to accept it.

NOTE **Although many sources, including Microsoft documents, use the term *printer* to refer to the printing hardware, this chapter uses the term *print device* to refer to the hardware, while *printer* refers to the Windows logical component.**

Administrators can distribute these components around the network in various ways, to accommodate the printing strategy they want to create. Every computer that generates print jobs must have a printer and a printer driver, but you can locate print servers and print devices anywhere on the network.

Windows Printing Process

The process by which a computer prints a document includes the following steps and is shown in Figure 10-1:

1. A user working with an application activates its print function, selects one of the printers installed on the computer, and configures application-related settings, such as what pages of the document to print.

2. The application calls the printer driver associated with the selected printer, enabling the user to configure printer-related settings, such as which paper tray to use.
3. The printer driver converts the application's print output into XML Paper Specification (XPS) or EMF commands and data, which it sends to the print server.
4. The print server stores the job in a print queue called a *spooler*, in which it waits until the print device is ready to accept the job.
5. When the print device is ready, the print server reads the job from the spooler, converts it from EMF to a Printer Control Language (PCL) format, if necessary, and sends it to the print device using the appropriate port.
6. The print device receives the job from the print server, processes the commands and data, and generates the hard copy output.

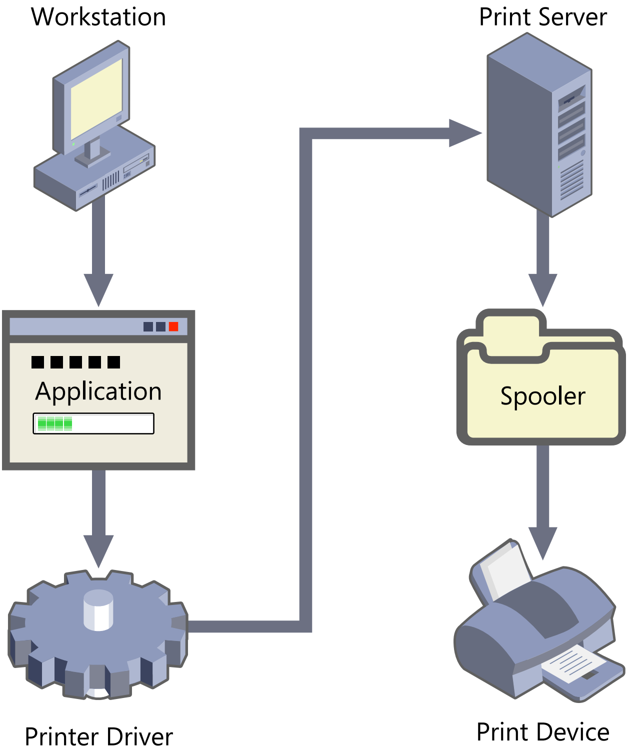


FIGURE 10-1 The Windows printing process.

Designing a Network Printing Solution

The printing architecture on a small business network is usually not complicated. Small businesses typically have, at most, two or three print devices, but administrators still have to make design decisions such as the following:

- How will the print devices connect to the network?
- Which computer(s) should function as print servers?
- Who has access to the print devices and when?
- Who is responsible for daily printer maintenance?

Connecting Print Devices

Before you can share a print device with your Windows SBS 2011 network, you must connect the hardware to one of the computers on the network or connect it directly to the network. Most of the print devices on the market today connect to a computer using a USB or IEEE 1394 port, and many also have an integrated network interface adapter, which enables you to connect the device directly to your Ethernet or wireless network. Older print devices might connect to a computer using a parallel or serial port, and, in some cases, you can purchase a network interface adapter as an expansion card that plugs into the printer. Finally, you can purchase an external print server device that connects directly to the network and has a port for connecting the print device.

The type of print device connection you use should depend on your network design, the layout of your office, and, as always, your budget. When you connect a print device to a computer, as shown in Figure 10-2, that computer functions as a print server, receiving jobs from other computers on the network and feeding them to the print device. Any Windows computer, whether server or workstation, can function as a print server. However, if your users do a lot of printing, the print server functions can impose a significant burden on a workstation that does not have much more than the minimum recommended Windows hardware to support them. A constantly running printer can also be an annoyance to a user trying to accomplish other tasks on the workstation.

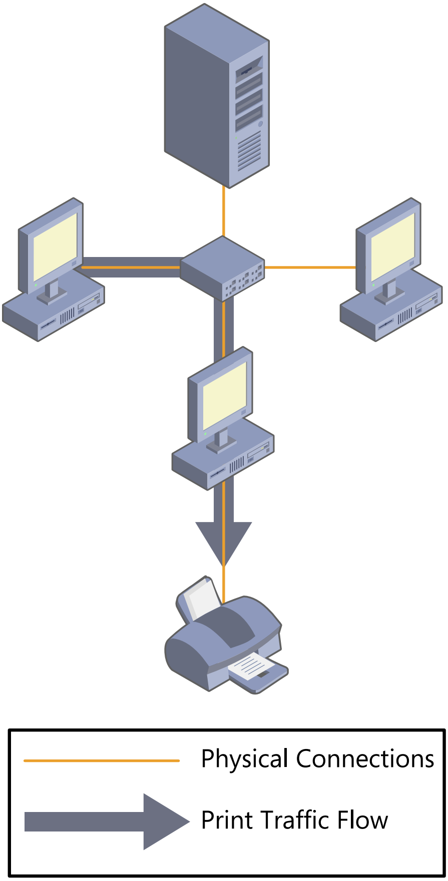


FIGURE 10-2 A print device connected to a computer.

If at all possible, connecting the print devices to server computers is preferable to workstation connections unless the servers are in a location that would be inconvenient for users having to retrieve their printed documents. For example, if you plan to locate your servers in a locked data center or server closet, it would not be practical to locate your print devices there as well.

The best solution, by far, is to connect your print devices directly to the network. This solution enables you to locate your print devices anywhere a network connection is available. You can also designate any computer on the network as a print server, which enables you to use your server computers for their intended purpose, no matter where they are located, as shown in Figure 10-3.

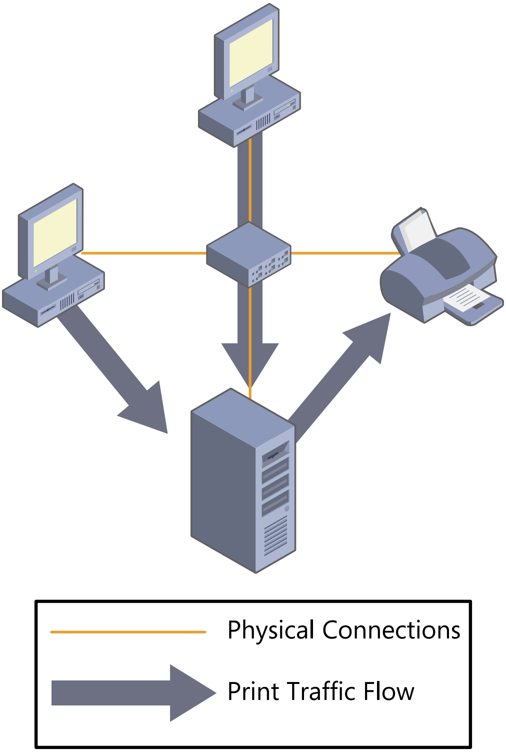


FIGURE 10-3 A print device connected to the network with a single print server.

It is also possible for each computer to function as its own print server, sending jobs directly to the print device, as shown in Figure 10-4. The only drawback to network–attached print devices is that units with network adapters tend to be more expensive than those without them.

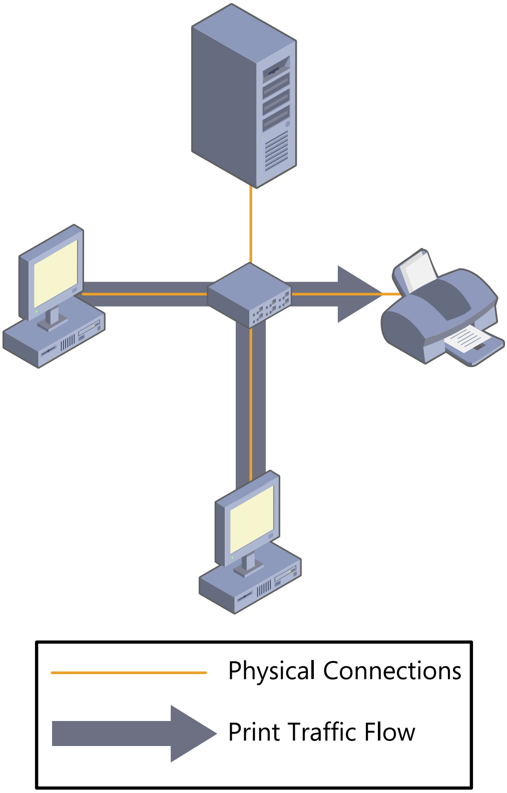


FIGURE 10-4 A print device connected to the network, with each computer acting as its own print server.

Selecting a Print Server

The first deciding factor in selecting a computer to function as a print server is the type of print device connections you plan to use. As mentioned earlier, if you connect a print device directly to a computer, that computer must function as the print server. Network-attached printers provide greater flexibility.

In addition to the type of connections you plan to use, however, you should also base your selection of a print server on the following factors:

- **Print volume** The more printing your users do, the greater the burden on the print server. Large numbers of documents use more print server resources than small numbers, lengthy documents use more resources than brief ones, and graphical documents use more than plain text.

- **Print rendering** When a print server is running Windows Server 2008 R2 or Windows 7, you can specify whether the client or the print server should render the print jobs. Client-side rendering (CSR) reduces the burden on the print server.
- **Computer resources** Print volume and CSR both affect the resources used by print server functions. For example, a workstation with the minimum recommended system requirements can function adequately as a print server, but its functionality as a workstation might be compromised.

Controlling Access to Print Devices

In many cases, administrators grant users unrestricted access to the print devices on the network. However, you might want to regulate access to color print devices, or other units with expensive consumables such as letterhead paper. Windows printers have their own permission system, which functions similar to NTFS and share permissions. You can specify which users can send jobs to a printer and also control access based on other factors, such as the time of day and the user's priority.

> ***REAL WORLD*** **Print devices are some of the few network hardware components that require maintenance on almost a daily basis. Part of your printing solution should include a decision as to who is responsible for the print devices' regular maintenance, including tasks such as loading media, clearing paper jams, and replacing toner or ink cartridges. These are thankless tasks that many people try to avoid, so it is important to delegate them decisively. Otherwise, you might find a huge backlog of print jobs left in the queue because the print device is out of paper or toner, and no one has bothered to replenish them.**

Deploying Network Printers

The process of deploying a printer on your Windows SBS 2011 network consists of the following basic steps:

- Connect the print device to the computer or network.
- Create a printer on the print server and install drivers.
- Share the printer.
- Configure clients to access the printer.

These steps are discussed in the following sections.

Connecting a Print Device

For most of the print devices on the market today, the process of connecting the device consists of simply plugging a cable into a USB or IEEE 1394 port on the computer you intend to use as a print server, or plugging a cable into any network connection. Keep in mind, however, that many print devices do not include the required USB or network cable in the box, so you might have to purchase one separately.

Older print devices might use a parallel or serial port connection to connect to a computer. Parallel connections use a large, heavy cable that is limited to a maximum length of 6 to 9 feet. Serial cables are thinner and lighter, and can be longer, but print devices with serial connectors are relatively rare.

To connect a print device that does not have a built-in network adapter directly to the network, you can purchase a device that provides a network connection. Some print device models have an expansion slot that can accept a proprietary network adapter/print server made by the print device manufacturer, but external print server devices are also available that are not proprietary, which enable you to connect any print device to your network. Print server devices supporting either wired or wireless networks are available, providing you with virtually unlimited freedom in placing your computers.

NOTE **The network interface adapters that print devices use are different from those you install in computers. The expansion slots in print devices are not standardized like those in computers, so the adapters that fit into them use proprietary designs that are uniquely designed for specific print devices.**

Creating a Printer

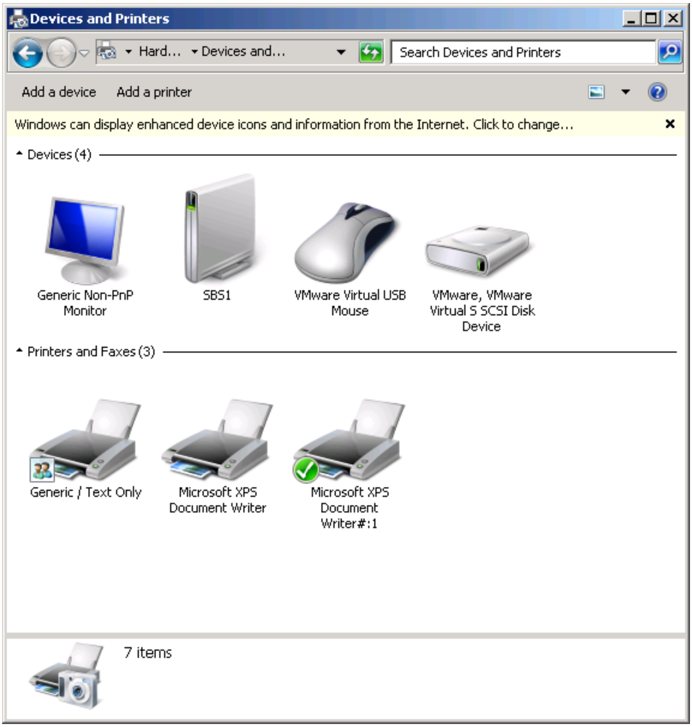
USB and IEEE 1394 are both Plug and Play interfaces, so when you connect a print device to a Windows computer using one of those ports and turn on the print device, the system typically detects it and automatically starts a Plug and Play hardware detection and installation sequence. During the installation process, Windows creates a printer, configures the port that provides access to the print device, installs printer drivers, and typically offers to share the printer with the network as well.

All the current Windows operating systems include a large collection of printer drivers, but if your print device is a newly released model, or a particularly obscure one, the system might prompt you to supply drivers. Print devices typically include a driver disk, and manufacturers usually have the latest drivers available on a website. Your print device might also include additional software, such as a print device management application. In most cases, Windows can access the print device without any special software other than drivers, so installing these other products is usually optional.

Installing a Local Printer Manually

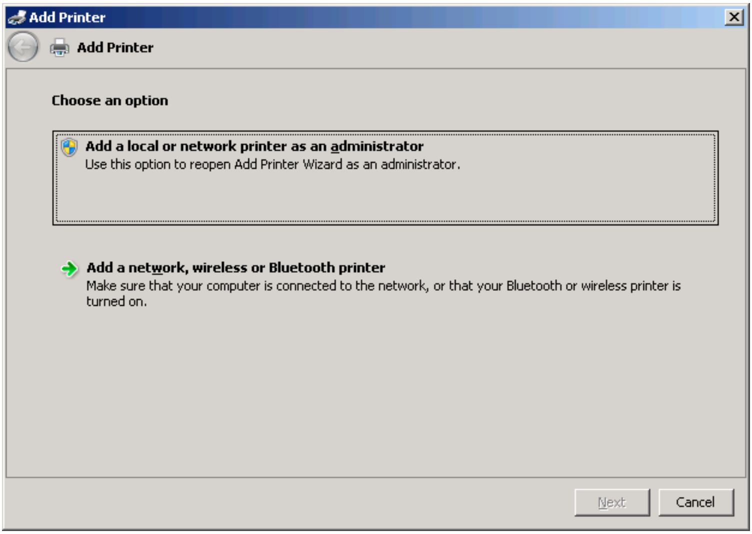
If you have a print device that does not use a Plug and Play interface, such as one that connects to the computer's parallel or serial port, you have to run the Add Printer Wizard. The following procedure illustrates the process of installing a printer connected to a server running Windows SBS 2011 using a parallel or serial port:

1. Click *Start*, and then click *Devices and printers*. The Devices And Printers Control panel appears.



Windows can display enhanced device icons and information from the Internet. Click to change…

2. Click *Add printer*. The Add Printer Wizard appears, displaying the Choose An Option page.

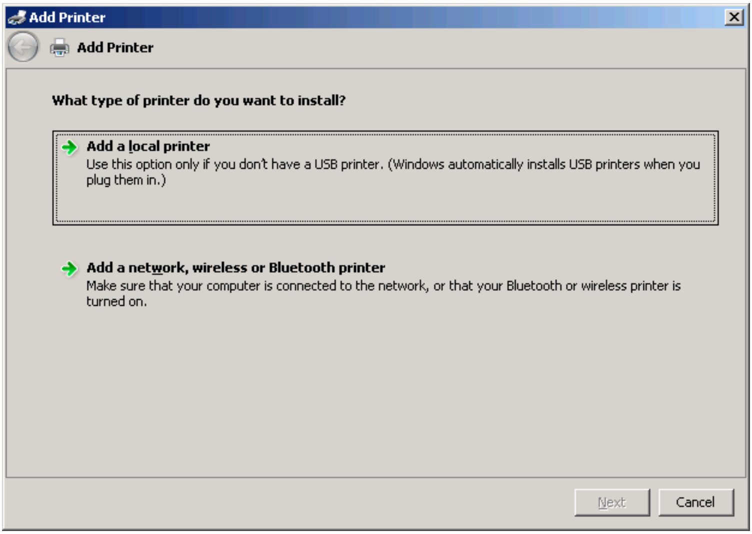


Choose an option

Add a local or network printer as an administrator
Use this option to reopen Add Printer Wizard as an administrator.

Add a network, wireless or Bluetooth printer
Make sure that your computer is connected to the network, or that your Bluetooth or wireless printer is turned on.

3. Click *Add a local or network printer as an administrator*. The What Type Of Printer Do You Want To Install? page appears.

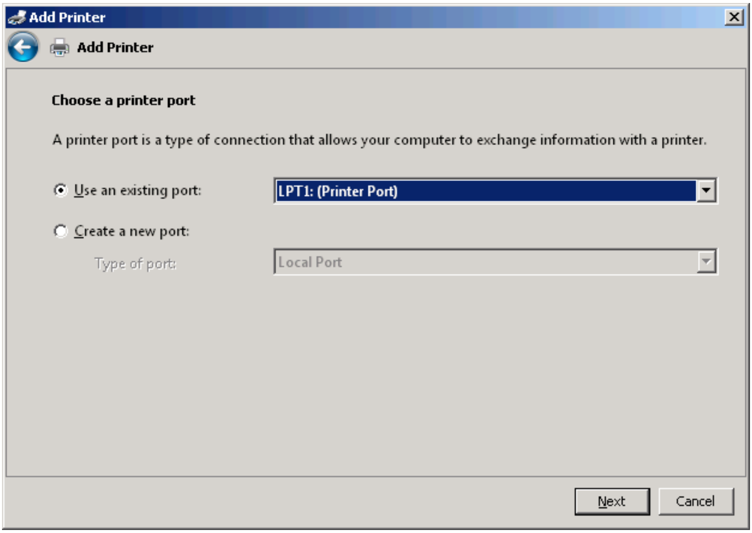


What type of printer do you want to install?

→ **Add a local printer**
Use this option only if you don't have a USB printer. (Windows automatically installs USB printers when you plug them in.)

→ **Add a network, wireless or Bluetooth printer**
Make sure that your computer is connected to the network, or that your Bluetooth or wireless printer is turned on.

4. Click *Add a local printer*. The Choose A Printer Port page appears.



Choose a printer port

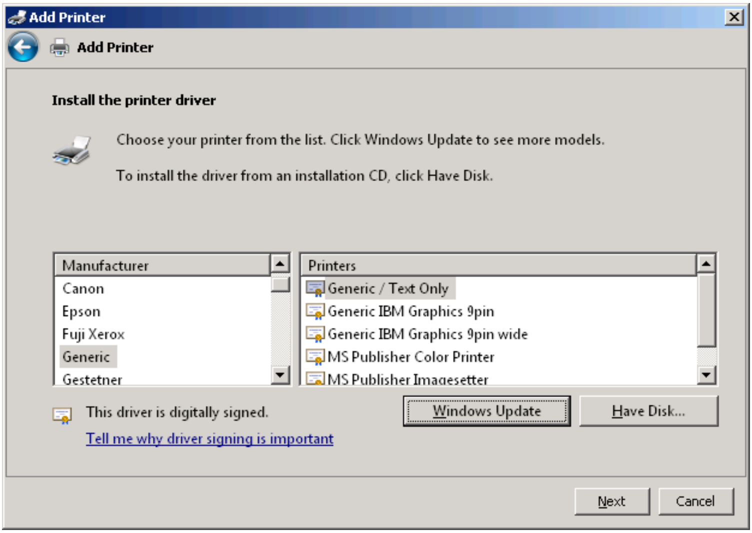
A printer port is a type of connection that allows your computer to exchange information with a printer.

● Use an existing port: LPT1: (Printer Port)

○ Create a new port:

Type of port: Local Port

5. Leave the *Use an existing port* option selected and choose the correct port from the drop-down list. Then click *Next*. The Install The Printer Driver page appears.



Install the printer driver

Choose your printer from the list. Click Windows Update to see more models.

To install the driver from an installation CD, click Have Disk.

Manufacturer	Printers
Canon	Generic / Text Only
Epson	Generic IBM Graphics 9pin
Fuji Xerox	Generic IBM Graphics 9pin wide
Generic	MS Publisher Color Printer
Gestetner	MS Publisher Imagesetter

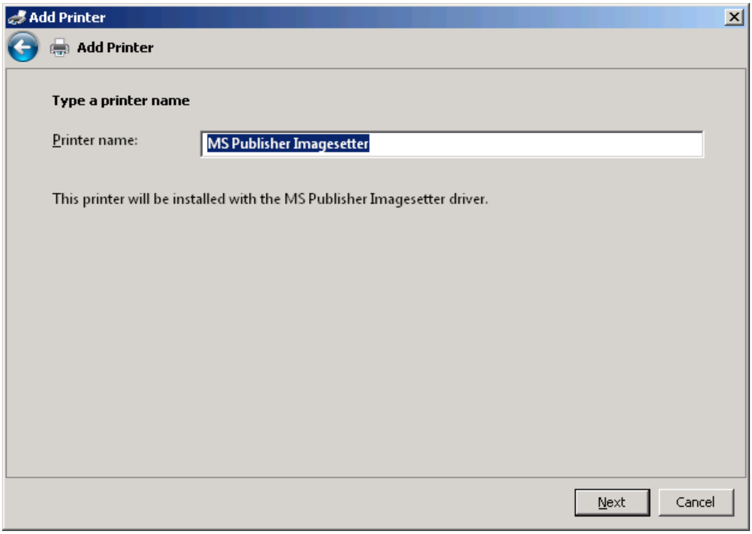
This driver is digitally signed.

Tell me why driver signing is important

6. From the list on the left, select the manufacturer of the print device.

NOTE **If your printer does not appear in the list, you must obtain a printer driver from the manufacturer and click *Have disk* to install it.**

7. From the list of the manufacturers' printers on the right, select your print device and click *Next*. The Type A Printer Name page appears.

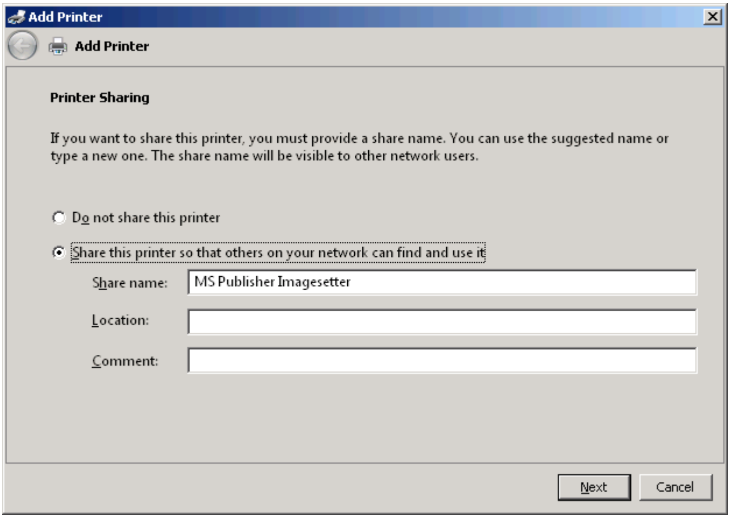


Type a printer name

Printer name: MS Publisher Imagesetter

This printer will be installed with the MS Publisher Imagesetter driver.

8. Specify the name that the system will use to identify the print device and click *Next*. The wizard installs the printer and the Printer Sharing page appears.



Printer Sharing

If you want to share this printer, you must provide a share name. You can use the suggested name or type a new one. The share name will be visible to other network users.

○ Do not share this printer

● Share this printer so that others on your network can find and use it

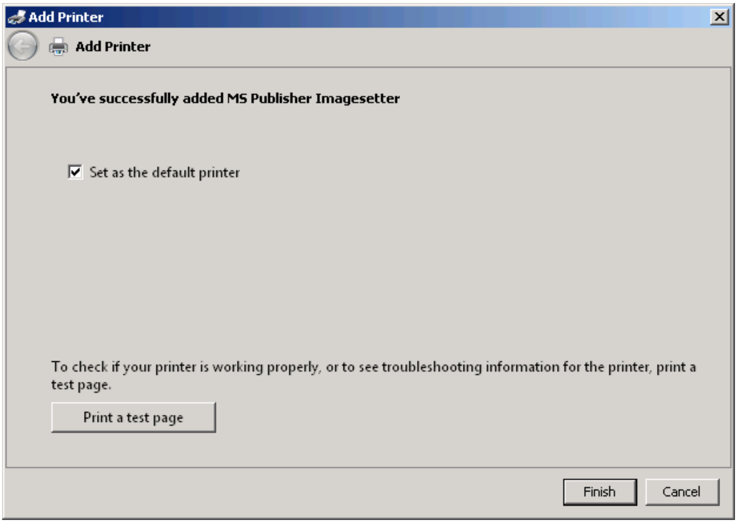
Share name: MS Publisher Imagesetter

Location:

Comment:

9. Leave the *Share this printer so that others on your network can find and use it* option selected and, in the *Share name* text box, specify the name by which the printer will be known on the network. Optionally, you can also specify additional information about the printer in the *Location* and *comment* text boxes.

10. Click *Next*. The You've Successfully Added the printer page appears.

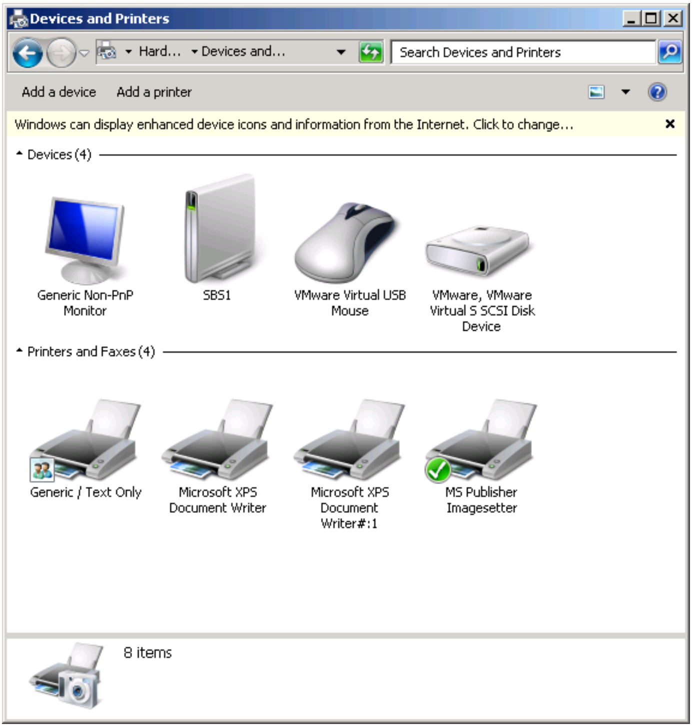


You've successfully added MS Publisher Imagesetter

☑ Set as the default printer

To check if your printer is working properly, or to see troubleshooting information for the printer, print a test page.

11. Click *Finish*. The wizard closes and the printer appears in the Devices And Printers Control panel.



Devices and Printers
Hard... ▸ Devices and...
Search Devices and Printers
Add a device
Add a printer
Windows can display enhanced device icons and information from the Internet. Click to change...
Devices (4)
Generic Non-PnP Monitor
SBS1
VMware Virtual USB Mouse
VMware, VMware Virtual S SCSI Disk Device
Printers and Faxes (4)
Generic / Text Only
Microsoft XPS Document Writer
Microsoft XPS Document Writer#:1
MS Publisher Imagesetter
8 items

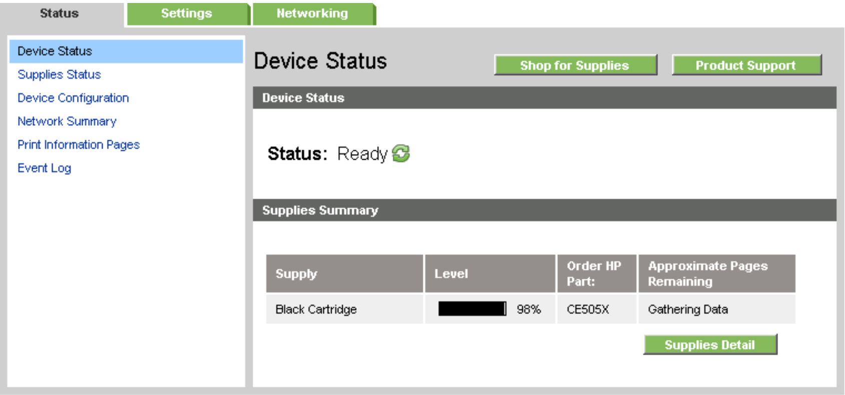
CAUTION **If you open the Windows SBS Console immediately after installing a printer using this procedure, the printer does not appear in the *Printers* list on the Network/Devices page. This is because although the Add Printer Wizard has shared the printer, it has not added it to your Active Directory Domain Services (AD DS) domain. To complete the installation, you must perform one of the procedures discussed in "Sharing a Printer," later in this chapter.**

Installing a Network-Attached Printer

The process of installing a print device that connects directly to the network and creating a printer for it is largely determined by the hardware manufacturer. In most cases, you simply connect the print device to the network and run an installation program on the computer that you want to function as the print server. The program detects the print device on the network, creates a Transmission Control Protocol/Internet Protocol (TCP/IP) port that points to the print device's IP address, creates a printer using that port, and installs the appropriate drivers. The program might also provide you with the opportunity to share the printer and install additional proprietary tools.

A print device that connects directly to a network has a network interface adapter, just like a computer, and like a computer, it must have an IP address. Most of the network print devices manufactured today include a Dynamic Host Configuration Protocol (DHCP) client, which enables them to obtain an IP address from the DHCP server on your network. Others might have a preconfigured IP address, which you can learn from reading the product documentation or by printing out a test page.

As with most other types of network peripherals, many network print devices have an integrated web server, which provides a configuration interface, like the one shown in Figure 10-5. This interface typically enables you to specify whether you want the print device to obtain its IP address using DHCP or use a specific address that you configure manually.



Device Status

Device Status

Status: Ready

Supplies Summary

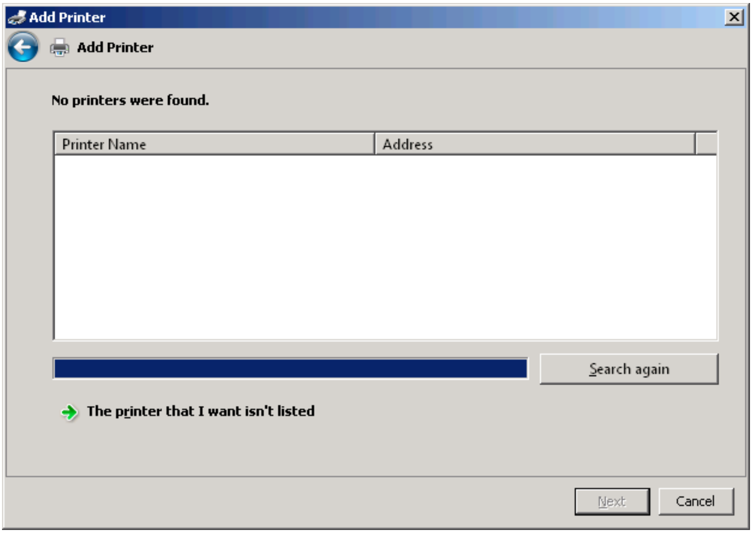
Supply	Level	Order HP Part:	Approximate Pages Remaining
Black Cartridge	98%	CE505X	Gathering Data

FIGURE 10-5 The configuration interface for a network-attached printer.

Installing a Network Printer Manually

For a network-attached print device that does not have an installation program, or for a print device connected to a stand-alone print server that does not have an installation program, you can install a printer with a TCP/IP port manually using the following procedure:

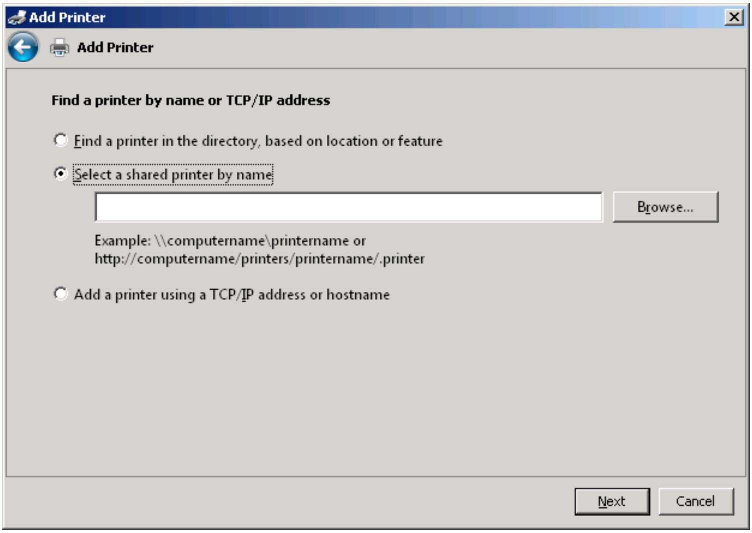
1. Click *Start*, and then click *Control Panel*. The Control Panel window appears.
2. Click *Hardware*. Then click *Devices and printers*. The Devices And Printers Control panel appears.
3. Click *Add a Printer*. The Add Printer Wizard appears, displaying the Choose An Option page.
4, Click *Add a local or network printer as an administrator*. The What Type Of Printer Do You Want To Install? page appears.
5. Click *Add a network, wireless, or Bluetooth printer*. The No Printers Were Found page appears.



No printers were found.

Printer Name	Address

6. Click *The printer that I want isn't listed*. The Find A Printer By Name Or TCP/IP Address page appears.



Find a printer by name or TCP/IP address

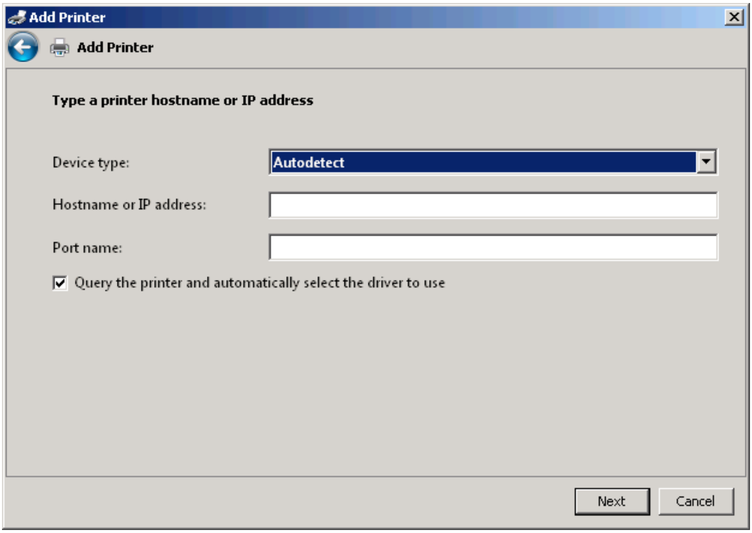
○ Find a printer in the directory, based on location or feature

● Select a shared printer by name

Example: \\computername\printername or
http://computername/printers/printername/.printer

○ Add a printer using a TCP/IP address or hostname

7. Select the *Add a printer using a TCP/IP address or hostname* option and click *Next*. The Type A Printer Hostname Or IP Address page appears.


Add Printer

Add Printer

Type a printer hostname or IP address

Device type: Autodetect

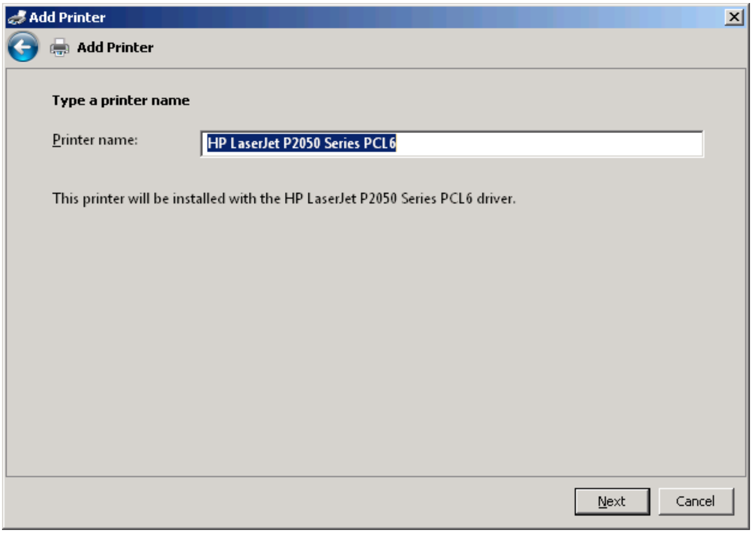
Hostname or IP address:

Port name:

☑ Query the printer and automatically select the driver to use

8. In the *Device type* drop-down list, select *TCP/IP device*.
9. In the *Hostname or IP address* text box, type the name or IP address of the print device or the stand-alone print server to which the print device is connected; then click *Next*.

   If the wizard can communicate with the print device, the print device identifies itself, and the Type A Printer Name page appears, specifying a default name for the print device and the driver that the wizard will install.


Add Printer

Add Printer

Type a printer name

Printer name: HP LaserJet P2050 Series PCL6

This printer will be installed with the HP LaserJet P2050 Series PCL6 driver.

If the wizard cannot communicate with the print device, the Install The Printer Driver page appears, as shown earlier in this chapter, in which you must select the manufacturer and model of the print device.

10. Change the default *Printer* name, if desired, and click *Next*. The wizard installs the printer and the Printer Sharing page appears.
11. Leave the *Share this printer so that others on your network can find and use it* option selected and, in the *Share name* text box, specify the name by which the printer will be known on the network. Optionally, you can also specify additional information about the printer in the *Location* and *comment* text boxes.
12. Click *Next*. The You've Successfully Added The Printer page appears.
13. Click *Finish*. The wizard closes, and the printer appears in the Devices And Printers Control panel.

Creating a DHCP Reservation for a Printer

DHCP client support is a common feature in network printer devices; it greatly simplifies the print device installation process. However, the *D* in *DHCP* stands for "Dynamic," meaning that it is possible for a client's IP address assignment to change. If, for example, a network print device is disconnected or offline long enough for its DHCP lease to expire, the DHCP server might assign it a different address when you reconnect it to the network. The print device can communicate with the network, but the print clients might still have ports that reference the old IP address.

MORE INFO **For more information on IP address assignment and DHCP, see Chapter 2, "A Networking Primer."**

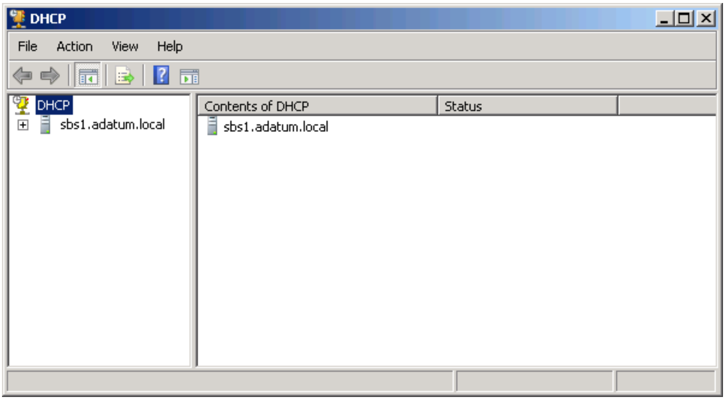
One of the best ways to ensure continued connectivity for a DHCP-equipped network print device is to create ports using the print device's name instead of its IP address. This way, even if the address changes, the name remains the same.

Another way is to create a reservation for the print device on the DHCP server. A *DHCP reservation* is an IP address that you permanently assign to a specific client, based on the Media Access Control (MAC) address encoded into its network interface adapter hardware. The print device still obtains its IP address from the DHCP server, but the server always assigns it the same address as long as the print device is connected to the same IP subnet.

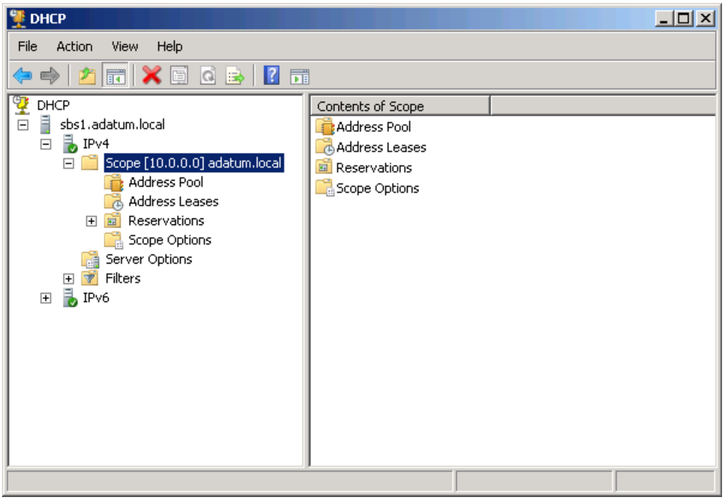
BEST PRACTICES **Although it might be possible to configure your print device manually to use a static IP address, creating a DHCP reservation is a better solution, so that all your IP address assignments are documented and managed in one place. If you manually assign an IP address in your DHCP scope to a device on your network, the DHCP server might attempt to assign that same address to another device later. DHCP servers check the network for IP address duplication before they complete each address assignment, but there is no way to know how the print device will react to an address conflict.**

To create a DHCP reservation for your network print device, use the following procedure:

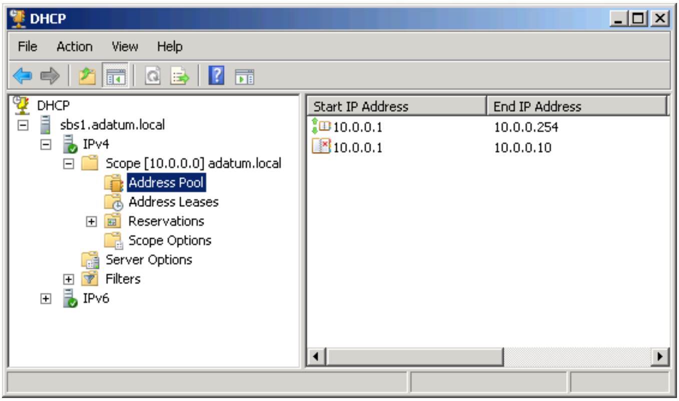
1. Connect your print device to the network and configure it to obtain its IP address using DHCP.
2. Log on to your Windows SBS 2011 server, using an account with network Administrator privileges.
3. Click *Start*, and then click *Administrative Tools* > *DHCP*. The DHCP Console appears.



4. Expand the node representing your server and browse to the scope that the Connect To The Internet Wizard created on your server.

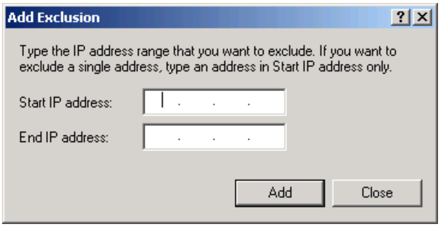


5. Expand the scope and click the *Address pool* node.



Start IP Address	End IP Address
10.0.0.1	10.0.0.254
10.0.0.1	10.0.0.10

6. Note the range of addresses available for distribution. Then right-click the *Address pool* node and, from the context menu, select *New exclusion range*. The Add Exclusion dialog box appears.

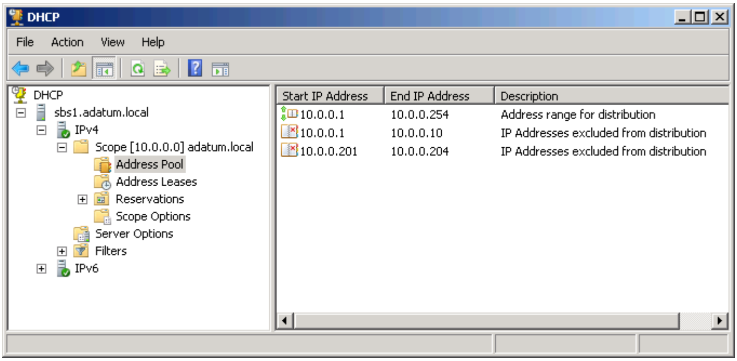


Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only.

Start IP address: . . .

End IP address: . . .

7. In the *Start IP address* and *End IP address* text boxes, specify a range of addresses at the end of your scope that is large enough to support all your network print devices. Click *Add*, and then click *Close*. The new exclusion range appears in the *Address pool* list.



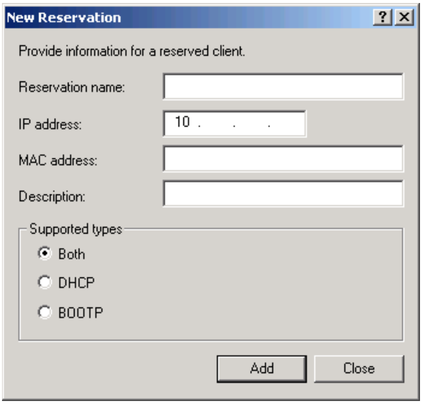
Start IP Address	End IP Address	Description
10.0.0.1	10.0.0.254	Address range for distribution
10.0.0.1	10.0.0.10	IP Addresses excluded from distribution
10.0.0.201	10.0.0.204	IP Addresses excluded from distribution

8. Click the *Address leases* node.

9. Locate the lease for your print device in the list and adjust the column widths in the console so that you can see the entire Unique ID value for the lease.

   NOTE **Your print device most likely has a host name that you do not recognize, one that is different from the names you have assigned to your network computers.**

10. Click the *Reservations* node, which displays an empty list, and then click the *Address leases* node again.
11. Right-click the *Reservations* node and, from the context menu, select *New reservation*. The New Reservation dialog box appears.



New Reservation

Provide information for a reserved client.

Reservation name:

IP address: 10 . . .

MAC address:

Description:

Supported types

● Both

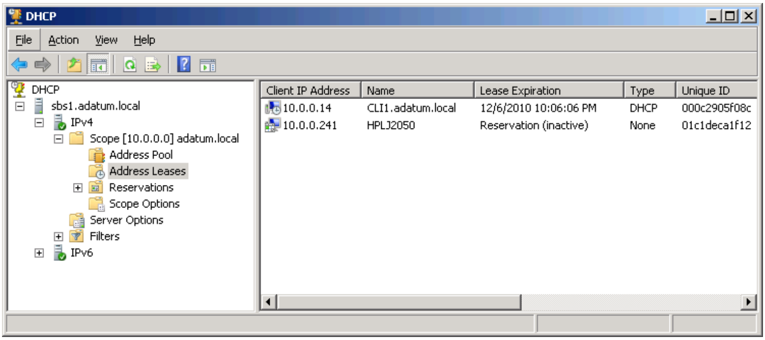
○ DHCP

○ BOOTP

12. In the *Reservation name* text box, type the name of your network print device.
13. In the *IP address* text box, type one of the IP addresses in the exclusion range you just created.
14. In the *MAC address* text box, type the *Unique ID* value for your print device's current address lease.

   NOTE **The Unique ID value is the hardware address assigned to the print device's network interface adapter by the manufacturer.**

15. Click *Add*, and then click *Close*. The reservation appears in the *Address leases* list, with a *Lease expiration* value of *Reservation (inactive)*.



Client IP Address	Name	Lease Expiration	Type	Unique ID
10.0.0.14	CLI1.adatum.local	12/6/2010 10:06:06 PM	DHCP	000c2905f08c
10.0.0.241	HPLJ2050	Reservation (inactive)	None	01c1deca1f12

16. Turn the print device off or unplug it from its power source. Wait 30 seconds; then turn the print device back on or plug it back in. Wait another 30 seconds for the print device to initialize.

17. In the DHCP Console, on the *Action* menu, click *Refresh*. The print device's original address lease disappears from the *Address leases* list, and the reservation you created now has a *Lease expiration* value of *Reservation (active)*.

18. Close the DHCP Console.

From now on, each time the DHCP server receives an IP address request from the print device containing the MAC address you specified, the server assigns the address in the reservation you created.

Sharing a Printer

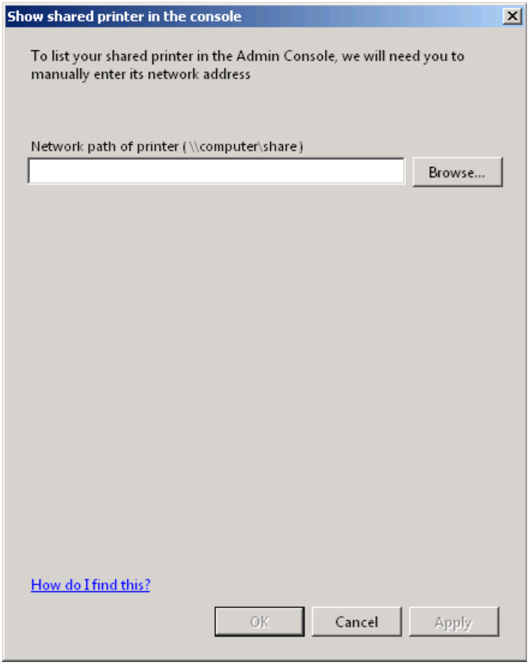
Once you have installed a printer on one of your network computers, you must share it to make it accessible to all the other computers on the network, if you have not done so during the installation. When you share a printer, Windows also enables you to add printer drivers for other Windows platforms. This way, when a client computer on the network installs the printer, it can download the correct driver from the print server automatically.

Installing a printer on one of your network computers is only one piece of the printing solution; you must share the printer to make it accessible to the other computers on the network. In many cases, you can share the printer as you create it using the Add Printer Wizard, or you can set up sharing after the installation is complete.

Be aware, however, that the Add Print Wizard's Sharing page lacks one critical facility: It does not list the shared printer in AD DS. When you share a printer without adding it to AD DS, computers on the network can send jobs to the printer, but they cannot search the directory for it, and, more importantly, administrators cannot manage the printer using the controls on the Network/Devices page of the Windows SBS Console.

The console populates the Devices list by searching the AD DS database for printer objects, so if you have a shared printer on your network that does not appear in the console, you can add it to the directory in one of two ways:

- By clicking *List a shared printer in this console* in the *Tasks* list on the Network/Devices page and specifying the path to the printer share, using the interface shown here.

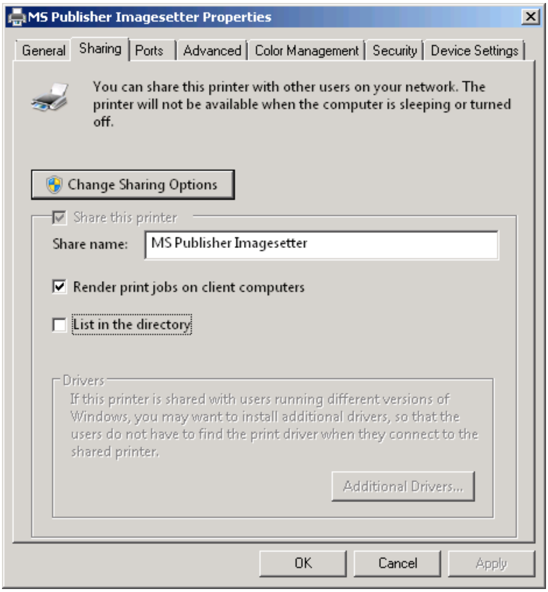


Show shared printer in the console

To list your shared printer in the Admin Console, we will need you to manually enter its network address

Network path of printer (\\computer\share)

- By opening the *Sharing* tab in the printer's Properties sheet, and selecting the *List in the directory* check box.



You can share this printer with other users on your network. The printer will not be available when the computer is sleeping or turned off.

☑ Share this printer

Share name: MS Publisher Imagesetter

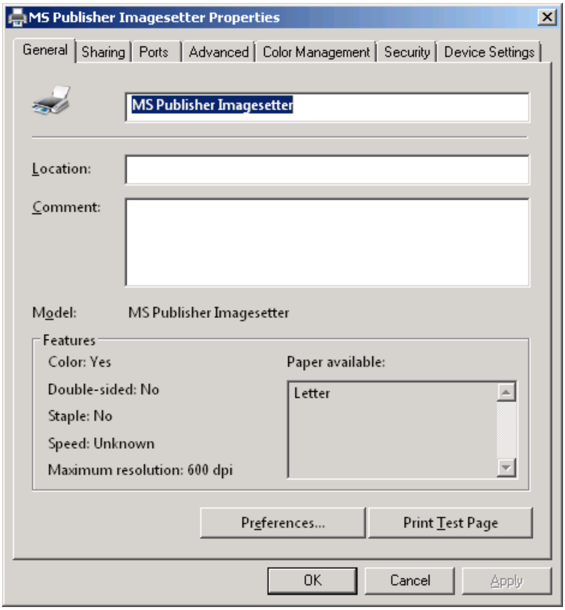
☑ Render print jobs on client computers

□ List in the directory

If this printer is shared with users running different versions of Windows, you may want to install additional drivers, so that the users do not have to find the print driver when they connect to the shared printer.

Alternately, you can install the printer first, and then set up sharing. This procedure adds your printer to the AD DS database automatically. To share an existing printer on your server running Windows SBS 2011, use the following procedure:

1. Log on to your Windows SBS 2011 server, using an account with network Administrator privileges.
2. Click *Start*, and then click *Control panel*. The Control Panel window appears.
3. Click *Hardware*. Then click *Devices and printers*. The Devices And Printers Control panel appears.
4. Right-click the printer you want to share and, from the context menu, select *Printer properties*. The Properties sheet for the printer appears.



MS Publisher Imagesetter Properties

MS Publisher Imagesetter

Location:

Comment:

Model: MS Publisher Imagesetter

Features

Color: Yes

Double-sided: No

Staple: No

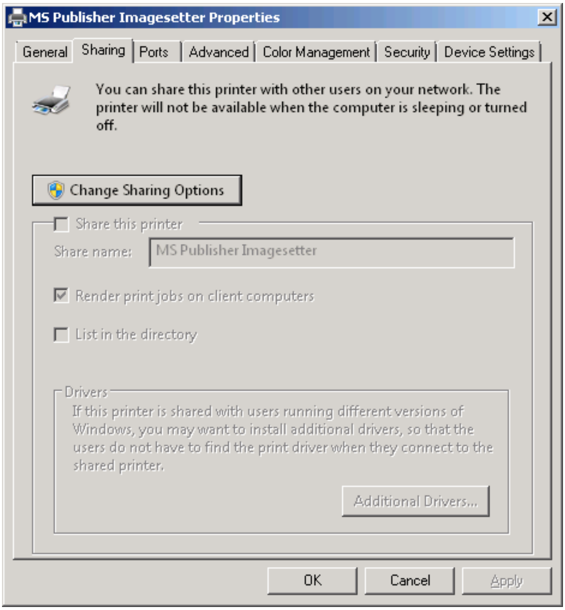
Speed: Unknown

Maximum resolution: 600 dpi

Paper available:

Letter

5. Click the *Sharing* tab.



MS Publisher Imagesetter Properties

You can share this printer with other users on your network. The printer will not be available when the computer is sleeping or turned off.

☐ Share this printer

Share name: MS Publisher Imagesetter

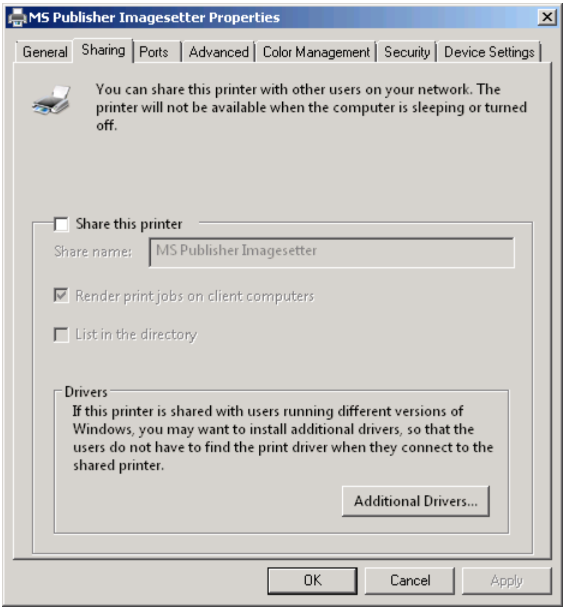
☑ Render print jobs on client computers

☐ List in the directory

Drivers

If this printer is shared with users running different versions of Windows, you may want to install additional drivers, so that the users do not have to find the print driver when they connect to the shared printer.

6. Click *Change sharing options*. The sharing controls are activated.



You can share this printer with other users on your network. The printer will not be available when the computer is sleeping or turned off.

□ Share this printer

Share name: MS Publisher Imagesetter

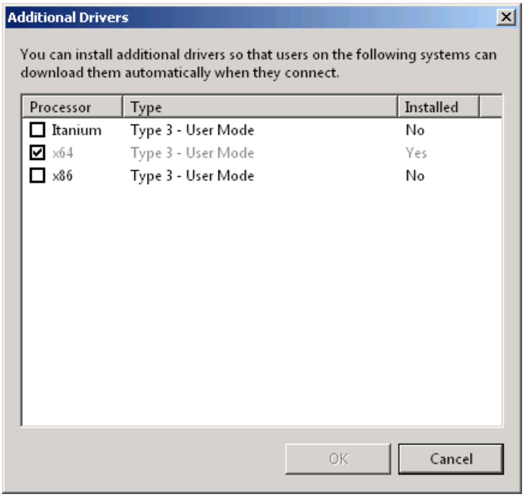
☑ Render print jobs on client computers

□ List in the directory

Drivers

If this printer is shared with users running different versions of Windows, you may want to install additional drivers, so that the users do not have to find the print driver when they connect to the shared printer.

7. Select the *Share this printer* check box.
8. In the *Share name* text box, type the name by which the printer will be known on the network.
9. Select the *Render print jobs on client computers* check box, if you want to minimize the processing load on the print server.
10. Select the *List in the directory* check box.
11. Click *Additional drivers*. The Additional Drivers dialog box appears.

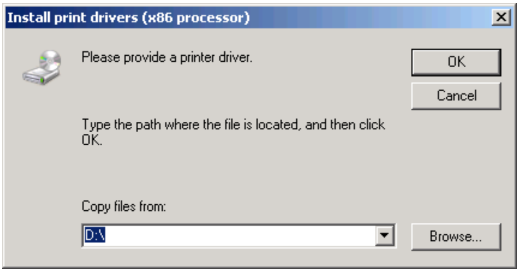


Additional Drivers

You can install additional drivers so that users on the following systems can download them automatically when they connect.

Processor	Type	Installed
□ Itanium	Type 3 - User Mode	No
☑ x64	Type 3 - User Mode	Yes
□ x86	Type 3 - User Mode	No

12. Select the check boxes for the platforms you want to install and click *OK*. A Printer Drivers dialog box appears for each platform you selected.



Install print drivers (x86 processor)

Please provide a printer driver.

Type the path where the file is located, and then click OK.

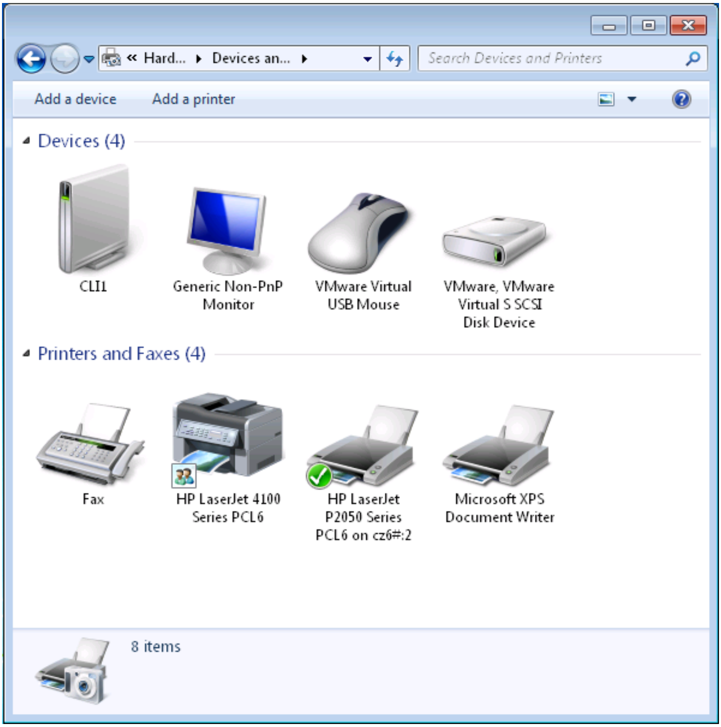
Copy files from: D:\

13. Type or browse to the location of the printer driver for each platform and click *OK*.
14. Click *OK* to close the Additional Drivers dialog box.
15. Click *OK* to close the printer's Properties sheet.

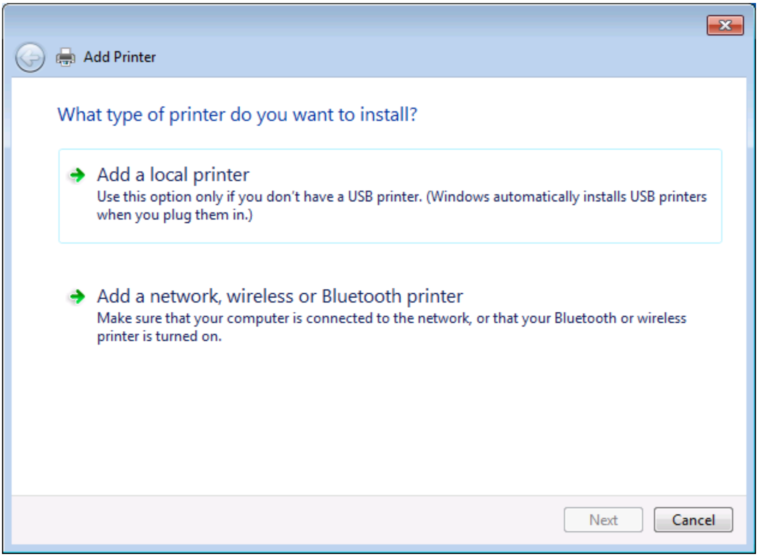
Deploying Printers on Clients

After you install a print device, create a printer for it, and share the printer with the network, you can add the printer to client computers as needed. To install a network printer on a Windows 7 client, use the following procedure:

1. Click *Start*, and then click *Control panel*. The Control Panel window appears.
2. Click *Hardware*. Then click *Devices and printers*. The Devices And Printers Control panel appears.


« Hard... ▸ Devices an... ▸
Search Devices and Printers
Add a device
Add a printer
Devices (4)
CLI1
Generic Non-PnP Monitor
VMware Virtual USB Mouse
VMware, VMware Virtual S SCSI Disk Device
Printers and Faxes (4)
Fax
HP LaserJet 4100 Series PCL6
HP LaserJet P2050 Series PCL6 on cz6#:2
Microsoft XPS Document Writer
8 items

3. Click *Add a printer*. The Add Printer Wizard appears, displaying the What Type Of Printer Do You Want To Install? page.

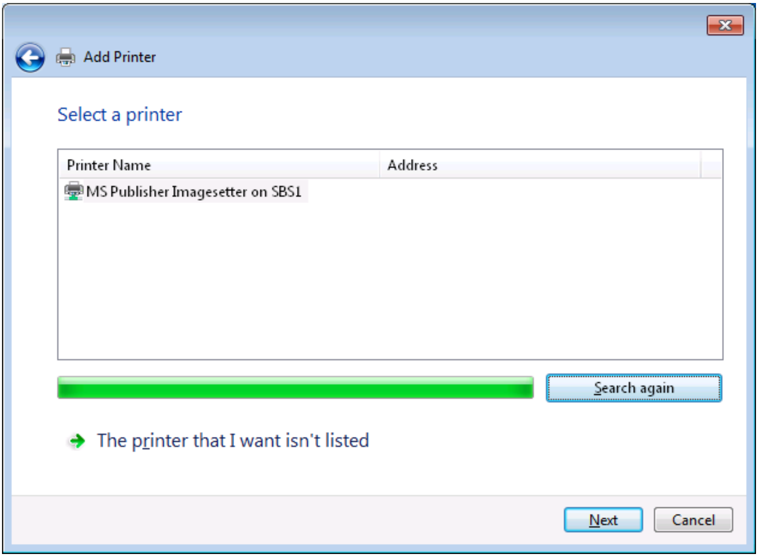

Add Printer

What type of printer do you want to install?

Add a local printer
Use this option only if you don't have a USB printer. (Windows automatically installs USB printers when you plug them in.)

Add a network, wireless or Bluetooth printer
Make sure that your computer is connected to the network, or that your Bluetooth or wireless printer is turned on.

4. Click *Add a network, wireless or Bluetooth printer*. The Searching For Available Printers page appears briefly and then the Select A Printer page appears.

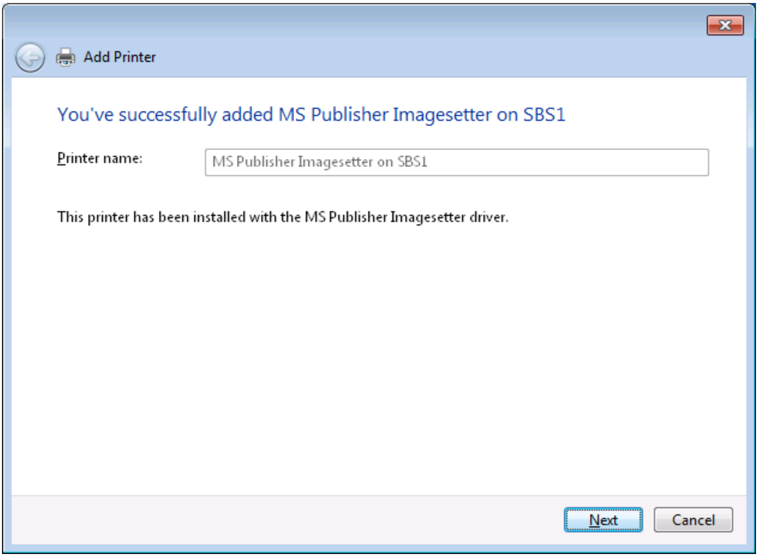

Add Printer

Select a printer

Printer Name	Address
MS Publisher Imagesetter on SBS1	

The printer that I want isn't listed

5. Select the printer you want to install and click *Next*. A Windows printer Installation progress indicator box appears as the system installs the printer. Then the You've Successfully Added The Printer page appears.



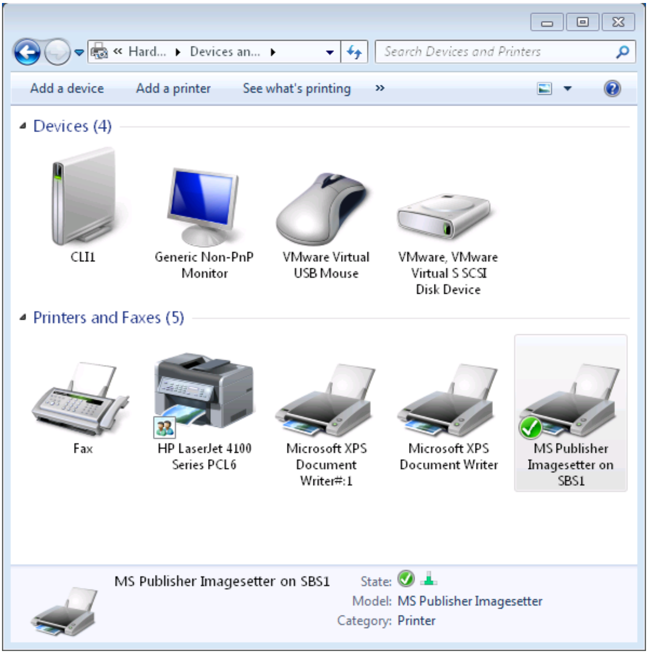
Add Printer

You've successfully added MS Publisher Imagesetter on SBS1

Printer name: MS Publisher Imagesetter on SBS1

This printer has been installed with the MS Publisher Imagesetter driver.

6. Click *Next*. Another You've Successfully Added The Printer page appears.
7. Click *Finish*. The wizard closes, and the printer appears in the Devices And Printers Control panel.



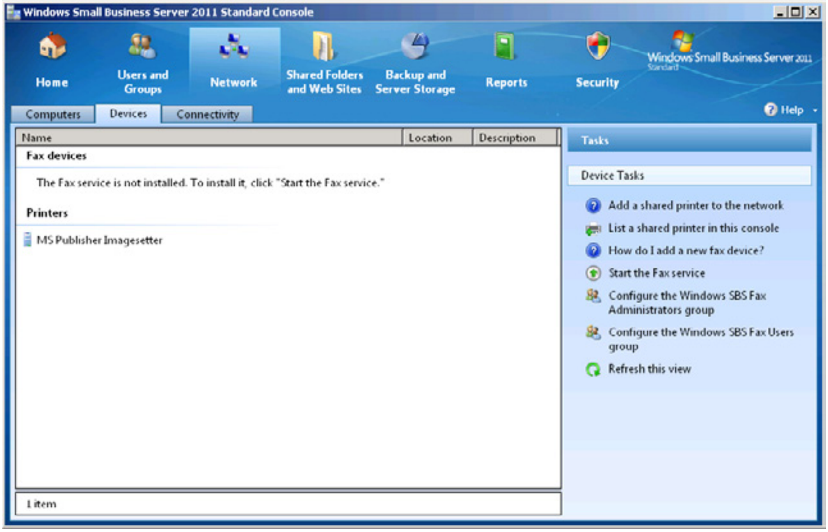
« Hard... ▸ Devices an... ▸
Search Devices and Printers
Add a device
Add a printer
See what's printing
»
Devices (4)
CLI1
Generic Non-PnP Monitor
VMware Virtual USB Mouse
VMware, VMware Virtual S SCSI Disk Device
Printers and Faxes (5)
Fax
HP LaserJet 4100 Series PCL6
Microsoft XPS Document Writer#:1
Microsoft XPS Document Writer
MS Publisher Imagesetter on SBS1

MS Publisher Imagesetter on SBS1 State: ✓
Model: MS Publisher Imagesetter
Category: Printer

MORE INFO In addition to installing printers on client computers manually, you can also deploy a printer to all the clients on the network using Group Policy settings. For more information, see Chapter 13, "Managing Windows SBS 2011."

Managing Printers Using the Windows SBS Console

Once you have deployed your print devices, created printers for them, shared them, and listed them in the AD DS directory, you can manage them all from the Windows SBS Console on your primary server, no matter which computers you are using as print servers. When you click the *Network* button in the console and select the *Devices* tab, you see a list of the shared printers on the network, as shown in Figure 10-6.


Windows Small Business Server 2011 Standard Console
Home
Users and Groups
Network
Shared Folders and Web Sites
Backup and Server Storage
Reports
Security
Windows Small Business Server 2011 Standard
Computers
Devices
Connectivity
Help
Name
Location
Description
Tasks
Device Tasks

Fax devices

The Fax service is not installed. To install it, click "Start the Fax service."

Printers

MS Publisher Imagesetter

1 item

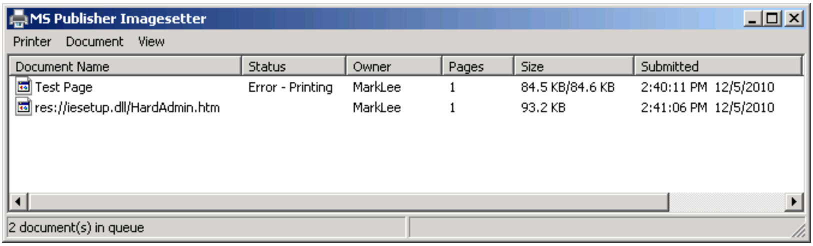
- Add a shared printer to the network
- List a shared printer in this console
- How do I add a new fax device?
- Start the Fax service
- Configure the Windows SBS Fax Administrators group
- Configure the Windows SBS Fax Users group
- Refresh this view

FIGURE 10-6 Installed and shared printers in the Windows SBS Console.

By selecting a printer and clicking one of the items in the printer-specific *Tasks* list, you can perform the management tasks described in the following sections.

Managing Queued Print Jobs

When you select a printer and click *Printer jobs* in the *Tasks* list, a window appears, named for the printer and containing a list of the jobs currently waiting in the print queue, as shown in Figure 10-7. With the appropriate permissions, you can pause, resume, and cancel individual print jobs, as well as pause and cancel the entire queue.


MS Publisher Imagesetter

Printer Document View

Document Name	Status	Owner	Pages	Size	Submitted
Test Page	Error - Printing	MarkLee	1	84.5 KB/84.6 KB	2:40:11 PM 12/5/2010
res://iesetup.dll/HardAdmin.htm		MarkLee	1	93.2 KB	2:41:06 PM 12/5/2010

2 document(s) in queue

FIGURE 10-7 The Print Queue window for a shared printer.

Controlling Printer Access

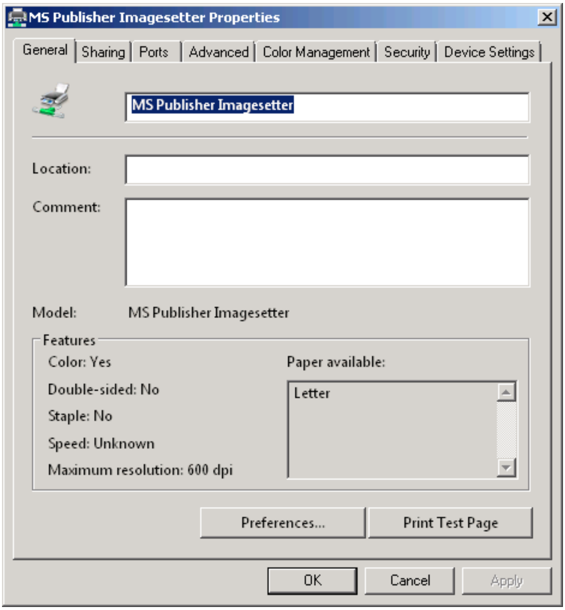
As mentioned earlier in this chapter, Windows printers have their own system of permissions, which you can use to specify who is allowed to access and manage your shared printers. By default, Windows grants the Allow Print permission to the Everyone special identity on all printers. This enables all users to send jobs to the printers. The other permission assignments, and the capabilities provided by the various print permissions, are listed in Table 10-1.

TABLE 10-1 Windows Printer Permission

PERMISSION	CAPABILITIES	DEFAULT ASSIGNMENTS
Print	■ Connect to a printer ■ Print documents ■ Pause, resume, restart, and cancel the user's own documents	■ Everyone ■ Administrators ■ Server Operators ■ Print Operators
Manage Printers	■ Cancel all documents ■ Share a printer ■ Change printer properties ■ Delete a printer ■ Change printer permissions	■ Administrators ■ Server Operators ■ Print Operators
Manage Documents	■ Pause, resume, restart, and cancel all users' documents ■ Control job settings for all documents	■ Creator Owner ■ Administrators ■ Server Operators ■ Print Operators

To limit printer access to specific users, you must revoke the permissions from the Everyone special identity and then grant the Allow Print permission to the users or groups that you want to give access to the printer. To modify the default print permissions, use the following procedure:

1. Log on to your Windows SBS 2011 server, using an account with network Administrator privileges. The Windows SBS Console appears.
2. Click *Network*, and then select the *Devices* tab.
3. Select the printer that you want to manage and, in the *Tasks* list, click *Printer properties*. The Properties sheet for the printer appears.



MS Publisher Imagesetter Properties

MS Publisher Imagesetter

Location:

Comment:

Model: MS Publisher Imagesetter

Features

Color: Yes

Double-sided: No

Staple: No

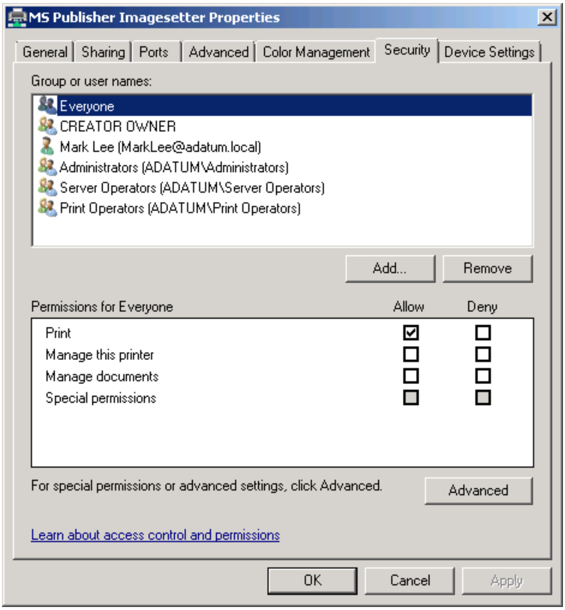
Speed: Unknown

Maximum resolution: 600 dpi

Paper available:

Letter

4. Click the *Security* tab.



Group or user names:

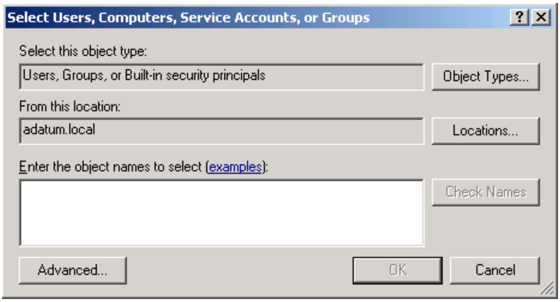
- Everyone
- CREATOR OWNER
- Mark Lee (MarkLee@adatum.local)
- Administrators (ADATUM\Administrators)
- Server Operators (ADATUM\Server Operators)
- Print Operators (ADATUM\Print Operators)

Permissions for Everyone	Allow	Deny
Print	☑	□
Manage this printer	□	□
Manage documents	□	□
Special permissions	□	□

For special permissions or advanced settings, click Advanced.

The *Group or user names* list in the top half of the tab specifies all the security principals possessing permissions to the selected printer. The *Permissions* list in the bottom half of the tab specifies the permissions assigned to the selected security principal.

5. To revoke existing permissions, select one of the security principals in the *Group or user names* list and clear any or all of the *Allow* check boxes in the *Permissions* list.
6. To grant new permissions, click *Add*. The Select Users, Computers, Service Accounts, Or Groups dialog box appears.



Select this object type:
Users, Groups, or Built-in security principals

From this location:
adatum.local

Enter the object names to select (examples):

7. In the *Enter the object names to select* text box, type the name of the user or group you want to add to the list and click *OK*. The user or group appears in the list.
8. Select the security principal you just added and, in the *Permissions* list, select the check boxes for the permissions you want to assign.
9. Click *OK*. The Properties sheet closes.

CHAPTER 11

Deploying Updates

Microsoft releases updates for its operating systems at least once per month, and while some are relatively minor, many of those updates are intended to address important issues. The classifications that Microsoft uses to describe its update releases are as follows:

- **Critical update** A bug fix that addresses a specific problem not related to security.
- **Definition update** An addition to the definition database that a product uses to detect viruses or other malware.
- **Driver** An update to a software component that enables the computer to use a specific hardware device.
- **Feature pack** An update providing new functionality between major product releases.
- **Security update** A bug fix that addresses a specific security-related problem. Security updates are further classified according to their severity: critical, important, moderate, or low.
- **Service pack** A cumulative, tested update package containing all the updates since the product release or the last service pack. Service packs might also include new features.
- **Tool** A new feature designed to perform a specific task or tasks.
- **Update rollup** A cumulative, tested collection of updates for a specific component, such as Internet Explorer, or addressing a specific area, such as security.
- **Update** A bug fix that addresses a specific noncritical problem not related to security.

Keeping servers and workstations updated is one of the most important jobs of a network administrator, and Windows Small Business Server (SBS) 2011 includes features that simplify the process.

Understanding the Update Process

All the current Windows operating systems include a Windows Update client, which you can configure to connect to the Microsoft Update servers on the Internet at regular intervals, download the latest operating system updates, and install them, all without user intervention. However, in a network environment, Windows Update has several limitations in its default configuration, including the following:

- **Client configuration** In a network environment, configuring and activating the Windows Update client on each individual computer is a time- and labor-intensive task. The larger the network, the longer and more difficult the task.
- **Bandwidth utilization** When each computer on the network performs its own separate downloads from the Microsoft Update servers, as shown in Figure 11-1, your Internet connection can become saturated with multiple downloads of the same files. This can consume a great deal of bandwidth and slow down other processes, especially when large updates, such as service packs, are involved.

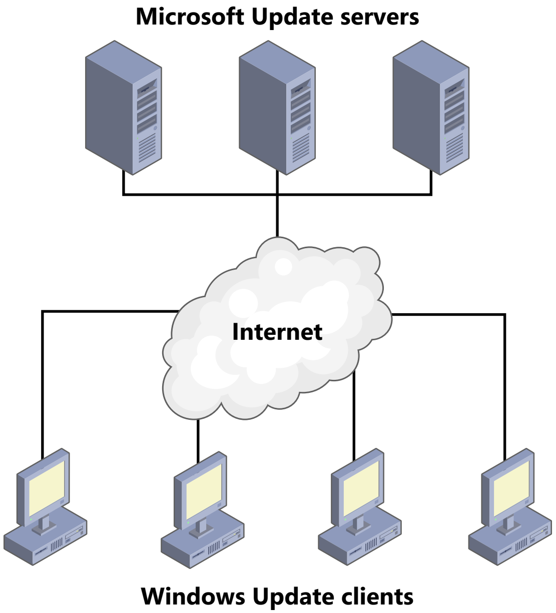


FIGURE 11-1 Individual Windows Update clients downloading updates from the Internet.

- **Update evaluation** You can configure the Windows Update client to download updates and wait for a user to install them, but the decision of whether to install a specific update is then out of the hands of the network administrator. In this default configuration, the only way to regain control would be to travel to each computer and manually install the updates.

Fortunately, Windows SBS 2011 includes tools that address all these problems.

Windows Server Update Services

Windows Server Update Services (WSUS) is a Windows Server 2008 R2 role that enables network administrators to deploy what is essentially a Microsoft Update server on their local networks. WSUS downloads all the latest updates from the Microsoft Update servers on the Internet, and then the clients on the network download their updates from the WSUS server.

To use WSUS with Windows Server 2008, an administrator must download the WSUS product, install it on a server, configure it to download updates, approve the updates for deployment, and configure the clients on the network to use WSUS. Beginning with the Windows Server 2008 R2 release, WSUS is incorporated into the operating system as a role. In Windows SBS 2011, the setup program performs all the installation and configuration tasks automatically. Your Windows SBS server then becomes a WSUS server, in addition to performing its other roles.

> ***NOTE*** **Windows SBS 2011 uses the simplest possible WSUS architecture, which consists of a single WSUS server that provides updates for all the network clients. However, it is also possible to create more complex WSUS installations for larger networks, in which one WSUS server functions as the source for other WSUS servers.**

When you use WSUS to deploy updates, instead of each computer downloading the same files from the Internet independently, only the WSUS server uses the Internet connection, as shown in Figure 11-2. The WSUS server downloads a copy of each selected update and saves it in a local data store, making it available for access by all the computers on the network. Because the WSUS server has to download only one copy of each update, the amount of Internet bandwidth consumed by the update process is reduced drastically. WSUS also provides administrators with the opportunity to research, evaluate, and test updates before deploying them to the network clients.

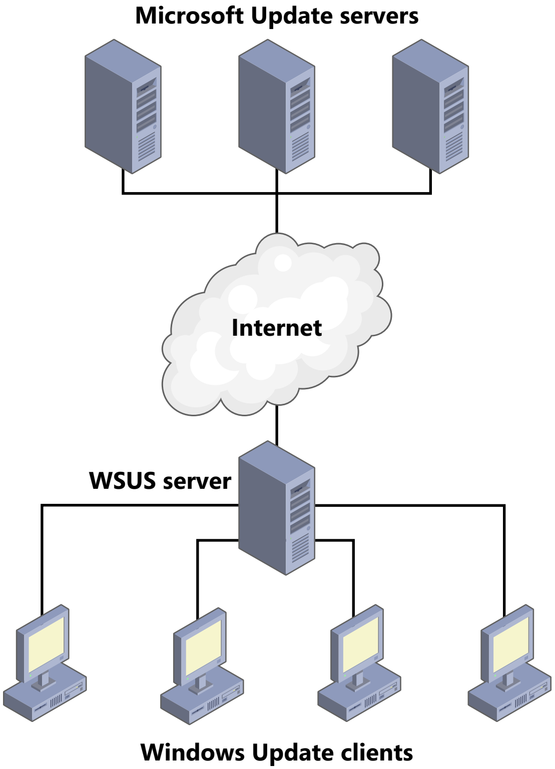


FIGURE 11-2 WSUS downloading a single copy of each update and distributing it to the network.

By incorporating WSUS into its default installation, Windows SBS 2011 completes many of the configuration tasks that Windows Server 2008 R2 administrators must perform manually. When the Windows SBS installation is finished, the WSUS server is ready to download a catalog of updates from the Internet, a process called *synchronization*. WSUS then automatically approves certain updates for distribution, downloads them, and prepares to deploy them to the clients on the network. You can also modify the default behavior of WSUS using the Windows SBS Console or the Update Services snap-in for the Microsoft Management Console (MMC). For example, If you want to evaluate or test updates before deploying them, you can configure WSUS to perform the downloads and store them until an administrator approves them for distribution.

Group Policy and Windows Update

WSUS addresses the problems of bandwidth utilization and update evaluation, but not the client configuration problem. WSUS provides a service that clients can use, but it does not configure the clients to use it. To do this, Windows SBS 2011 uses Group Policy settings to configure the Windows Update client on network workstations.

> ***MORE INFO*** **For more information on Group Policy, see Chapter 6, "Working with Users, Computers, and Groups."**

During the server installation, the Windows SBS 2011 setup program creates three Update Services Group Policy objects (GPOs). These GPOs contain settings that configure the Windows Update clients on all the network's servers and workstations to request updates from the WSUS server instead of from the Microsoft Update servers on the Internet.

Understanding the WSUS Default Settings

WSUS is essentially a web application that uses a Microsoft SQL Server database to store information about the updates that it downloads from the Internet. The Windows SBS 2011 setup program creates a website for WSUS and installs the Windows Internal Database feature, which is a limited version of SQL Server included with Windows Server 2008 R2. Clients connect to the server using a Uniform Resource Locator (URL) specified in their Group Policy settings and download all the updates that are approved for their use.

WSUS is a highly configurable application. When you deploy WSUS on a server running Windows Server 2008 R2, you have to install a role and then install the Windows Server Update Services Configuration Wizard. These two procedures enable you to configure a variety of parameters, including what database to use, where to store the update files, what products and operating systems to update, and when to synchronize with the Microsoft Update servers.

> ***NOTE*** **Prior to Windows Server 2008 R2, WSUS was a standalone free product that you had to obtain from the Microsoft Download Center and install manually. The standalone version, now known as WSUS 3.0 SP2, is still available for download.**

Windows SBS 2011 configures all these options for you, though. Once the installation is completed, the server automatically synchronizes with the Microsoft Update servers, approves new updates, and deploys them to clients. You can reconfigure WSUS to conform to your organization's timetable and other needs, but first you must become familiar with the application's default settings:

- **Synchronization** The setup program configures WSUS to synchronize with the Microsoft Update servers daily at 10 P.M.

- **Products** By default, WSUS synchronizes updates for all the products that it supports, including server and workstation operating systems; server applications, such as Microsoft Exchange Server and SQL Server; and productivity applications, such as Microsoft Office.
- **Classifications** WSUS synchronizes, by default, all critical updates, definition updates, security updates, service packs, and update rollups. It does not synchronize drivers; feature packs; tools; or noncritical, nonsecurity updates.
- **Languages** WSUS synchronizes only updates in the language that you specified when installing Windows SBS 2011.
- **Approvals** By default, WSUS automatically approves all security, critical, and definition updates for servers. For clients, WSUS approves all security, critical, and definition updates, plus service packs.
- **Storage** WSUS downloads only the approved updates and stores them, in CAB format, in the C:\WSUS\WsusContent folder by default.
- **Server updates** Servers download the latest updates from the WSUS server and inform the administrator that they are ready to install. An administrator must install them manually using the Windows Update Control panel.
- **Client updates** Clients connect to the WSUS server and download the latest updates for their respective operating systems, and then install them automatically each day at 3 A.M. If necessary, the Windows Update client restarts the computer when the update installations finish.

There is almost nothing you have to do to use WSUS in its default configuration. The server synchronizes itself, approves the most important updates, and downloads them. As you add clients to the network, they receive the Group Policy settings from the server that configures their Windows Update clients, causing the computers to download and install new updates as they become available.

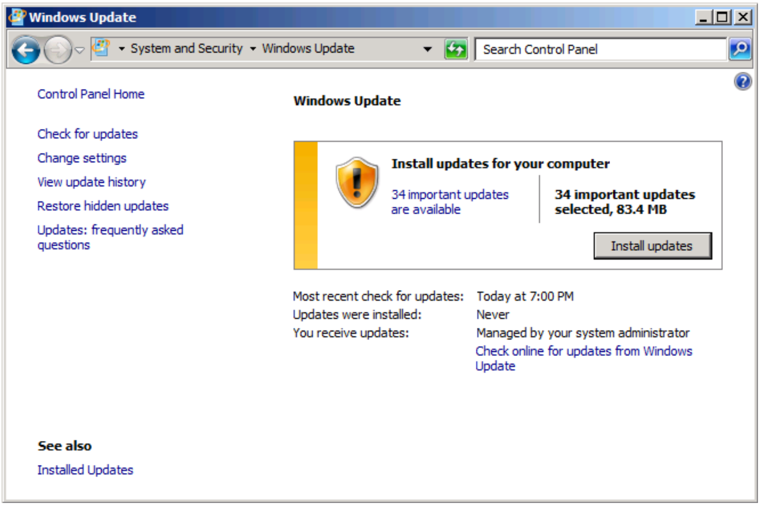
Installing Server Updates Manually

The main WSUS-related task that administrators have to perform on a regular basis is to install updates on the servers manually. By default, servers receive Group Policy settings that configure the Windows Update client to download updates from the WSUS server, but not to install them. There are several reasons for this arrangement.

The servers in a Windows SBS 2011 installation are critical to the operation of the network, and administrators should exercise more care in the maintenance of servers than they do with the maintenance of workstations. Although Microsoft tests updates before releasing them to the public, updates still can cause problems. Windows SBS 2011 administrators should evaluate each update intended for the servers by reading the documentation associated with it and then deciding whether to install it. You might also want to test an update on another computer before installing it on your production server or wait to see if other users experience any issues.

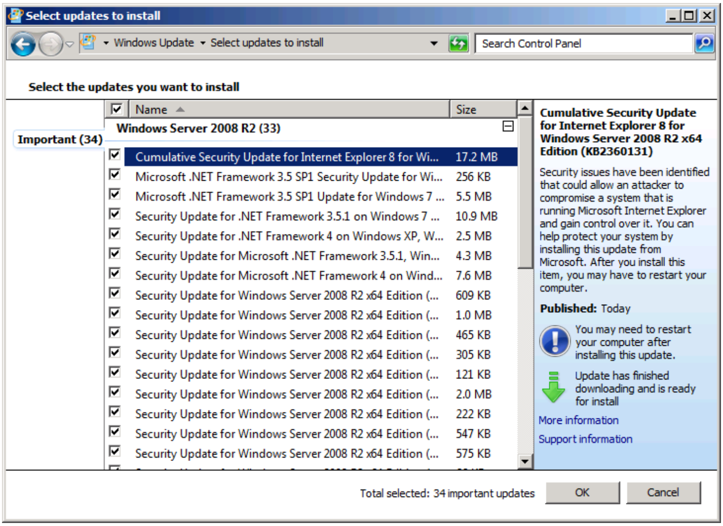
Another important factor is that many updates require a system restart before they take effect. The default Windows Update configuration permits client workstations to restart themselves if an update requires it. However, this action is not recommended for a server, which might be in the middle of a system backup or other important operation. WSUS therefore requires administrators to install manually any updates that WSUS supplies to them using the following procedure:

1. Log on to a Windows SBS 2011 server, using an account with network Administrator privileges.
2. Click *Start*, then click *Control panel*. The Control Panel window appears.
3. Click *System security* and then click *Windows UPDATE*. The Windows Update Control panel appears.



Most recent check for updates: Today at 7:00 PM
Updates were installed: Never
You receive updates: Managed by your system administrator
Check online for updates from Windows Update

4. In the *Install updates for your computer* box, click the hyperlink specifying the number of updates available for your computer. The Select Updates To Install window appears.



Select updates to install

Windows Update ▸ Select updates to install

Search Control Panel

Select the updates you want to install

Important (34)

☑	Name	Size
	Windows Server 2008 R2 (33)	
☑	Cumulative Security Update for Internet Explorer 8 for Wi...	17.2 MB
☑	Microsoft .NET Framework 3.5 SP1 Security Update for Wi...	256 KB
☑	Microsoft .NET Framework 3.5 SP1 Update for Windows 7 ...	5.5 MB
☑	Security Update for .NET Framework 3.5.1 on Windows 7 ...	10.9 MB
☑	Security Update for .NET Framework 4 on Windows XP, W...	2.5 MB
☑	Security Update for Microsoft .NET Framework 3.5.1, Win...	4.3 MB
☑	Security Update for Microsoft .NET Framework 4 on Wind...	7.6 MB
☑	Security Update for Windows Server 2008 R2 x64 Edition (...	609 KB
☑	Security Update for Windows Server 2008 R2 x64 Edition (...	1.0 MB
☑	Security Update for Windows Server 2008 R2 x64 Edition (...	465 KB
☑	Security Update for Windows Server 2008 R2 x64 Edition (...	305 KB
☑	Security Update for Windows Server 2008 R2 x64 Edition (...	121 KB
☑	Security Update for Windows Server 2008 R2 x64 Edition (...	2.0 MB
☑	Security Update for Windows Server 2008 R2 x64 Edition (...	222 KB
☑	Security Update for Windows Server 2008 R2 x64 Edition (...	547 KB
☑	Security Update for Windows Server 2008 R2 x64 Edition (...	575 KB

Cumulative Security Update for Internet Explorer 8 for Windows Server 2008 R2 x64 Edition (KB2360131)

Security issues have been identified that could allow an attacker to compromise a system that is running Microsoft Internet Explorer and gain control over it. You can help protect your system by installing this update from Microsoft. After you install this item, you may have to restart your computer.

Published: Today

You may need to restart your computer after installing this update.

Update has finished downloading and is ready for install

More information

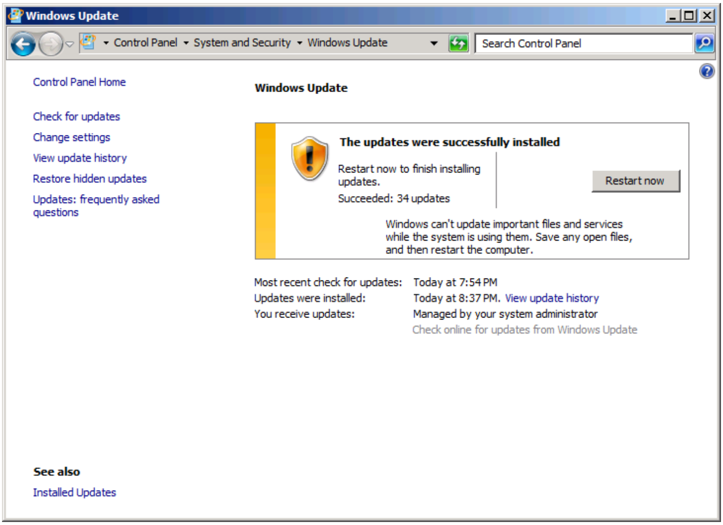
Support information

Total selected: 34 important updates

OK Cancel

5. Clear the check boxes for the updates that you do not want to install. Then click *OK*. The Windows Update window reappears.
6. Click *Install updates*. The Control panel displays the progress as the system installs the updates.

   When the installation is finished, the Windows Update window indicates the outcome of the installation and specifies which updates failed to install, if any.



Windows Update

Control Panel ▸ System and Security ▸ Windows Update

Search Control Panel

Control Panel Home

Check for updates

Change settings

View update history

Restore hidden updates

Updates: frequently asked questions

Windows Update

The updates were successfully installed

Restart now to finish installing updates.

Succeeded: 34 updates

Restart now

Windows can't update important files and services while the system is using them. Save any open files, and then restart the computer.

Most recent check for updates: Today at 7:54 PM

Updates were installed: Today at 8:37 PM. View update history

You receive updates: Managed by your system administrator

Check online for updates from Windows Update

See also

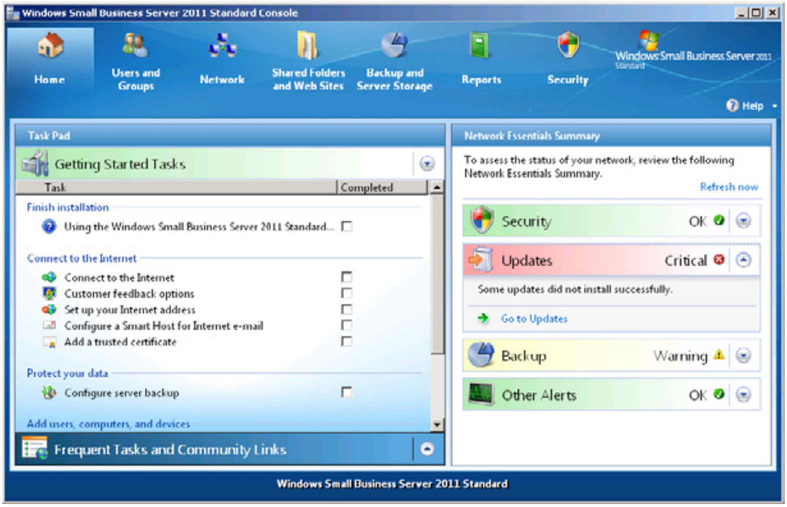
Installed Updates

7. Click *Restart now* if the system prompts you to do so. The server restarts.

Monitoring WSUS Activity

The only other task that administrators should perform on a regular basis when running WSUS in its default configuration is to monitor the WSUS activities to make sure that all servers and workstations are receiving the updates they should on a regular basis.

In the Windows SBS Console, the Network Essentials Summary pane on the Home page contains an *Updates* indicator, as shown in Figure 11-3, which displays the current overall status of WSUS operations. An *OK* status means that all the computers on the network have all the latest updates installed, while a *Warning* status means that there are updates yet to be installed on all or some of the network's computers.



Windows Small Business Server 2011 Standard Console
Home
Users and Groups
Network
Shared Folders and Web Sites
Backup and Server Storage
Reports
Security
Windows Small Business Server 2011 Standard
Help
Task Pad
Getting Started Tasks
Task
Completed
Network Essentials Summary
Refresh now
Frequent Tasks and Community Links
Windows Small Business Server 2011 Standard

Finish installation

- Using the Windows Small Business Server 2011 Standard... □

Connect to the Internet

- Connect to the Internet □
- Customer feedback options □
- Set up your Internet address □
- Configure a Smart Host for Internet e-mail □
- Add a trusted certificate □

Protect your data

- Configure server backup □

Add users, computers, and devices

To assess the status of your network, review the following Network Essentials Summary.

Security	OK
Updates	Critical
Backup	Warning
Other Alerts	OK

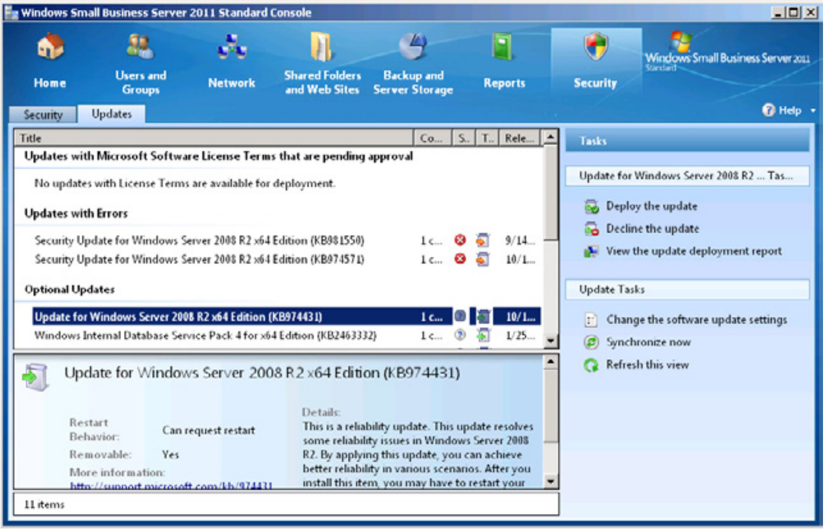
Some updates did not install successfully.

Go to Updates

FIGURE 11-3 The *Updates* indicator in the Network Essentials Summary pane.

When you click the *Go to updates* link in the Network Essentials Summary pane or click the Security page and select the *Updates* tab, the display shown in Figure 11-4 appears. The main element on this page is a list of updates in the following four categories:

- **Updates with Microsoft software license terms that are pending approval** Updates with special license terms to which you must agree before installing them
- **Updates with errors** Updates that failed to install correctly on one or more computers
- **Optional updates** Unapproved updates that are not essential to secure and efficient system operation
- **Updates in progress** Updates that have been installed on some of the network's computers, but not all of them


Windows Small Business Server 2011 Standard Console
Home
Users and Groups
Network
Shared Folders and Web Sites
Backup and Server Storage
Reports
Security
Windows Small Business Server 2011 Standard
Security
Updates
Help
Tasks
Update for Windows Server 2008 R2 ... Tas...
Deploy the update
Decline the update
View the update deployment report
Update Tasks
Change the software update settings
Synchronize now
Refresh this view

Title	Co...	S...	T...	Rele...
Updates with Microsoft Software License Terms that are pending approval				
No updates with License Terms are available for deployment.				
Updates with Errors				
Security Update for Windows Server 2008 R2 x64 Edition (KB981550)	1 c...			9/14...
Security Update for Windows Server 2008 R2 x64 Edition (KB974571)	1 c...			10/1...
Optional Updates				
Update for Windows Server 2008 R2 x64 Edition (KB974431)	1 c...			10/1...
Windows Internal Database Service Pack 4 for x64 Edition (KB2463332)	1 c...			1/25...

Update for Windows Server 2008 R2 x64 Edition (KB974431)

Restart Behavior: Can request restart

Removable: Yes

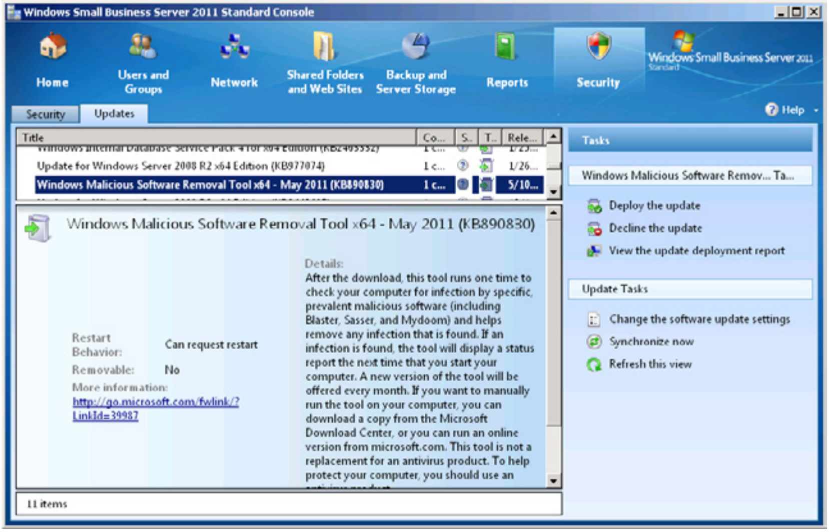
More information: http://support.microsoft.com/kb/974431

Details: This is a reliability update. This update resolves some reliability issues in Windows Server 2008 R2. By applying this update, you can achieve better reliability in various scenarios. After you install this item, you may have to restart your

11 items

FIGURE 11-4 The Updates page in the Windows SBS Console.

When you select an update from any of these four lists, the pane below the list displays information about that specific update, as shown in Figure 11-5, plus a link to the Microsoft Knowledge Base article containing documentation for the update.


Windows Small Business Server 2011 Standard Console
Home
Users and Groups
Network
Shared Folders and Web Sites
Backup and Server Storage
Reports
Security
Windows Small Business Server 2011 Standard
Security
Updates
Help
Tasks
Windows Malicious Software Remov... Ta...
Deploy the update
Decline the update
View the update deployment report
Update Tasks
Change the software update settings
Synchronize now
Refresh this view

Title	Co...	S...	T...	Rele...
Windows Internal Database Service Pack 4 for x64 Edition (KB2463332)	1 c...			1/25...
Update for Windows Server 2008 R2 x64 Edition (KB977074)	1 c...			1/26...
Windows Malicious Software Removal Tool x64 - May 2011 (KB890830)	1 c...			5/10...

Windows Malicious Software Removal Tool x64 - May 2011 (KB890830)

Restart Behavior: Can request restart

Removable: No

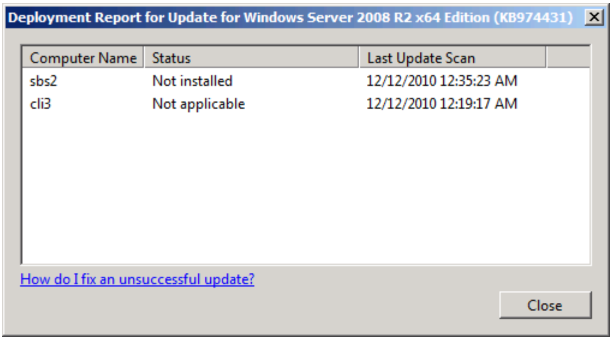
More information: http://go.microsoft.com/fwlink/?LinkId=39987

Details: After the download, this tool runs one time to check your computer for infection by specific, prevalent malicious software (including Blaster, Sasser, and Mydoom) and helps remove any infection that is found. If an infection is found, the tool will display a status report the next time that you start your computer. A new version of the tool will be offered every month. If you want to manually run the tool on your computer, you can download a copy from the Microsoft Download Center, or you can run an online version from microsoft.com. This tool is not a replacement for an antivirus product. To help protect your computer, you should use an antivirus product.

11 items

FIGURE 11-5 Update information, as displayed in the Windows SBS Console.

When you select an update from the list and click *View the update deployment report* in the Tasks pane, a Deployment Report window appears, as shown in Figure 11-6. This window provides the status of that update on each of the network's computers.

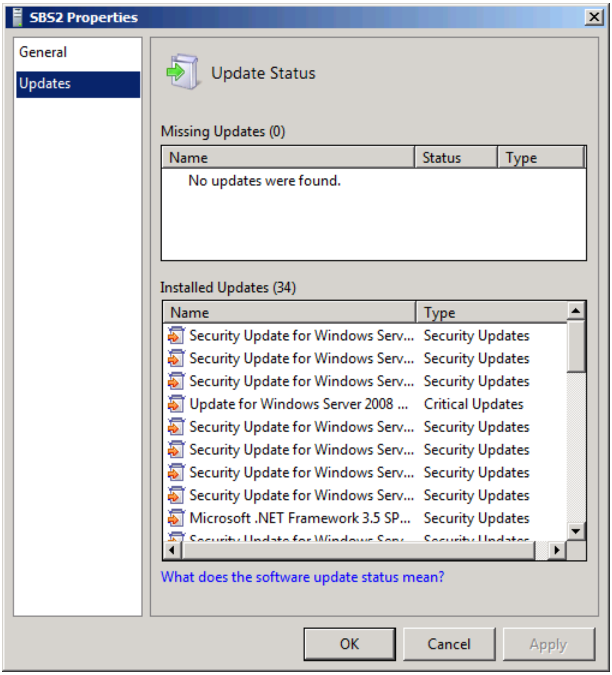


Deployment Report for Update for Windows Server 2008 R2 x64 Edition (KB974431)

Computer Name	Status	Last Update Scan
sbs2	Not installed	12/12/2010 12:35:23 AM
cli3	Not applicable	12/12/2010 12:19:17 AM

FIGURE 11-6 An Update's Deployment Report window.

Notice that the Updates page does not contain a list of the updates that all the computers on the network have installed successfully. The Windows SBS Console is more concerned with informing administrators of conditions that require their attention than providing complete documentation of background activities. However, it is possible to display the installed and missing updates for a specific computer by opening its Properties sheet from the *Computers* tab of the Network page and clicking *Updates*, as shown in Figure 11-7.



Missing Updates (0)

Name	Status	Type
No updates were found.		

Installed Updates (34)

Name	Type
Security Update for Windows Serv...	Security Updates
Security Update for Windows Serv...	Security Updates
Security Update for Windows Serv...	Security Updates
Update for Windows Server 2008 ...	Critical Updates
Security Update for Windows Serv...	Security Updates
Security Update for Windows Serv...	Security Updates
Security Update for Windows Serv...	Security Updates
Security Update for Windows Serv...	Security Updates
Microsoft .NET Framework 3.5 SP...	Security Updates
Security Update for Windows Serv...	Security Updates

FIGURE 11-7 The Updates page in a computer's Properties sheet.

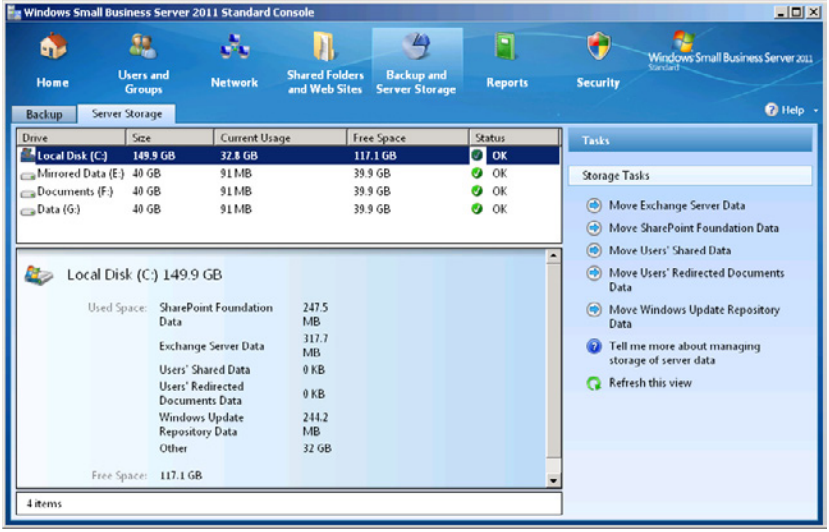
Configuring WSUS Using the Windows SBS Console

Windows SBS 2011 provides a functional WSUS installation by default, but there are many possible reasons why administrators might want to modify those default settings. The following sections examine the various WSUS configuration settings that you can change using the Windows SBS Console, as well as the reasons why you might want to change them.

Moving the Update Repository

The Windows SBS 2011 setup program configures WSUS to store the updates that it downloads from the Internet on the computer's C drive. This is largely because C is usually the only drive available during a new server installation. However, you might want to move the update repository to another drive later. To move the WSUS data store, click *Backup* and *Server storage* in the Windows SBS Console, then choose the *Server storage* tab. Finally, under the *Storage tasks* list, select the *Move Windows Update repository data* task, as shown in Figure 11-8.

> ***MORE INFO*** **For a reminder of the general procedure and reasons for moving the various data stores that Windows SBS 2011 creates on the C drive by default, see the "Moving Data Stores" section of Chapter 9, "Managing Storage."**


Windows Small Business Server 2011 Standard Console
Home
Users and Groups
Network
Shared Folders and Web Sites
Backup and Server Storage
Reports
Security
Windows Small Business Server 2011 Standard
Backup
Server Storage
Help
Tasks
Storage Tasks
Move Exchange Server Data
Move SharePoint Foundation Data
Move Users' Shared Data
Move Users' Redirected Documents Data
Move Windows Update Repository Data
Tell me more about managing storage of server data
Refresh this view

Drive	Size	Current Usage	Free Space	Status
Local Disk (C:)	149.9 GB	32.8 GB	117.1 GB	OK
Mirrored Data (E:)	40 GB	91 MB	39.9 GB	OK
Documents (F:)	40 GB	91 MB	39.9 GB	OK
Data (G:)	40 GB	91 MB	39.9 GB	OK

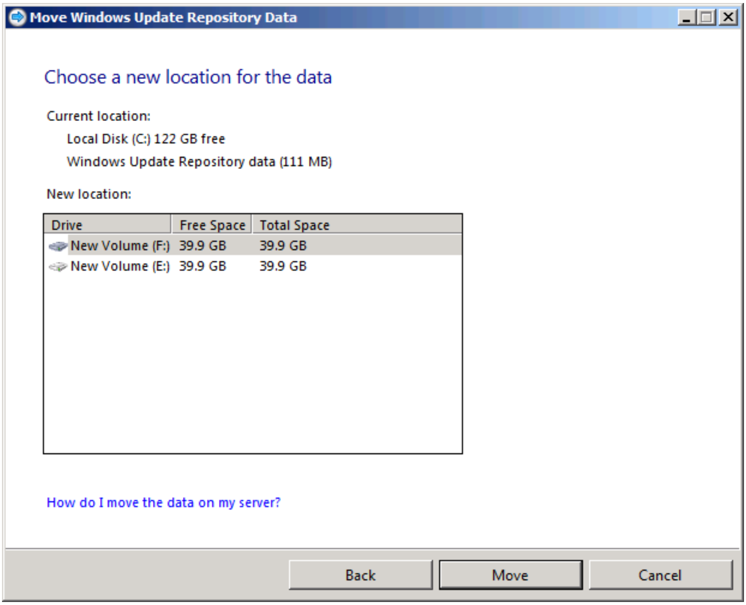
Local Disk (C:) 149.9 GB

Used Space:	SharePoint Foundation Data	247.5 MB
	Exchange Server Data	317.7 MB
	Users' Shared Data	0 KB
	Users' Redirected Documents Data	0 KB
	Windows Update Repository Data	244.2 MB
	Other	32 GB
Free Space:	117.1 GB	

4 items

FIGURE 11-8 The Backup And Server Storage page of the Windows SBS Console.

As with the other data stores on the server running Windows SBS 2011, you can move the WSUS data to any available volume on the computer (see Figure 11-9). Because the updates are readily available on the Internet, there is usually no need to store them on a fault tolerant volume—that would be a needless expense. The most common reason for moving the WSUS data store is to free up disk space on the C drive.



Choose a new location for the data

Current location:

Local Disk (C:) 122 GB free

Windows Update Repository data (111 MB)

New location:

Drive	Free Space	Total Space
New Volume (F:)	39.9 GB	39.9 GB
New Volume (E:)	39.9 GB	39.9 GB

How do I move the data on my server?

FIGURE 11-9 The Choose A New Location For The Data page.

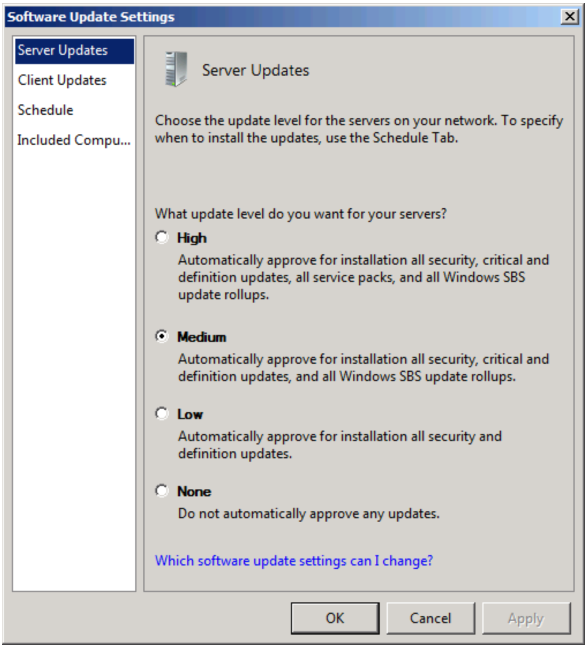
Configuring Software Update Settings

The Windows SBS Console enables you to modify the default settings for some of the most basic WSUS and Windows Update parameters. To configure these settings, use the following procedure:

1. Log on to your Windows SBS 2011 server, using an account with network Administrator privileges. The Windows SBS Console appears.
2. Click *Security*, and then select the *Updates* tab.
3. In the *Tasks* list, click *Change the software update settings*. The Software Update Settings dialog box appears.

4. Select one of the following tabs and use the controls to configure the following settings located there:

   - **Server updates** Specifies, by classification, which updates WSUS should automatically approve for servers. The default Medium setting omits service packs.



Server Updates

Choose the update level for the servers on your network. To specify when to install the updates, use the Schedule Tab.

What update level do you want for your servers?

○ **High**
Automatically approve for installation all security, critical and definition updates, all service packs, and all Windows SBS update rollups.

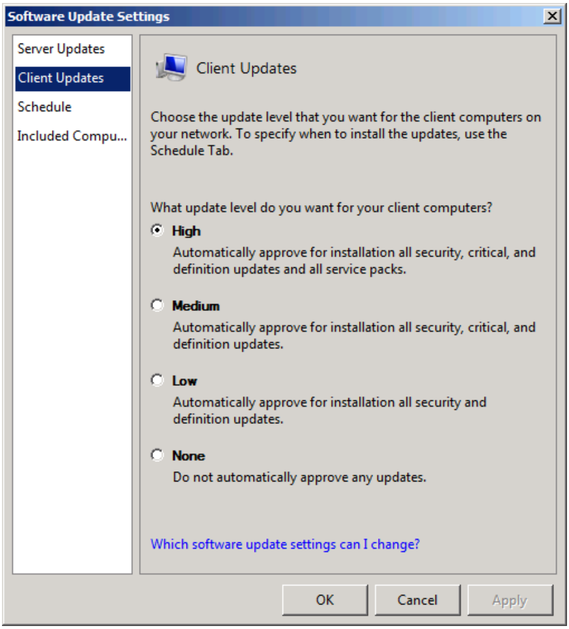
● **Medium**
Automatically approve for installation all security, critical and definition updates, and all Windows SBS update rollups.

○ **Low**
Automatically approve for installation all security and definition updates.

○ **None**
Do not automatically approve any updates.

Which software update settings can I change?

   - **Client updates** Specifies, by classification, which updates WSUS should approve automatically for clients. The default High setting includes all high-priority updates and service packs.



Client Updates

Choose the update level that you want for the client computers on your network. To specify when to install the updates, use the Schedule Tab.

What update level do you want for your client computers?

● **High**
Automatically approve for installation all security, critical, and definition updates and all service packs.

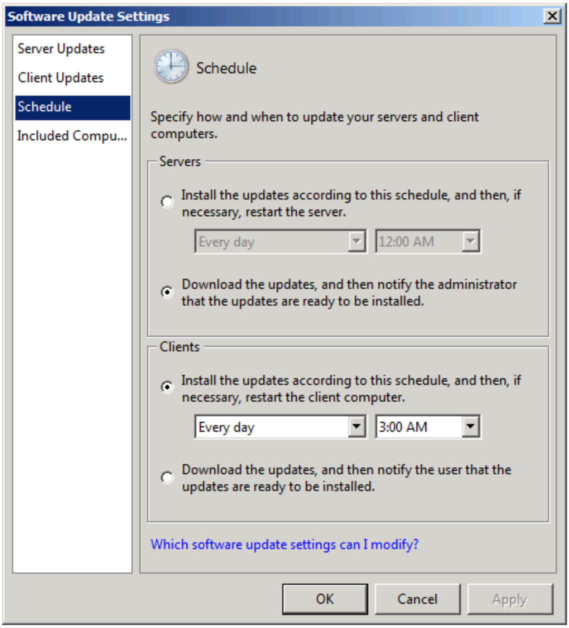
○ **Medium**
Automatically approve for installation all security, critical, and definition updates.

○ **Low**
Automatically approve for installation all security and definition updates.

○ **None**
Do not automatically approve any updates.

Which software update settings can I change?

- **Schedule** Specifies whether servers and clients should install updates automatically and, if so, how often and at what time the installations should occur.



Schedule

Specify how and when to update your servers and client computers.

Servers

○ Install the updates according to this schedule, and then, if necessary, restart the server.
Every day | 12:00 AM

● Download the updates, and then notify the administrator that the updates are ready to be installed.

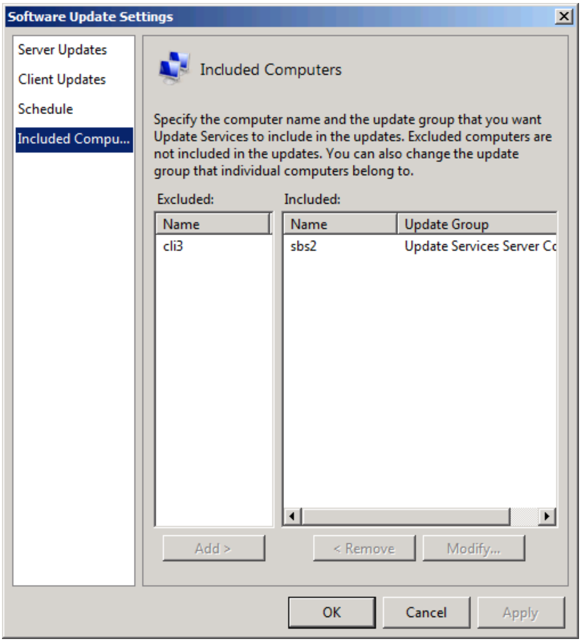
Clients

● Install the updates according to this schedule, and then, if necessary, restart the client computer.
Every day | 3:00 AM

○ Download the updates, and then notify the user that the updates are ready to be installed.

Which software update settings can I modify?

- **Included computers** Specifies which of the computers on the network should obtain their updates from the WSUS server.



Software Update Settings

Included Computers

Specify the computer name and the update group that you want Update Services to include in the updates. Excluded computers are not included in the updates. You can also change the update group that individual computers belong to.

Excluded:

Name
cli3

Included:

Name	Update Group
sbs2	Update Services Server Cc

5. Click *OK*. The Software Update Settings dialog box closes.

Specifying Update Levels

The Server Updates And Client Updates pages in the Software Update Settings dialog box specify which types of updates WSUS should approve automatically for your servers and client workstations, respectively. In the default configuration, the only difference between the server and client settings is the inclusion of service packs for the clients.

Service packs are major updates, and many administrators do not like to install them as soon as they are released, preferring instead to wait to see if problems arise. The installation of a service pack requires a system restart and can also be a lengthy process, so you must be sure that the installation occurs at an appropriate time of day.

If you prefer to wait before installing service packs on your clients, you can change the *Client updates* setting to *Medium*. This enables you to gauge the industry response to the service pack release and possibly install it manually in a test laboratory environment before deploying it on the whole network.

Scheduling Update Installations

The installation of the updates on your network computers is controlled by the Windows Update client, not WSUS. Therefore, the *Schedule* tab of the Software Update Settings dialog box actually modifies the Group Policy settings that configure the Windows Update client.

Here again, servers and clients have their own separate settings. The default setting for clients is to install new updates automatically every day at 3 A.M. Depending on your organization's work schedule, you might want to change the time of the installation or even limit it to one day a week instead of every day. Microsoft typically releases new updates once per month, so you might feel that a daily schedule is not necessary. However, Microsoft does sometimes release updates that are particularly critical between the usual monthly cycles.

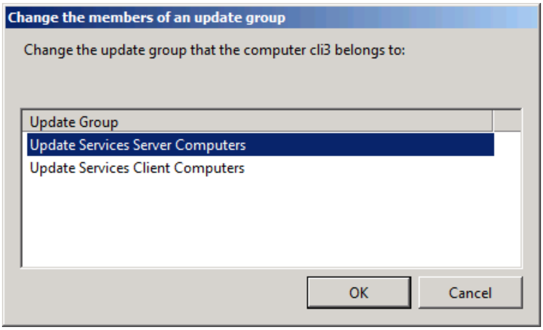
Another element to consider with client updates is whether your users are accustomed to shutting their computers down at the end of each workday. Obviously, an update installation cannot occur when a computer is turned off. If a scheduled installation does not occur, because the computer is shut down or for any other reason, the Windows Update client triggers the installation one minute after the computer's next startup. If this causes problems, you can change this behavior, but only by modifying the GPOs directly. For more information on modifying the Group Policy settings that control the Windows Update client, see the section entitled "Configuring the Windows Update Client Using Group Policy," later in this chapter.

For servers, the default setting enables the computers to download new updates from the WSUS server, but the computers do not install them automatically. This enables administrators to exercise greater control over which updates the servers receive, and when. For information on how to install updates manually on servers running Windows SBS 2011, see the section entitled "Installing Server Updates Manually," earlier in this chapter.

Excluding Computers

The Included Computers page of the Software Update Settings dialog box enables you to specify which of the computers on your network you want to receive updates from WSUS. By default, all your computers are included, but if you want to change the default, you can select a computer and click *Remove* to disable its Windows Update client entirely.

You can also select a computer and click *Modify* to display the Change The Members Of An Update Group dialog box, as shown in Figure 11-10. This dialog box enables you to put a client workstation in the *Update services server computers* group to prevent it from automatically installing updates, or to put a server in the *Update services client computers* group to enable automatic update installations.



Change the members of an update group

Change the update group that the computer cli3 belongs to:

Update Group
Update Services Server Computers
Update Services Client Computers

FIGURE 11-10 The Change The Members Of An Update Group dialog box.

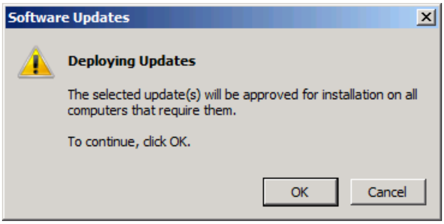
Synchronizing WSUS

WSUS synchronizes with the Microsoft Update servers on the Internet once every day, but you can trigger a manual synchronization using the Windows SBS Console at any time by clicking *Synchronize now* in the *Tasks* list on the Security/Updates page.

Approving Updates

WSUS automatically approves the most important updates by default, but the Security/Updates page also contains a list of optional updates. WSUS does not approve these updates automatically. If you want to deploy them on your network, you must approve them manually, using the following procedure:

1. Log on to your Windows SBS 2011 server using an account with network Administrator privileges. The Windows SBS Console appears.
2. Click *Security*, and then select the *Updates* tab.
3. Select one of the entries in the *Optional updates* list and, in the *Tasks* list, click *Deploy the update*. A Software Updates message box appears, prompting you to confirm your action.



Software Updates

Deploying Updates

The selected update(s) will be approved for installation on all computers that require them.

To continue, click OK.

4. Click *OK*. Another Software Updates message box appears, informing you that the update is approved.
5. Click *OK*. The update moves from the *Optional updates* list to the *Updates in progress* list.

> **TIP** **You can also remove an entry from the *Optional updates* list and delete it permanently from the update repository by selecting it and clicking *Decline the update*.**

Configuring the Windows Update Client Using Group Policy

The Windows SBS Console contains controls that enable you to configure only the most basic properties of the Windows Update client on your network computers, such as the time that installations should occur. To exercise more complete control over the client, you must modify the GPOs that contain the configuration settings for Windows Update.

Windows SBS 2011 creates three separate GPOs to configure Windows Update clients, as follows:

- **Update Services Common Settings Policy** Applies to all computers on the network
- **Update Services Client Computers Policy** Applies only to computers that are members of the Update Services Client Computers group
- **Update Services Server Computers Policy** Applies only to computers that are members of the Update Services Server Computers group

As part of its startup procedure, every computer on the network downloads and applies the Update Services Common Settings Policy GPO. This GPO contains most of the Windows Update policy settings that computers on the Windows SBS 2011 network need. The settings and default values for the Update Services Common Settings Policy GPO are listed in Table 11-1.

TABLE 11-1 Default Settings in the Update Services Common Settings Policy GPO

GROUP POLICY SETTING	DEFAULT VALUES	FUNCTION
Configure Automatic Updates	■ Notify for download and notify for install ■ 0—Every day ■ 03:00	Enables the Windows Update client, specifies whether the client should download and install updates with or without user intervention, and specifies the installation interval and time of day.

GROUP POLICY SETTING	DEFAULT VALUES	FUNCTION
Specify intranet Microsoft update service location	http://*SERVER*:####, where *SERVER* is the name of your server and #### is the port number assigned to the WSUS web application	Specifies the URL that Windows Update clients use to access the WSUS server on the local network.
Automatic Updates detection frequency	1 hour	Specifies the interval at which Windows Update clients check the server for new updates.
Allow non-administrators to receive update notifications	Enabled	Enables users without administrative privileges to receive notifications of impending update downloads or installations from the Windows Update client.
Allow Automatic Updates immediate installation	Enabled	Specifies whether the Windows Update client should install updates that do not require a service interruption or system restart immediately.
No auto-restart with logged on users for scheduled automatic updates installations	Disabled	Specifies whether the Windows Update client can trigger a system restart when a user is logged on to the system. When set to Disabled, the computer can restart automatically while a user is logged on to the computer.
Re-prompt for restart with scheduled installations	10 minutes	Specifies the time interval the Windows Update client should wait before restarting the computer after a user postponed a previous restart request.
Delay Restart for scheduled installations	5 minutes	Specifies the time interval the Windows Update client should wait before restarting the computer after an update installation.

GROUP POLICY SETTING	DEFAULT VALUES	FUNCTION
Reschedule Automatic Updates scheduled installations	1 minute	Specifies the time interval the Windows Update client should wait after system startup before initiating an update installation that did not occur because the computer was offline.

After applying the Update Services Common Settings Policy GPO, each computer then applies either the Update Services Client Computers Policy or Update Services Server Computers Policy GPO, depending on its group membership. These GPOs contain only one policy setting each, as listed in Tables 11-2 and 11-3, with each having a different default value. Because the computers apply these GPOs after the Update Services Common Settings Policy GPO, the client- or server-specific value for the Configure Automatic Updates policy setting overwrites the existing value from the first GPO.

TABLE 11-2 Default Settings in the Update Services Client Computers Policy GPO

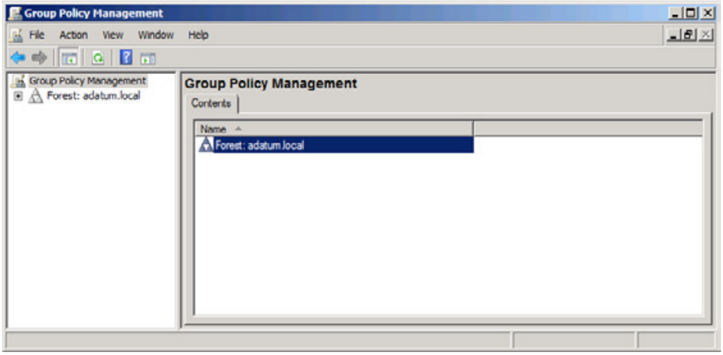
GROUP POLICY SETTING	DEFAULT VALUES	FUNCTION
Configure Automatic Updates	■ Auto download and schedule the install ■ 0—Every day ■ 03:00	Enables the Automatic Updates client, specifies whether the client should download and install updates with or without user intervention, and specifies the installation interval and time of day

TABLE 11-3 Default Settings in the Update Services Server Computers Policy GPO

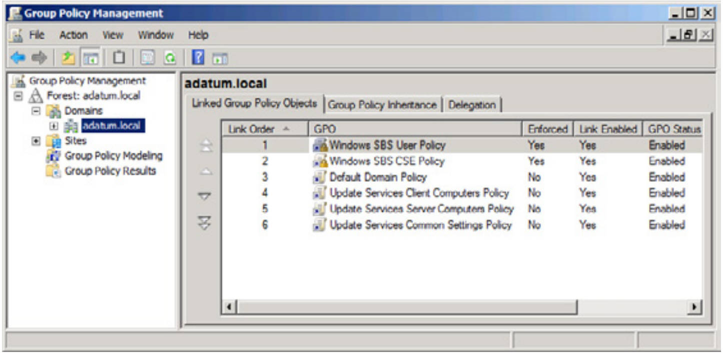
GROUP POLICY SETTING	DEFAULT VALUES	FUNCTION
Configure Automatic Updates	■ Auto download and notify for install ■ 0—Every day ■ 03:00	Enables the Automatic Updates client, specifies whether the client should download and install updates with or without user intervention, and specifies the installation interval and time of day

To modify the default settings for the Update Services Common Settings Policy GPO, use the following procedure:

1. Log on to your Windows SBS 2011 server, using an account with network Administrator privileges.
2. Click *Start*. Then click *Administrative Tools* > *Group Policy Management*. The Group Policy Management Console appears.



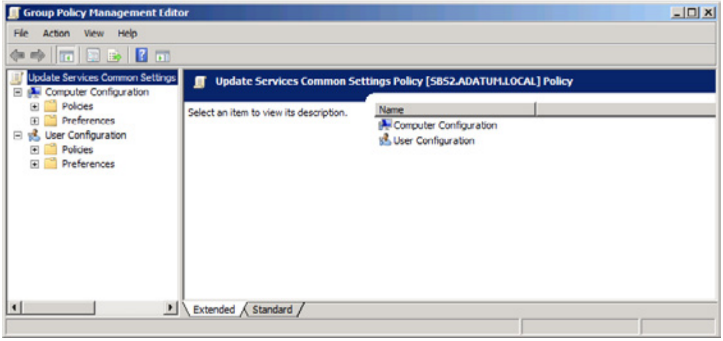
3. In the Scope (left) pane, expand the *Forest* node and browse to the node representing your domain. The Detail (right) pane lists the Group Policy objects linked to your domain object, including the three Update Services GPOs.



Link Order	GPO	Enforced	Link Enabled	GPO Status
1	Windows SBS User Policy	Yes	Yes	Enabled
2	Windows SBS CSE Policy	Yes	Yes	Enabled
3	Default Domain Policy	No	Yes	Enabled
4	Update Services Client Computers Policy	No	Yes	Enabled
5	Update Services Server Computers Policy	No	Yes	Enabled
6	Update Services Common Settings Policy	No	Yes	Enabled

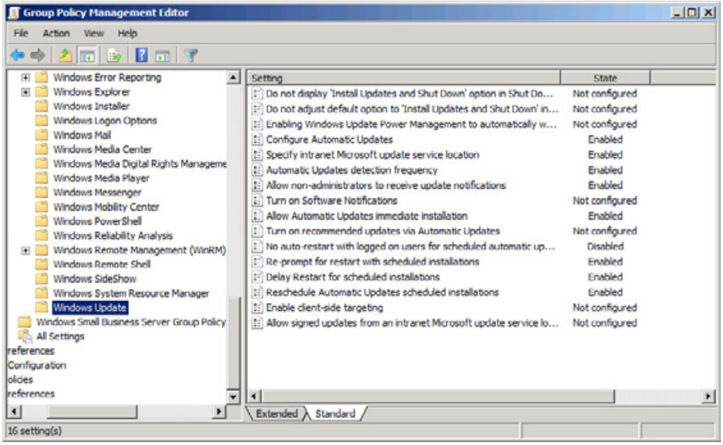
NOTE **When a domain has multiple GPOs linked to it, the computers on the network apply the GPOs in order, beginning with the last GPO in the list and ending with the first. If the same policy settings appear in more than one GPO, the settings that the system applies last take precedence. Therefore, the GPO that is number one on the list has the highest priority.**

4. Right-click the *Update services common settings policy* and, from the context menu, select *Edit*. The Group Policy Management Editor Console appears, displaying the contents of the GPO.



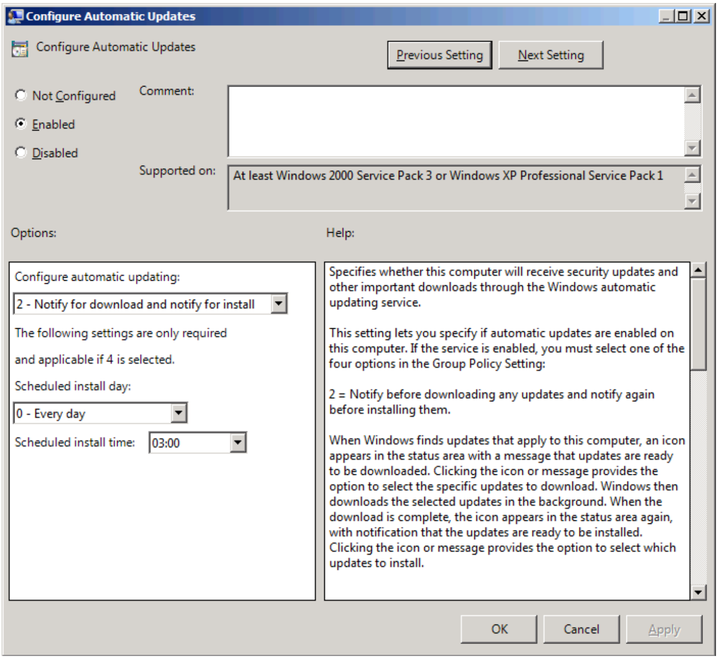
Select an item to view its description.

5. In the Scope (right) pane, browse to the Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update folder.



Setting	State
Do not display 'Install Updates and Shut Down' option in Shut Do...	Not configured
Do not adjust default option to 'Install Updates and Shut Down' in...	Not configured
Enabling Windows Update Power Management to automatically w...	Not configured
Configure Automatic Updates	Enabled
Specify intranet Microsoft update service location	Enabled
Automatic Updates detection frequency	Enabled
Allow non-administrators to receive update notifications	Enabled
Turn on Software Notifications	Not configured
Allow Automatic Updates immediate installation	Enabled
Turn on recommended updates via Automatic Updates	Not configured
No auto-restart with logged on users for scheduled automatic up...	Disabled
Re-prompt for restart with scheduled installations	Enabled
Delay Restart for scheduled installations	Enabled
Reschedule Automatic Updates scheduled installations	Enabled
Enable client-side targeting	Not configured
Allow signed updates from an intranet Microsoft update service lo...	Not configured

6. In the Detail pane, double-click one of the policy settings listed in Table 11-1. The dialog box for the policy setting appears.



Configure Automatic Updates

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows 2000 Service Pack 3 or Windows XP Professional Service Pack 1

Options:

Configure automatic updating: 2 - Notify for download and notify for install

The following settings are only required and applicable if 4 is selected.

Scheduled install day: 0 - Every day

Scheduled install time: 03:00

Help:

Specifies whether this computer will receive security updates and other important downloads through the Windows automatic updating service.

This setting lets you specify if automatic updates are enabled on this computer. If the service is enabled, you must select one of the four options in the Group Policy Setting:

2 = Notify before downloading any updates and notify again before installing them.

When Windows finds updates that apply to this computer, an icon appears in the status area with a message that updates are ready to be downloaded. Clicking the icon or message provides the option to select the specific updates to download. Windows then downloads the selected updates in the background. When the download is complete, the icon appears in the status area again, with notification that the updates are ready to be installed. Clicking the icon or message provides the option to select which updates to install.

7. Modify the values for the policy setting as desired and click *OK* to close the dialog box.
8. Repeat steps 6 and 7 to modify additional policy settings.
9. Close the Group Policy Management Editor Console.
10. Close the Group Policy Management Console.

To modify the *Configure automatic updates* policy settings that your computers actually use, you must repeat the procedure and edit the Update Services Client Computers Policy and Update Services Server Computers Policy GPOs.

The most common modifications that administrators are likely to make to these GPOs is to change the installation time and frequency in the Configure Automatic Updates policy setting, or disable the automatic installation process for clients. Some of the other modifications you might consider are the following:

- Enabling the *No auto-restart with logged on users for scheduled automatic updates installations* policy setting prevents users from being interrupted by an update installation if they are logged on when it is scheduled to occur. The potential drawback of this is that installations do not occur if a user leaves the computer logged on at the end of the day.

- The only situation in which you would want to modify the *Specify intranet Microsoft Update service location* policy setting is if you deploy another WSUS server on your network and want your users to obtain their updates from that server.
- If you want to insulate your users from the update process, you can disable the *Allow non-administrators to receive update notifications* policy setting. When you do this, most Windows Update activities occur invisibly.
- Setting the *Reschedule automatic updates scheduled installations* policy setting to *Disabled* prevents missed update installations from occurring the next time the computer starts. Instead, the installation occurs at the next scheduled time. This modification can prevent users from facing what might be a lengthy and unexpected installation procedure during business hours.

When you modify the settings in these GPOs, the new values do not take effect until the next time the computer restarts.

CHAPTER 12

Backing Up and Restoring

Backing up data is a critical administrative function for every network, one that many administrators tend to neglect. In many cases, hard disk contents are an organization's most precious possession. Their loss can cause production to cease, commerce to falter, and businesses to fail.

As the primary moving parts in a computer, hard disk drives operate at incredibly close tolerances. The platters on which hard drives store data spin at anywhere from 5,000 to 15,000 revolutions per minute (RPM), with read and write heads floating over the moving surface at distances measured in millionths of an inch. The traditional analogy is to imagine storing your most valuable possessions on an airliner flying at 600 miles per hour, a few feet over the ground.

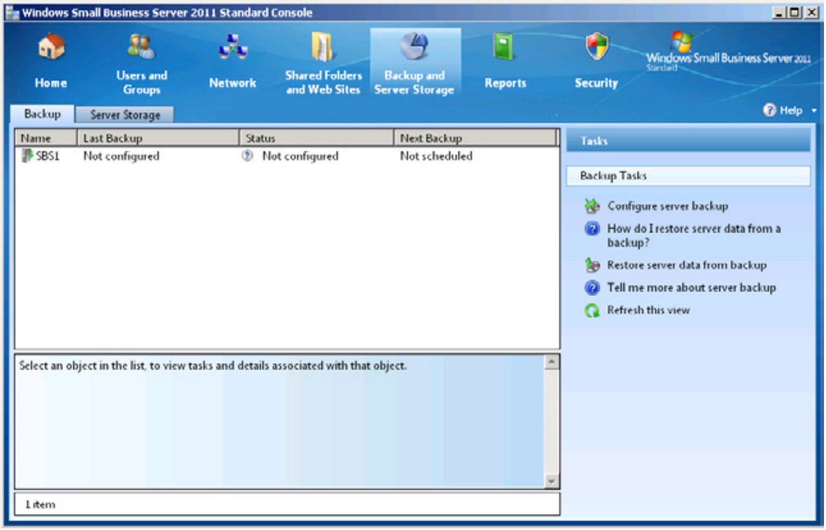
When a hard disk drive fails, whether due to a power interruption, a physical shock, a manufacturer's defect, or just simple wear and tear, it is common for the drive heads to come in contact with the platter surface and scratch the recording medium, destroying data in the process. This is called a *head crash*. Hard drive failures are inevitable; it's just a matter of when they occur. In addition to hardware malfunctions, computers are also susceptible to other disasters, such as fire and theft, which can be equally destructive to your data. Performing regular backups enables you to replace your data at the same time that you replace a drive or computer, and resume productivity as quickly as possible.

Windows Server 2008 R2 includes a basic backup software program called Windows Server Backup, which is sufficient to provide your Windows SBS 2011 server with protection against a drive failure. Depending on how you organize the storage on your network, however, this basic coverage might or might not be sufficient. This chapter provides an introduction to the complexities of network backups and enables you to design a solution suitable to your needs.

Creating a Backup Strategy

In a large enterprise network environment, creating an effective backup strategy can require a huge investment of time, effort, and money. Backing up a large number of servers typically requires additional third-party software and an extensive amount of specialized hardware. For small business networks, however, the task is usually far less difficult.

The Windows SBS Console in Windows Small Business Server (SBS) 2011 incorporates server backups into the *Getting started tasks* list, which you perform after completing the operating system installation. The Server Storage wizards in the console, which you can use to move specific data stores to new locations, even check to make sure that you have performed a backup before they complete their tasks. The Windows SBS Console also has a Backup And Server Storage page, as shown in Figure 12-1, which you can use to create and modify a backup job.


Windows Small Business Server 2011 Standard Console
Home
Users and Groups
Network
Shared Folders and Web Sites
Backup and Server Storage
Reports
Security
Windows Small Business Server 2011 Standard
Help
Backup
Server Storage
Tasks
Backup Tasks
Configure server backup
How do I restore server data from a backup?
Restore server data from backup
Tell me more about server backup
Refresh this view
1 item

Name	Last Backup	Status	Next Backup
SBS1	Not configured	Not configured	Not scheduled

Select an object in the list, to view tasks and details associated with that object.

FIGURE 12-1 The Backup And Server Storage page in the Windows SBS Console.

The backup interface in the Windows SBS Console provides access to some of the features of the Windows Server Backup program, but not all of them. Designing a backup job consists of the following tasks:

- **Select a backup medium** What device will store the backups?
- **Select backup targets** What data will be backed up?
- **Create a backup schedule** When will the backups occur?
- **Select backup software** What program will you use to perform backups?

The console's backup controls enable you to create and manage a scheduled backup job that copies the entire system volume, and selected other volumes, to an external hard drive connected to the server at a time you specify. The result is basic disaster control, enabling you to restore entire volumes lost due to drive failure or loss of an entire computer.

Although Windows SBS 2011 includes a backup software program, Windows Server Backup is relatively limited in its capabilities. Depending on your needs, you might want to consider using a third-party software product as part of your backup solution.

The following sections examine the factors listed earlier in more detail. You should consider these factors when planning a network backup strategy. If, however, the default backup scenario just described sounds perfect for you, you can skip to "Configuring Server Backups," later in this chapter.

Selecting a Backup Medium

A *backup* is simply a copy of your data saved to another storage medium. Any medium can provide protection again data loss due to a hard drive failure, but to protect against fire, theft, and other disasters, a removable backup medium that you can store offsite is preferable. The traditional network backup medium is magnetic tape, but external hard drives and USB flash drives are increasingly popular solutions.

There are three factors to consider when evaluating the suitability of a storage medium for use as a backup device:

- **Storage capacity** The ideal capacity for a backup medium is large enough to hold an entire backup job without having to change media. This enables you to run your backup jobs unattended, preferably at night or during other offline hours. This usually rules out DVDs and other optical disks. Magnetic tape drives are available with capacities of more than 3 terabytes (TB), or 3,000 gigabytes (GB), but they can be extremely expensive. Inexpensive, external hard disk drives are available in sizes up to 3 TB, and are increasing in capacity at a rapid pace.
- **Data transfer speed** The speed of your backup device might or might not be a major issue, depending on how much data you have to back up and how much time you have available to perform your backups. Hard disk drives are generally the fastest backup solution. There are high-speed magnetic tape drives available, but again their prices can be prohibitive for small business use.
- **Hardware cost** Price is always a consideration. As a general rule, the price of high-performance magnetic tape equipment goes steadily up as capacity and performance levels increase, while the price of hard disk storage has been going steadily down for years. Prices for high-end tape drives can easily run into five figures (in U.S. dollars), plus you must consider the price of the tape cartridges themselves, while external hard drives are available for as little as US $100 per terabyte.

If you plan to use the Windows Server Backup software included with Windows SBS 2011, selecting a backup medium is less of a problem. The Configure Server Backup Wizard in the Windows SBS Console supports only external hard drives. You can use the Windows Server Backup Console to perform interactive backups to writable optical disks or to network shares, but the software includes no support for magnetic tape drives.

Using External Hard Disk Drives

In addition to the standard hard disk drive unit, identical to the ones you install inside your computers, an external hard disk consists only of a case, a power supply, and an interface to your computer. You can remove the hard disk from the case and install it in a computer if you want to. You can also purchase an empty external drive housing and install a hard disk drive you already own into it. External hard disk drives make excellent backup solutions. They are inexpensive, fast, hold a lot of data, and disconnect easily from the computer.

External hard drives have been available for many years, but until recently, they were Small Computer System Interface (SCSI) drives that required a special host adapter in the computer and an expensive cable. Today, there are three external interfaces that are suitably fast for hard disk connections. They are listed in Table 12-1.

TABLE 12-1 External Hard Drive Interface Specifications

INTERFACE	OTHER NAMES	BANDWIDTH (MB/SEC)	MAXIMUM CABLE LENGTH (METERS)
Universal Serial Bus 2.0	USB 2.0	480	5
Universal Serial Bus 3.0	USB 3.0	5,000	3
IEEE 1394a	FireWire 400, i.LINK, Lynx	400	4.5
IEEE 1394b	FireWire 800	800	100
External Serial Advanced Technology Attachment	eSATA 300	3000	2

Virtually all the PCs on the market today include USB ports, and many have some combination of eSATA and IEEE 1394 ports as well. Computers with ports on the front of the case are particularly attractive for backup devices, so that you can remove them easily. All these interfaces support hot swapping, which enables you to attach and detach devices without powering down the computer.

Nearly all the external hard drives on the market support USB, and most have at least one additional interface, such as eSATA, IEEE 1394b, or IEEE 1394a. Some products include support for all of the interfaces. Most external hard drive products use Serial AT Attachment (SATA) hard drives, with a bridge circuit that enables them to connect to a USB or IEEE 1394 interface. The eSATA interface eliminates the need for the bridge, which can enable certain advanced drive technologies to function as in an internal installation, and provides a far faster transfer rate. Cable length for eSATA devices is limited to 2 meters, however.

Although the USB 2.0 specification indicates a better level of performance than IEEE 1394a, IEEE 1394a devices tend to outperform USB 2.0 ones in real-world implementations, but only marginally. IEEE 1394b is decidedly faster than USB 2.0, but eSATA can provide substantially better performance than either. However, USB 2.0 and IEEE 1394a are both adequate backup solutions for most situations. If your server has an integrated eSATA port, you would be well to use it, but unless you have a need for the fastest possible interface, an integrated USB or IEEE 1394 connection is likely to be a more reliable and economical solution than an after-market eSATA card.

Most external hard drives have their own power supplies, but there are a few models that draw power from the USB or IEEE 1394 interface. These latter devices are generally designed as portable solutions for notebook computers. For server backups, an independent power supply is preferable. Apart from these factors, the only other specifications to consider are those of the hard drive itself. More RPMs and a larger cache are certainly preferable for a backup solution, but they can add to the cost of the unit.

Using Magnetic Tape Drives

Magnetic tape has long been the industry standard backup medium. Tape capacities and transfer speeds have kept pace with hard disk characteristics over the years; they can store data for years, and the media cost per gigabyte of storage is relatively low. With magnetic tape, because the storage medium is separate from the drive mechanism, there is far less that can go wrong. If you drop a tape cartridge on the floor, it is probably still usable; not so with a hard disk drive, in many cases.

Magnetic tape drives are different from the other types of storage media that computers use, in that they are not random access devices. You cannot immediately access any file on a tape by moving the drive heads to a specific location or by accessing a specific memory address, as you can with other media. With magnetic tape, the drive must spool through the reel of tape until it locates the desired file, a process that can take several minutes.

Because of this, you cannot use a magnetic tape drive for anything other than backups. You can’t mount a tape as a volume and assign it a drive letter, as you can with other media. Instead, computers use a special software driver to address the tape drive and send data to it. When you purchase a backup software product that supports magnetic tape, you must make sure that it supports the specific magnetic tape drive you plan to use.

There are a variety of magnetic tape drive technologies available, with varying tape capacities, transfer speeds, and prices. At one time, there were relatively low-cost tape systems on the market, intended for backups of standalone computers and small networks. However, they have been made almost entirely obsolete by writable optical disks, flash drives, and external hard drives. Today, the magnetic tape drive market is concentrated on high-end network backup solutions, using technologies such as Digital Linear Tape (DLT), Linear Tape-Open (LTO) Ultrium, Advanced Intelligent Tape (AIT), and Digital Data Storage/Digital Audio Tape (DDS/DAT).

In addition, complex hardware devices called *autoloaders* can be as large as household refrigerators and house multiple tape drives and dozens of tape cartridges. These devices can provide fully automated backup solutions for enormous amounts of data.

The question then is whether a modest magnetic tape solution is suitable for a small business network. In most cases, the answer is no. The combination of a magnetic tape drive and its required software provide far more capability than Windows Server Backup and an external hard drive, but with prices that start at US $1,000 and climb steeply into the stratosphere, most small business owners find the cost to be prohibitive.

Using a Redundant Medium

As mentioned earlier, one of the requirements for full backup protection is a removable storage medium that you can take offsite to protect against fire, theft, and other disasters. If you use magnetic tape, this is easy. Most tape backup software packages implement a tape rotation scheme that makes copies of your data to store offsite.

> ***NOTE*** ***Offsite storage* of a backup medium can refer to anything from a safe deposit box in a bank vault to a fireproof cabinet in the owner's home, to the glove compartment of the IT manager's car. Obviously, a location that protects against theft and environmental damage is the preferable solution.**

With external hard drives, storing data offsite means removing the entire device, not just the storage medium. Fortunately, the devices are not so expensive that it is impractical to purchase more than one, and Windows Server Backup provides the ability to perform simultaneous backups to multiple devices. Therefore, if you plan to use external hard drives for your backup medium, you should purchase at least two, so that you can create two copies of your data and store one offsite. For organizations that require a permanent archive of their data, you might want to purchase a new backup drive each month, perform an additional backup job, and store those monthly drives offsite.

Using Online Backup

Online backup—sometimes called *remote backup* or *managed backup*—is a third-party service that enables an organization to back up its data to a remote site over the Internet. These services typically can provide many or all of the same features as a high-end backup software product, with the additional advantage that the consumer is not responsible for the purchase and maintenance of the backup hardware.

Online backup services provide many additional advantages over onsite solutions, including the following:

- Data is stored offsite without the need for administrators to manage backup media or transport devices to a storage facility.
- Backup jobs can run completely unattended.
- Storage capacity is virtually unlimited.
- Backup speed is limited only by the speed of your Internet connection.
- Data can be encrypted prior to storage.

There are potential disadvantages to online backup solutions as well, including the following:

- Many broadband Internet connections are asymmetrical, meaning that their upstream speeds are slower than their downstream speeds. A connection that provides adequate downstream bandwidth might not provide sufficient upstream bandwidth to support backup traffic.
- Data restoration might require special handling from the service provider and might be considerably slower than restoring from your own backup media.
- A service provider could go out of business or suffer their own data loss, affecting the availability of your backups.
- Data security is not guaranteed unless you take steps to encrypt it before it leaves your site.
- Online backup is an ongoing expense that never goes away and is likely to increase over time.

Online backup can provide any service that a standalone backup software package can. The customer typically configures the backup jobs using a website interface that functions very much like the application supplied with a backup software product.

Selecting Backup Targets

A *backup target* is a file, folder, or volume that you select to be copied to your backup device. Two of the most critical questions you should consider when devising a backup strategy are these:

- How much data is there to back up?
- Where is the data stored?

The amount of data you have to back up dictates how long your backup jobs take and what the capacity of your backup medium has to be. The location of the data to be backed up dictates the type of backup software you need.

Windows Server Backup is capable of backing up only the volumes on the computer running the program. When you create a backup job on your server using the Configure Server Backup Wizard, you must back up the entire system volume, and you can select any or all of the other volumes on the computer as well. For the wizard to create the job, your external hard drive must have sufficient storage space to accommodate all the data on the volumes you select.

BEST PRACTICES **To accommodate the future growth of your data, Microsoft recommends that you use an external hard drive with 2.5 times the capacity of the data you plan to back up.**

Unlike most third-party backup software products, Windows Server Backup can back up only entire volumes. If you want to select targets by choosing individual files and folders, you must use a third-party software product. Windows Server Backup is also unable to back up data stored on other computers. Third-party network backup solutions enable you to select targets from any computer on the network and back them up to a device connected to your server.

NOTE **Although Windows Server Backup can back up only entire volumes, you can restore individual files and folders from a backup.**

Network administrators often configure their client workstations to store all data files on a server rather than a local drive. One of the main reasons for this is to facilitate backups. If you plan to use Windows Server Backup on your primary Windows SBS server, you should arrange to store all your network data on that server. This means redirecting all critical folders from your client workstations to a server volume so that there is no need to back up the local drives on your workstations.

Creating a Backup Schedule

Another important question you should ask when planning your backup strategy is when the backups should occur. Most administrators schedule backups to run when the network is not in use, such as when the organization is closed. This is because many backup software programs are unable to back up files that are open or currently in use.

Windows Server Backup schedules its jobs by adding them to the Task Scheduler application in Windows. Some third-party backup software products do this as well, while others have their own schedulers, which typically run as a service, triggering jobs at the times you specify.

The object of scheduling backups is to simplify the administrator's daily role in the process as much as possible. Once you have created and scheduled your backup jobs, all you have to do is see to it that the correct medium is available each day. For magnetic tape users, this means swapping the tapes in the drive on a daily basis, while external hard drive users have to reconnect their offsite drives.

Selecting Backup Software

Although Windows SBS 2011 includes a backup software program, it has relatively limited capabilities. As part of your backup strategy planning process, you should consider whether you need any features that Windows Server Backup lacks. If you do, look for a backup software product that does provide them.

Using Windows Server Backup

The Windows operating systems have long included a backup software program, but Windows Server Backup, the program included with Windows SBS 2011 and 2008, is different from the previous Windows backup utilities in many ways. Chief among these differences is the fact that Windows Server Backup uses a different format for the backup files it creates. Therefore, you cannot use the Windows Server Backup program in Windows SBS 2011 to restore files you created with the Windows Server 2003 NTBackup utility.

> ***TIP*** **If you need to restore files you backed up with the NTBackup utility from a previous version of Windows, Microsoft offers a restore-only version of NTBackup. You can download it for free at *http://go.microsoft.com/FWLink/?Linkid=82917*.**

Some of the other differences between Windows Server Backup and previous Windows backup utilities are as follows:

- **Backup media** Windows Server Backup is designed primarily to perform backups to external hard drives. The program does not include any support for magnetic tape drives, and can back up to optical disks and network shares only during interactive jobs, not scheduled ones.
- **Volume formatting** When you select an external hard drive volume as your backup medium, Windows Server Backup reformats the volume (destroying any data it finds there) and dedicates it exclusively to backup use. After the reformat, the volume no longer has a drive letter and no longer appears in Windows Explorer.

- **System volume backup** When you create a backup job through the Windows SBS Console, Windows Server Backup always backs up the entire system volume, including the boot files, the registry, the Active Directory Domain Services (AD DS) database, and other system resources that do not appear as files in Windows Explorer.
- **Target selection** Windows Server Backup creates block-based images of your volumes and therefore can back up only entire volumes. You cannot include or exclude individual files or folders, as you can with file-based backup software products.
- **Job scheduling** Windows Server Backup can schedule only one backup job, which you can configure to run once or several times per day.
- **Job types** Windows Server Backup does not enable you to create incremental, differential, and full backup jobs on a per-job basis. The scheduled job you create with the Configure Server Backup Wizard performs incremental backups by default, to save space on the backup drive, but it does so in a way that is different from traditional backup software products.

  MORE INFO **For more information on the incremental backup mechanism in Windows Server Backup, see the section entitled "Configuring Performance Settings," later in this chapter.**

- **Backup format** Windows Server Backup creates image-based backup files using the Microsoft virtual hard disk (VHD) format. This enables you to open the files in a virtual machine, using the Hyper-V server role included in Windows Server 2011.
- **Application support** Windows Server Backup is capable of backing up and restoring both your Exchange Server message stores and your SharePoint Foundation database. The program automatically stops the required services before backing up these applications and automatically restarts them afterward.

Using Third-Party Backup Software

There are two basic classes for backup software products: those that are intended for standalone computers and those intended for network use. The main difference between the two is the ability to use one computer as a backup server that can back up data from other computers on the network. For a single-server, small business network, it might not be worth the additional time and expenses required to purchase and deploy a full-featured network backup product. If you configure your workstations to store all their data files on a single Windows SBS server, you can simply back up that one computer with a standalone product. If you have to back up other servers or workstation drives, however, a network backup software product is usually preferable.

Some of the features that differentiate third-party network backup software products from Windows Server Backup are the following:

- **Backup media** Third-party backup products typically provide support for a wider variety of backup media, including magnetic tape drives, tape autoloaders, and optical jukeboxes. Because a software product that supports devices like these must include hardware-specific drivers, be sure that the product you select supports the device(s) you plan to purchase.
- **Target selection** Third-party backup software products usually allow you to select backup targets using a tree display similar to that of the *Network* node in Windows Explorer. This enables you to create backup jobs that include or exclude specific files, folders, or volumes on any network computer.

  NOTE **The selection of targets in a network backup product is usually keyed into the product's software architecture and its licensing. For example, to back up additional servers and workstations over the network from a server equipped with a tape drive, you must purchase licenses for the remote computers and install software agents on them that enable them to communicate with the backup server.**

- **Job scheduling** Third-party backup software products enable you to create as many interactive or scheduled backup jobs as you need. Scheduling capabilities typically let you create jobs that run on a daily, weekly, or monthly basis.
- **Job types** Most third-party backup software products support incremental and differential backup jobs as well as full backups. Incremental and differential jobs enable you to back up only the data that has changed since the last backup. This complicates the restore process somewhat, but saves space on the backup medium and executes backups in far less time than full backup jobs.

  NOTE **In a traditional backup software package, a *differential backup* is a job that backs up only the files that have changed since the last full backup. To perform a full restore from differentials, you must restore the most recent full backup and then the most recent differential backup. An *incremental backup* is a job that backs up only the files that have changed since the last incremental backup. To perform a full restore from incrementals, you must restore the most recent full backup and then restore each of the incrementals you performed since that full backup in the order you performed them.**

- **Cataloging backups** Most third-party backup software products use a database to maintain a catalog of the jobs they perform and the files they save to the backup media. If you use magnetic tape, for example, the catalog enables you to search for a specific version of a specific file and easily locate the exact tape containing that file.

- **Media rotation** Third-party backup software products that support magnetic tape drives can usually implement a media rotation scheme that corresponds to your schedule of backup jobs. A media rotation scheme specifies the name you should use to label each tape and tells you which tape to insert in the drive for each daily job. This enables you to keep track of your tape usage and simplifies the daily administration of your backup regimen.
- **Application support** Many third-party backup software manufacturers produce add-on modules (at extra cost) that enable their products to back up network applications and services, such as mail servers and databases, while they are running. This prevents you from having to shut down critical services to back them up.

  NOTE **It is generally not possible to back up files that are locked open or in use. This is particularly true for email stores and databases. There are various techniques that backup applications use to protect these resources, such as temporary closure of the application or the use of delta files that contain changes made to the resource while the backup is taking place. Some network backup products implement these techniques as separate add-ons that you must purchase at additional cost.**

- **Restoring data** Third-party backup software products that enable you to select individual files and folders as backup targets also enable you to restore selected files or folders. This way, you can also use your backups to protect individual files against accidental damage or deletion.

Some of these capabilities are far more than the typical small business network needs, but for organizations with special security requirements, they can provide extra protection.

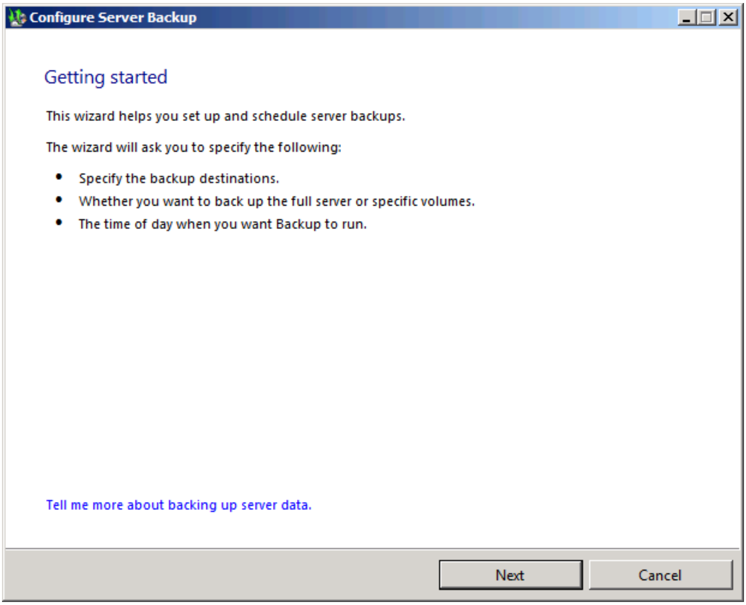
Configuring Server Backups

The Windows SBS Console simplifies the creation of scheduled backup jobs by supplying a wizard that steps you through the process. Once you have created the job, the console provides controls that enable you to modify its properties. Windows SBS 2011 also includes the Windows Server Backup Console, which provides more comprehensive control over the backup process and provides the means to restore data from a backup medium.

Creating a Scheduled Backup Job

To create a scheduled backup job with the Windows SBS Console, use the following procedure:

1. Connect your external hard drive to the computer by plugging it into a USB, IEEE 1394, or eSATA port.
2. Log on to your Windows SBS 2011 server using a domain account with administrative privileges. The Windows SBS Console appears.
3. Click *Backup and server storage*, and then select the *Backup* tab.
4. In the *Tasks* list, click *Configure server backup*. The Configure Server Backup Wizard appears.



Configure Server Backup

Getting started

This wizard helps you set up and schedule server backups.

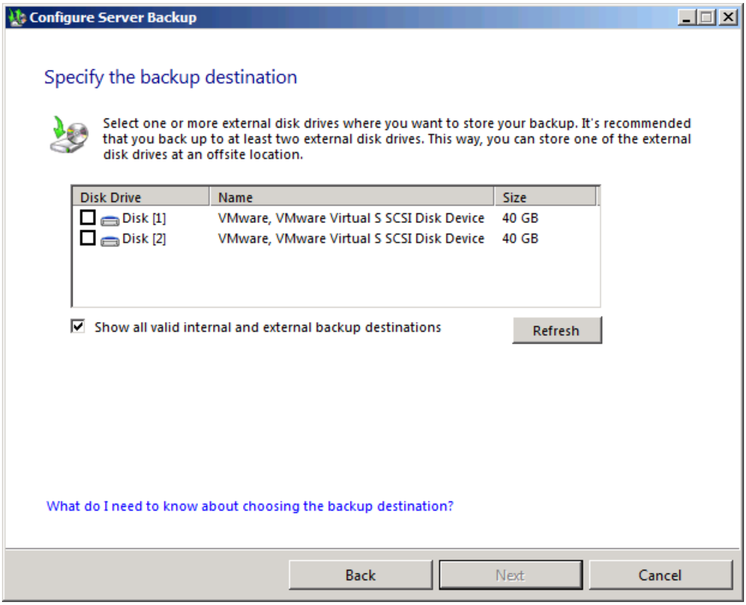
The wizard will ask you to specify the following:

- Specify the backup destinations.
- Whether you want to back up the full server or specific volumes.
- The time of day when you want Backup to run.

Tell me more about backing up server data.

TIP **Alternatively, you can start the Configure Server Backup Wizard by clicking *Configure server backup* in the *Getting started tasks* list in the Windows SBS Console.**

5. Click *Next* to bypass the Getting Started page. The Specify The Backup Destination page appears.



Configure Server Backup

Specify the backup destination

Select one or more external disk drives where you want to store your backup. It's recommended that you back up to at least two external disk drives. This way, you can store one of the external disk drives at an offsite location.

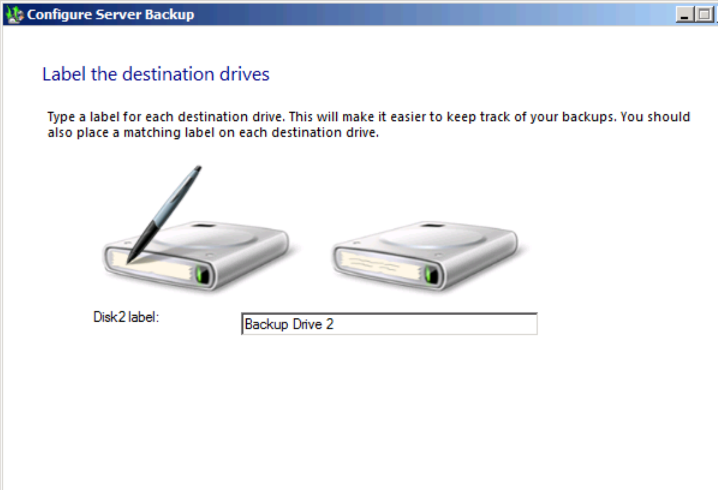
Disk Drive	Name	Size
□ Disk [1]	VMware, VMware Virtual S SCSI Disk Device	40 GB
□ Disk [2]	VMware, VMware Virtual S SCSI Disk Device	40 GB

☑ Show all valid internal and external backup destinations

Refresh
What do I need to know about choosing the backup destination?
Back
Next
Cancel

NOTE **By selecting the *Show all valid internal and external backup destinations* check box, you display the internal disks that are available for use as backup drives, as well as the external ones. Obviously, internal drives are more difficult to store offsite, but they can still be a functional part of your backup strategy.**

6. Select the check box(es) for the disk(s) you want to use as your backup drives and click *Next*. The Label The Destination Drives page appears.



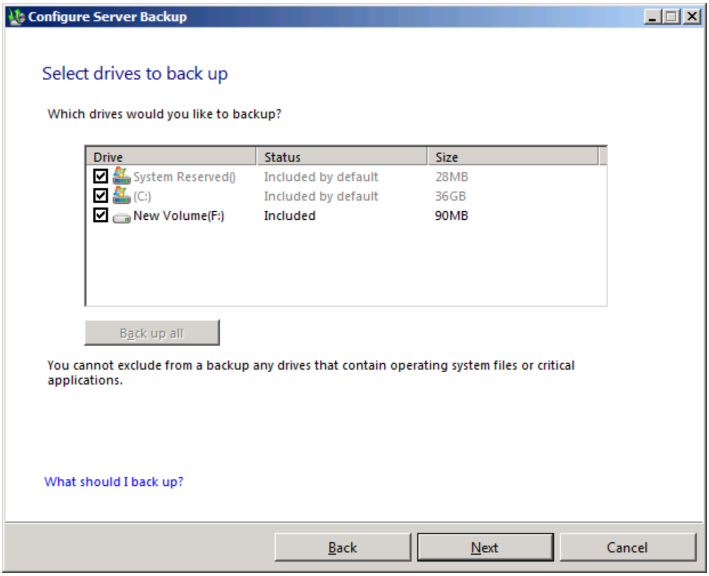
Configure Server Backup

Label the destination drives

Type a label for each destination drive. This will make it easier to keep track of your backups. You should also place a matching label on each destination drive.

Disk2 label: Backup Drive 2

7. Specify an alternative label for each drive, if desired, in the text box provided and click *Next*. The Select Drives To Back Up page appears.



Select drives to back up

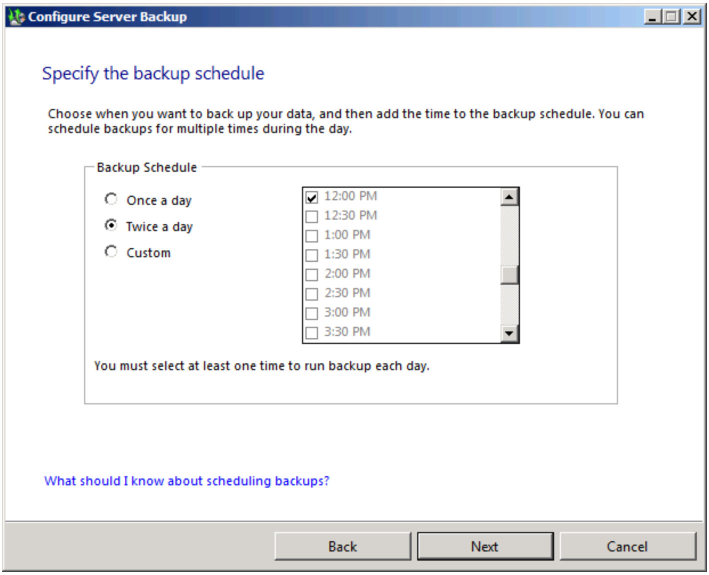
Which drives would you like to backup?

Drive	Status	Size
☑ System Reserved()	Included by default	28MB
☑ (C:)	Included by default	36GB
☑ New Volume(F:)	Included	90MB

You cannot exclude from a backup any drives that contain operating system files or critical applications.

What should I back up?

8. In addition to the default C drive, select the check boxes for any other volumes you want to include in the backup job and click *Next*. The Specify The Backup Schedule page appears.



Specify the backup schedule

Choose when you want to back up your data, and then add the time to the backup schedule. You can schedule backups for multiple times during the day.

Backup Schedule

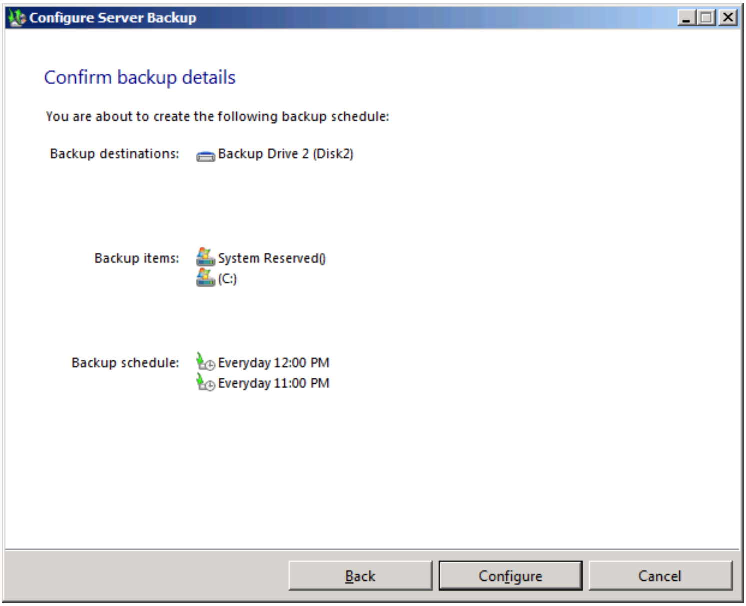
○ Once a day
● Twice a day
○ Custom

☑ 12:00 PM
□ 12:30 PM
□ 1:00 PM
□ 1:30 PM
□ 2:00 PM
□ 2:30 PM
□ 3:00 PM
□ 3:30 PM

You must select at least one time to run backup each day.

What should I know about scheduling backups?

9. Select one of the following scheduling options:
   - **Once a day** The backup occurs once daily at 11:00 P.M.
   - **Twice a day** The backup occurs twice daily at 12:00 P.M. and 11:00 P.M.
   - **Custom** The backup occurs as many times as you wish each day, at the times you select
10. Click *Next*. The Confirm Backup Details page appears.



Configure Server Backup

Confirm backup details

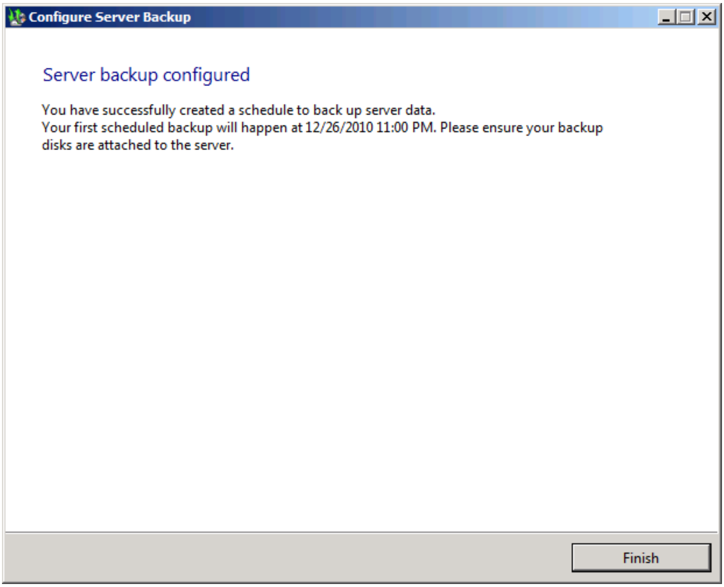
You are about to create the following backup schedule:

Backup destinations: Backup Drive 2 (Disk2)

Backup items: System Reserved()
(C:)

Backup schedule: Everyday 12:00 PM
Everyday 11:00 PM

11. Click *Configure*. A Configure Server Backup message box appears, warning you that the wizard is about to format the drives you selected as the backup destination.
12. Click *Yes*. The wizard prepares the backup drive, configures the backup job, and displays the Server Backup Configured page.

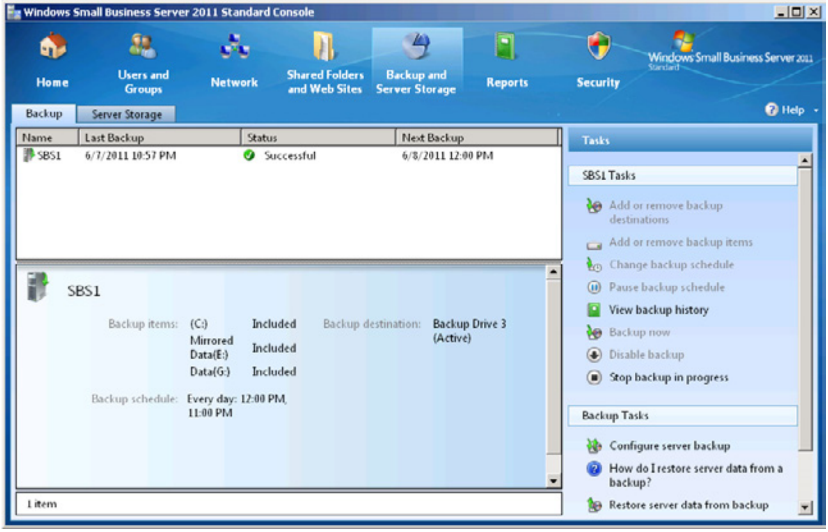


Server backup configured

You have successfully created a schedule to back up server data.
Your first scheduled backup will happen at 12/26/2010 11:00 PM. Please ensure your backup disks are attached to the server.

13. Click *Finish*. The wizard closes and the job appears on the *Backup* tab.

When the scheduled time for the backup arrives, the Task Scheduler application starts the job, which runs in the background as the server continues to function normally. When the backup finishes, its status appears in the console as *Successful*, as shown in Figure 12-2.


Windows Small Business Server 2011 Standard Console
Home
Users and Groups
Network
Shared Folders and Web Sites
Backup and Server Storage
Reports
Security
Windows Small Business Server 2011 Standard
Backup
Server Storage
Help
Tasks
SBS1 Tasks
Add or remove backup destinations
Add or remove backup items
Change backup schedule
Pause backup schedule
View backup history
Backup now
Disable backup
Stop backup in progress
Backup Tasks
Configure server backup
How do I restore server data from a backup?
Restore server data from backup

Name	Last Backup	Status	Next Backup
SBS1	6/7/2011 10:57 PM	Successful	6/8/2011 12:00 PM

SBS1

Backup items: (C:) Included; Mirrored Data(E:) Included; Data(G:) Included

Backup destination: Backup Drive 3 (Active)

Backup schedule: Every day: 12:00 PM, 11:00 PM

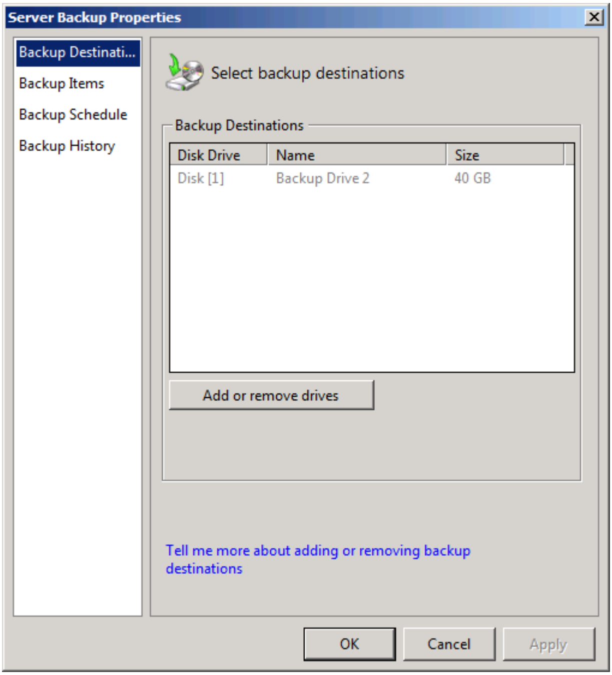
1 item

FIGURE 12-2 A successful backup job, as displayed in the Windows SBS Console.

Modifying a Backup Job

Once you have created a backup job using the Configure Server Backup Wizard, the *Tasks* list on the Backup And Server Storage page provides controls that enable you to modify the parameters of the job as needed. Click one of the following tasks listed to open the corresponding tab in the Server Backup Properties sheet, as follows:

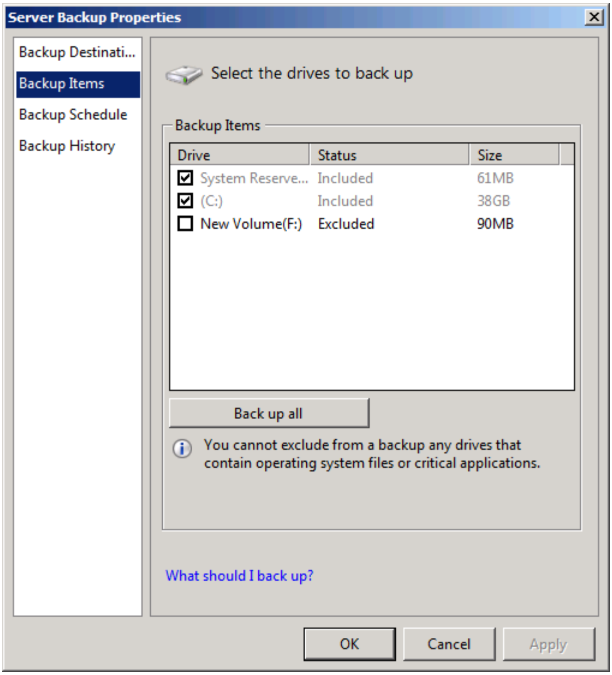
- **Add or remove backup destinations** Enables you to specify the devices you want to use to perform backups.



Disk Drive	Name	Size
Disk [1]	Backup Drive 2	40 GB

Tell me more about adding or removing backup destinations

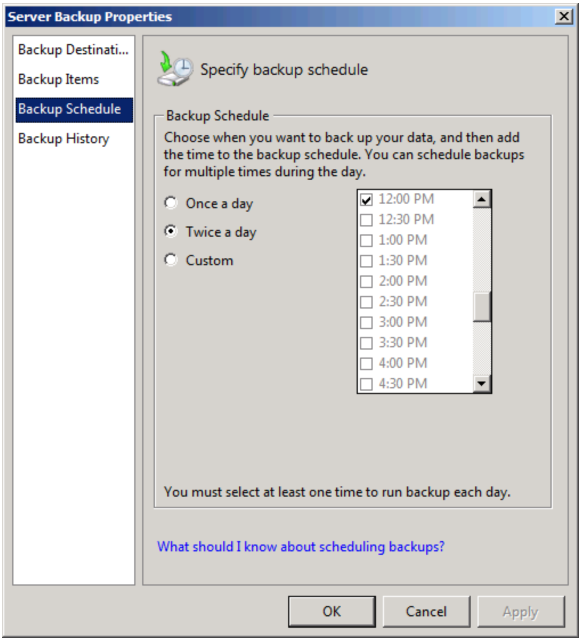
- **Add or remove backup items** Enables you to specify the targets for your backups.



Drive	Status	Size
☑ System Reserve...	Included	61MB
☑ (C:)	Included	38GB
□ New Volume(F:)	Excluded	90MB

You cannot exclude from a backup any drives that contain operating system files or critical applications.

- **Change backup schedule** Enables you to modify the times at which the backup jobs should occur.



Server Backup Properties

Specify backup schedule

Backup Schedule

Choose when you want to back up your data, and then add the time to the backup schedule. You can schedule backups for multiple times during the day.

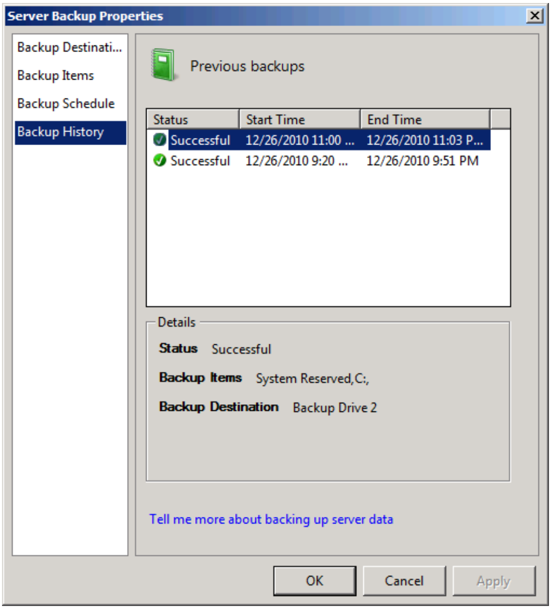
○ Once a day
● Twice a day
○ Custom

☑ 12:00 PM
□ 12:30 PM
□ 1:00 PM
□ 1:30 PM
□ 2:00 PM
□ 2:30 PM
□ 3:00 PM
□ 3:30 PM
□ 4:00 PM
□ 4:30 PM

You must select at least one time to run backup each day.

What should I know about scheduling backups?

- **View backup history** Displays a full record of all previous backups the system has performed.



Server Backup Properties

Previous backups

Status	Start Time	End Time
Successful	12/26/2010 11:00 ...	12/26/2010 11:03 P...
Successful	12/26/2010 9:20 ...	12/26/2010 9:51 PM

Details

Status Successful

Backup Items System Reserved,C:,

Backup Destination Backup Drive 2

Tell me more about backing up server data

You can also use the items in the tasks list to pause the backup schedule, disable the backup job entirely, or start a backup immediately, regardless of the schedule.

Creating a Backup Administrator Role

Once you have devised a backup strategy and created a scheduled backup job, the hard part of the process is over. What remains are the mundane tasks of swapping out backup media and checking to make sure that the backup job completes successfully each day. Network administrators often delegate these tasks to other users, and not necessarily to users to whom they want to grant full administrative privileges. Fortunately, Windows SBS 2011 includes a built-in group called Backup Operators, which provides the rights and permissions a user needs to manage backup jobs, and no more.

Backup Operators is not a Windows SBS group, so you cannot use the Windows SBS Console to add an existing user account to the group. However, you can create a user role that includes the group membership and then create user accounts based on that role. Alternatively, you can use the Active Directory Users And Computers Console to add an existing user to the Backup Operators group.

> ***MORE INFO*** **To create the user role, follow the procedure in the section entitled "Creating a New User Role" in Chapter 6, "Working with Users, Computers, and Groups." Base your new role on the Network Administrator role and, on the Choose User Role Permissions (Group Membership) page, remove all the default groups and add the Backup Operators group.**

Backing Up a Second Server

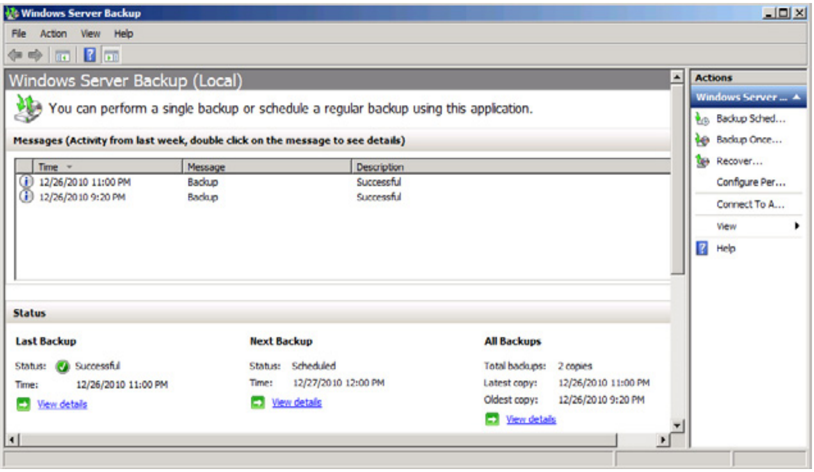
As mentioned earlier, Windows Server Backup is capable of backing up only volumes on the computer running the program. If you have purchased the Windows SBS 2011 Premium Add-on product and installed a second server on your network, you cannot back up your secondary server using the Windows Server Backup program and the backup medium on your primary server. However, your second server has its own copy of Windows Server Backup, which leaves you with two possible ways to facilitate the backup process:

- Connect a separate set of backup drives to the secondary server and create a separate, independent backup job on that server.
- Create a shared folder on your primary server and configure your secondary server to back itself up to the network share. Then use your backup media on the primary server to back up the shared folder.

Windows Server Backup is a feature that your primary Windows SBS 2011 server installs by default. However, you must install the feature yourself on your secondary server by using the Server Manager Console.

Using the Windows Server Backup Console

You can create and modify backup jobs using the Windows SBS Console, but when you click *Restore server data from backup* in the *Tasks* list, the console opens a Windows Server Backup Console window, as shown in Figure 12-3. You can also use this console to monitor backup activity, configure backup performance settings, and perform single backups with different parameters from your scheduled backup job.



Windows Server Backup (Local)

You can perform a single backup or schedule a regular backup using this application.

Messages (Activity from last week, double click on the message to see details)

Time	Message	Description
12/26/2010 11:00 PM	Backup	Successful
12/26/2010 9:20 PM	Backup	Successful

Status

Last Backup
Status: Successful
Time: 12/26/2010 11:00 PM
View details

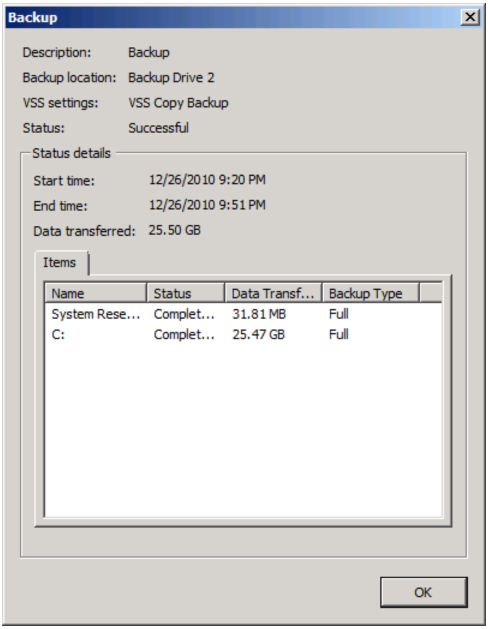
Next Backup
Status: Scheduled
Time: 12/27/2010 12:00 PM
View details

All Backups
Total backups: 2 copies
Latest copy: 12/26/2010 11:00 PM
Oldest copy: 12/26/2010 9:20 PM
View details

FIGURE 12-3 The Windows Server Backup Console.

When you open the Windows Server Backup Console, whether from the Windows SBS Console or from the Administrative Tools program group, you see a display divided into the following sections:

- **Messages** Displays a list of event messages providing detailed results of each backup the system has performed.



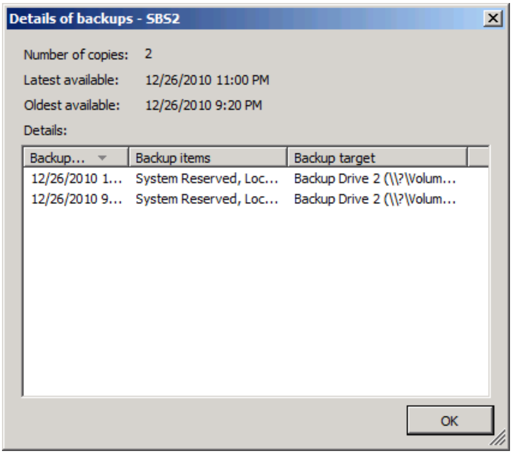
Description: Backup
Backup location: Backup Drive 2
VSS settings: VSS Copy Backup
Status: Successful

Status details

Start time: 12/26/2010 9:20 PM
End time: 12/26/2010 9:51 PM
Data transferred: 25.50 GB

Name	Status	Data Transf...	Backup Type
System Rese...	Complet...	31.81 MB	Full
C:	Complet...	25.47 GB	Full

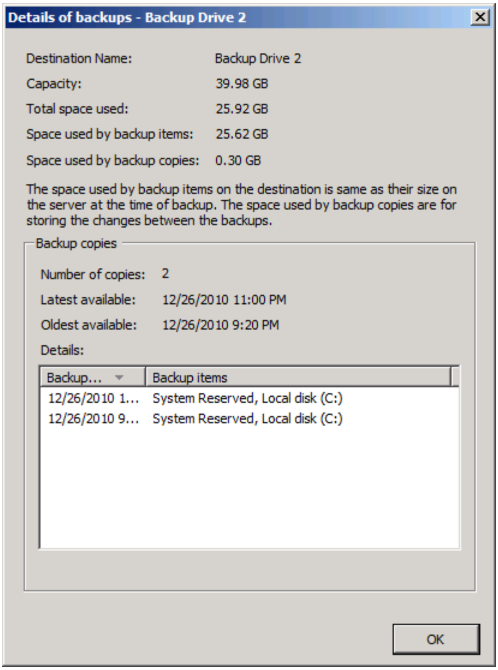
- **Status** Displays the results of the most recent backup, the scheduled time of the next backup, and a summary of all the backups available for restoration.



Number of copies: 2
Latest available: 12/26/2010 11:00 PM
Oldest available: 12/26/2010 9:20 PM
Details:

Backup...	Backup items	Backup target
12/26/2010 1...	System Reserved, Loc...	Backup Drive 2 (\\?\Volum...
12/26/2010 9...	System Reserved, Loc...	Backup Drive 2 (\\?\Volum...

- **Scheduled backup (below the Status section, not visible in the figure)** Displays the settings for the next scheduled backup and disk usage information for the backup medium.



Details of backups - Backup Drive 2

Destination Name:	Backup Drive 2
Capacity:	39.98 GB
Total space used:	25.92 GB
Space used by backup items:	25.62 GB
Space used by backup copies:	0.30 GB

The space used by backup items on the destination is same as their size on the server at the time of backup. The space used by backup copies are for storing the changes between the backups.

Backup copies

Number of copies:	2
Latest available:	12/26/2010 11:00 PM
Oldest available:	12/26/2010 9:20 PM

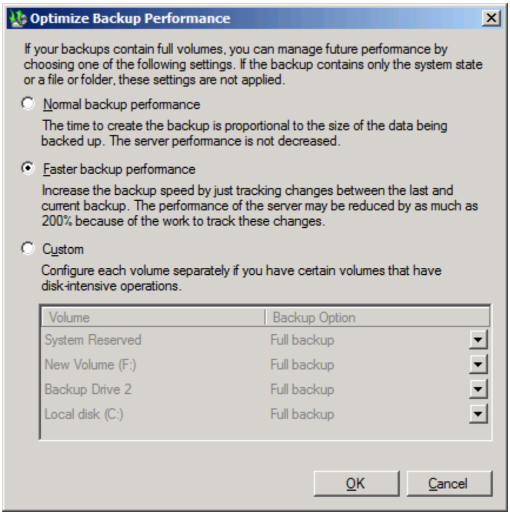
Details:

Backup...	Backup items
12/26/2010 1...	System Reserved, Local disk (C:)
12/26/2010 9...	System Reserved, Local disk (C:)

In addition to viewing information about the system's backup activities, you can perform additional tasks, as described in the following sections.

Configuring Performance Settings

When you click *Configure performance settings* in the Action pane of the Windows Server Backup Console, the Optimize Backup Performance dialog box appears, as shown in Figure 12-4. This dialog box enables you to specify whether Windows Server Backup should perform incremental backups.



Optimize Backup Performance

If your backups contain full volumes, you can manage future performance by choosing one of the following settings. If the backup contains only the system state or a file or folder, these settings are not applied.

○ Normal backup performance

The time to create the backup is proportional to the size of the data being backed up. The server performance is not decreased.

● Faster backup performance

Increase the backup speed by just tracking changes between the last and current backup. The performance of the server may be reduced by as much as 200% because of the work to track these changes.

○ Custom

Configure each volume separately if you have certain volumes that have disk-intensive operations.

Volume	Backup Option
System Reserved	Full backup
New Volume (F:)	Full backup
Backup Drive 2	Full backup
Local disk (C:)	Full backup

FIGURE 12-4 The Optimize Backup Performance dialog box.

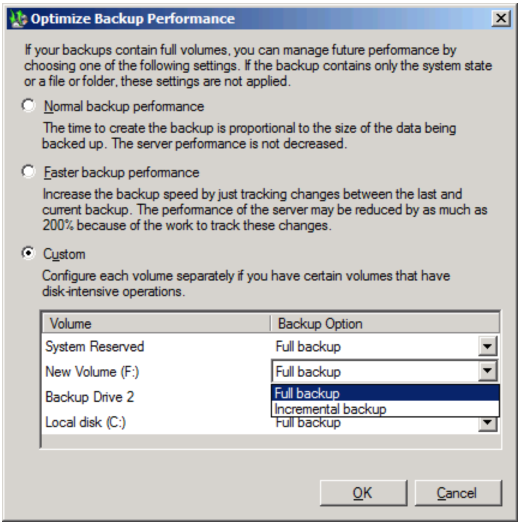
Traditional backup software products are designed for use with magnetic tape drives. Incremental and differential backups save storage space by copying only the files that have changed since the last backup. Each job, however, uses a separate tape, and to fully recover a lost volume you must perform multiple restores from different tapes: first the most recent full backup and then one or more of the incremental or differential tapes you have made since that full backup.

When Windows Server Backup performs incremental backups, it takes advantage of the hard disk's random access capabilities and updates the full backup on the disk by replacing the files that have changed since the last backup. The software then saves the previous versions of those changed files to another location on the disk, along with metadata that indicates its original location and when the system backed it up.

As a result of using incrementals, the backup drive always contains a full backup image that represents the most recent version of the target volumes. If you perform a restore and select the most recent version of a volume, the program simply accesses that full backup image. If you restore an earlier version of a volume, the software accesses the displaced files and integrates them into the full backup image to create a replica of the volume as it existed at the time that the system performed the earlier backup.

By default, the Optimize Backup Performance dialog box has the *Faster backup performance* option selected, which triggers the use of incrementals. By saving only the files that have changed, incremental backups not only save space on the backup disk; they also finish much faster. If you select the *Normal backup performance* option instead, Windows Server Backup creates a full image of the selected volumes during each backup, consuming more storage space and taking more time to complete.

You can also select the *Custom* option to specify different settings for each of the volumes in your backup job. This is the only place where you can explicitly choose between full and incremental backup jobs, as shown in Figure 12-5. However, in most cases, there is no compelling reason to perform a full backup each time a job runs.



Optimize Backup Performance

If your backups contain full volumes, you can manage future performance by choosing one of the following settings. If the backup contains only the system state or a file or folder, these settings are not applied.

○ Normal backup performance

The time to create the backup is proportional to the size of the data being backed up. The server performance is not decreased.

○ Faster backup performance

Increase the backup speed by just tracking changes between the last and current backup. The performance of the server may be reduced by as much as 200% because of the work to track these changes.

● Custom

Configure each volume separately if you have certain volumes that have disk-intensive operations.

Volume	Backup Option
System Reserved	Full backup
New Volume (F:)	Full backup
Backup Drive 2	
Local disk (C:)	Full backup

FIGURE 12-5 Individual volume options in the Optimize Backup Performance dialog box.

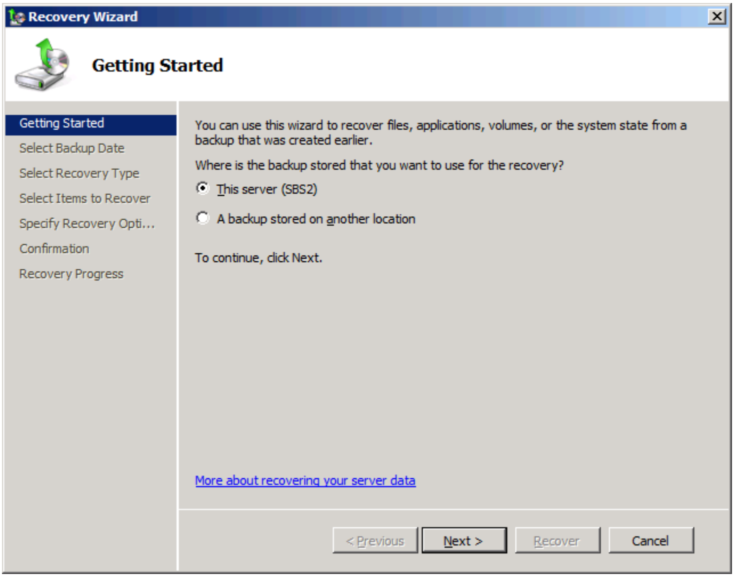
Performing Restores

As mentioned earlier, when you click *Restore server data from backup* in the Windows SBS Console, the Windows Server Backup Console appears. As with most backup software products, Windows Server Backup lets you select the elements you want to restore and specify whether to copy them to their original locations or to an alternative folder or volume.

CAUTION **One of the most crucial elements of any backup strategy is the need to perform regular test restores to ensure that your backups are viable. Even when your backup software indicates the successful completion of your backup jobs, there is no way to be absolutely sure you are protected against data loss other than actually performing a restore.**

To perform a restore, use the following procedure:

1. Log on to your Windows SBS 2011 server using a domain account with administrative privileges. The Windows SBS Console appears.
2. Click *Backup and server storage*, and then select the *Backup* tab.
3. In the *Tasks* list, click *Restore server data from backup*. The Windows Server Backup Console appears.
4. In the Actions pane, click *Recover*. The Recovery Wizard appears, displaying the Getting Started page.



You can use this wizard to recover files, applications, volumes, or the system state from a backup that was created earlier.

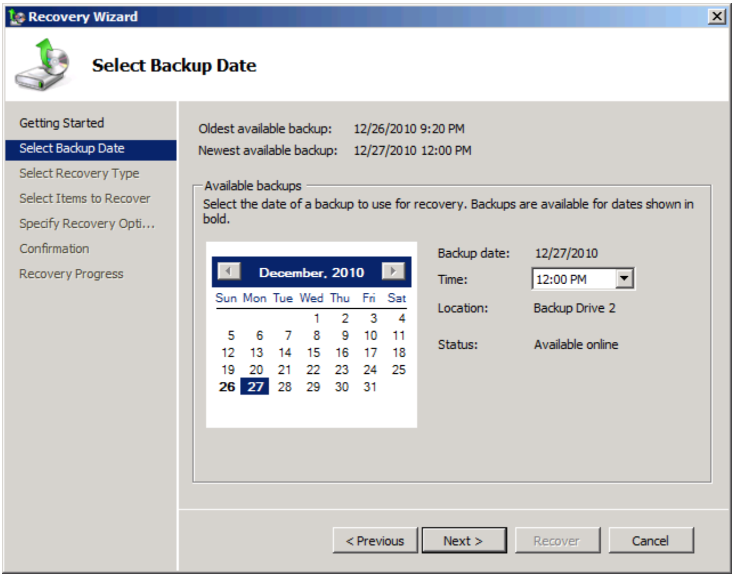
Where is the backup stored that you want to use for the recovery?

● This server (SBS2)

○ A backup stored on another location

To continue, click Next.

5. Click *Next* to accept the default *This server* option. The Select Backup Date page appears.



Select Backup Date

Oldest available backup: 12/26/2010 9:20 PM
Newest available backup: 12/27/2010 12:00 PM

Available backups

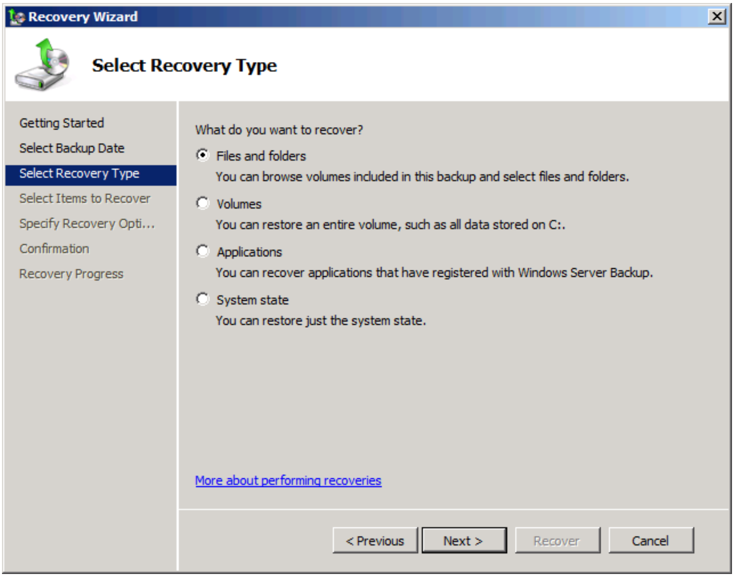
Select the date of a backup to use for recovery. Backups are available for dates shown in bold.

December, 2010

Sun	Mon	Tue	Wed	Thu	Fri	Sat
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	**27**	28	29	30	31	

Backup date: 12/27/2010
Time: 12:00 PM
Location: Backup Drive 2
Status: Available online

6. In the *Available backups* box, select the date and time of the backup you want to restore and click *Next*. The Select Recovery Type page appears.



Select Recovery Type

What do you want to recover?

● Files and folders
You can browse volumes included in this backup and select files and folders.

○ Volumes
You can restore an entire volume, such as all data stored on C:.

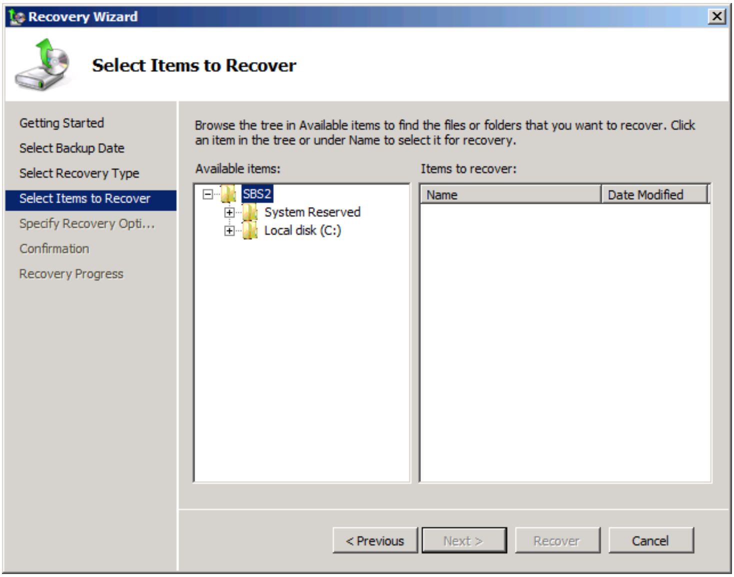
○ Applications
You can recover applications that have registered with Windows Server Backup.

○ System state
You can restore just the system state.

More about performing recoveries

7. Select one of the following options to specify what type of restore you want to perform:

   - **Files and folders** Displays the Select Items To Recover page, on which you can select the files or folders you want to restore, and the Specify Recovery Options page, on which you can select a destination for the restored files or folders and configure the program's overwrite behavior.

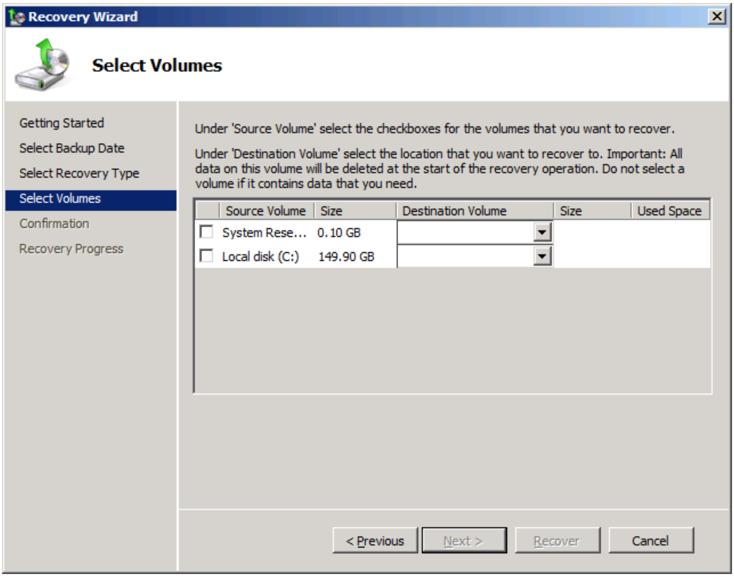


Browse the tree in Available items to find the files or folders that you want to recover. Click an item in the tree or under Name to select it for recovery.

Available items:

Items to recover:

   - **Volumes** Displays the Select Volumes page, on which you can select the volumes you want to restore and specify a destination for each one.

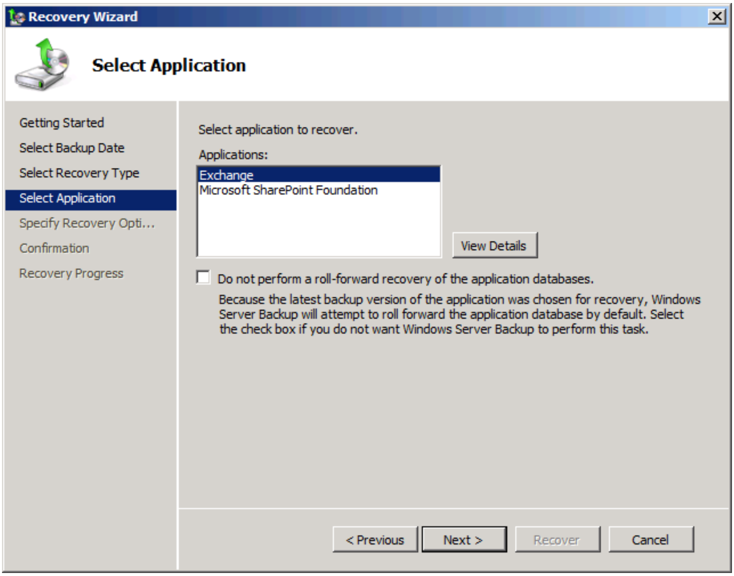


Under 'Source Volume' select the checkboxes for the volumes that you want to recover.

Under 'Destination Volume' select the location that you want to recover to. Important: All data on this volume will be deleted at the start of the recovery operation. Do not select a volume if it contains data that you need.

	Source Volume	Size	Destination Volume	Size	Used Space
□	System Rese...	0.10 GB	▾		
□	Local disk (C:)	149.90 GB	▾		

- **Applications** Displays the Select Application page, on which you can select the application you want to restore; and the Specify Recovery Options page, on which you can select a destination for the restored application.



Select application to recover.

Applications:

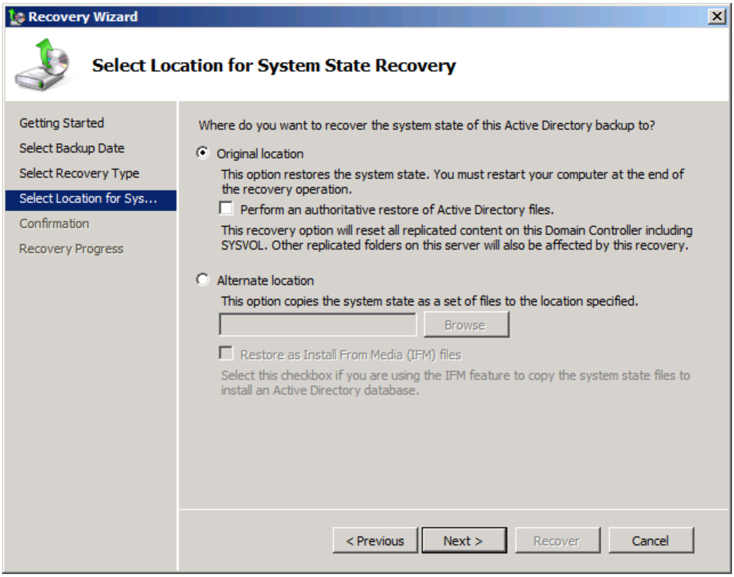
Exchange
Microsoft SharePoint Foundation

□ Do not perform a roll-forward recovery of the application databases.

Because the latest backup version of the application was chosen for recovery, Windows Server Backup will attempt to roll forward the application database by default. Select the check box if you do not want Windows Server Backup to perform this task.

NOTE Windows Server Backup is capable of performing only full restores of the system's Microsoft Exchange Server and SharePoint Foundation data. For example, you cannot select a particular Exchange Server mailbox for restoration.

- **System state** Displays the Select Location For System State Recovery page, on which you can choose to restore the Active Directory database to its original or an alternative location.



Recovery Wizard

Select Location for System State Recovery

Where do you want to recover the system state of this Active Directory backup to?

● Original location

This option restores the system state. You must restart your computer at the end of the recovery operation.

□ Perform an authoritative restore of Active Directory files.

This recovery option will reset all replicated content on this Domain Controller including SYSVOL. Other replicated folders on this server will also be affected by this recovery.

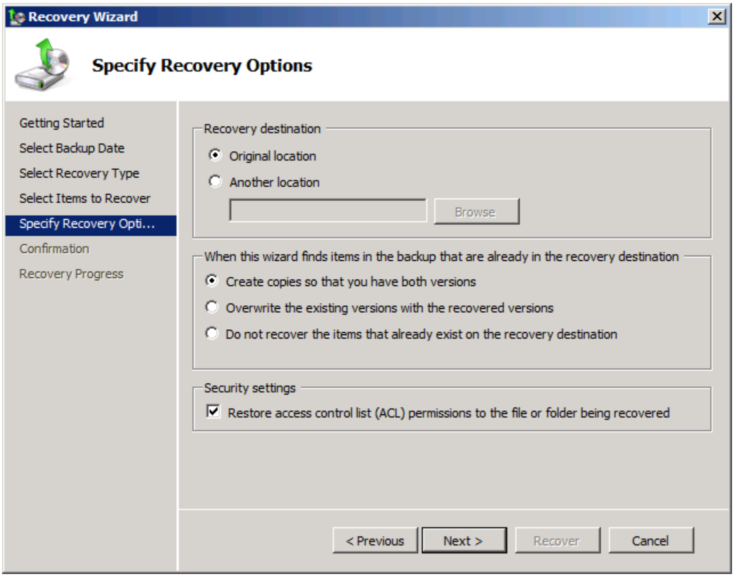
○ Alternate location

This option copies the system state as a set of files to the location specified.

□ Restore as Install From Media (IFM) files

Select this checkbox if you are using the IFM feature to copy the system state files to install an Active Directory database.

8. Configure the required settings for the type of restore you intend to perform. If you selected the *Files and folders* option or the *Applications* option, use the controls on the Specify Recovery Options page to select the destination for the restored elements and, if necessary, specify whether the program should overwrite existing files with the same names. If you selected the *Volumes* option, use the *Destination volume* drop-down lists on the Select Volumes page to specify the destinations for the restored volumes.



Specify Recovery Options

Recovery destination

● Original location

○ Another location

When this wizard finds items in the backup that are already in the recovery destination

● Create copies so that you have both versions

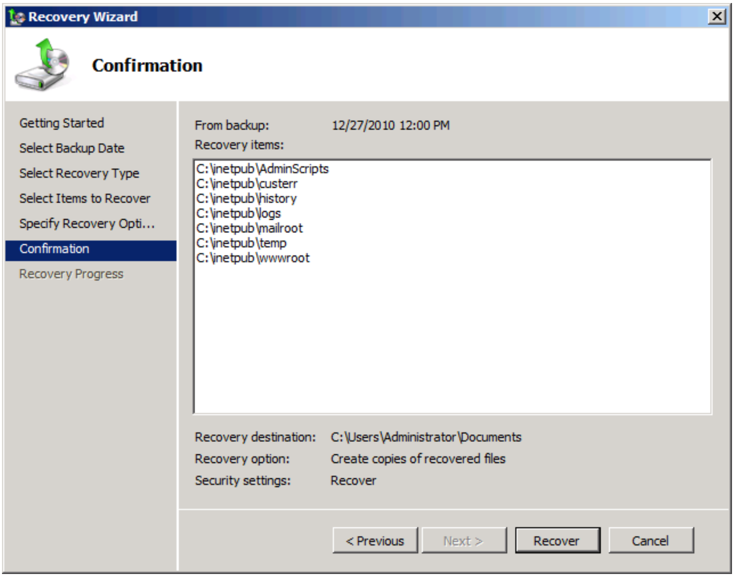
○ Overwrite the existing versions with the recovered versions

○ Do not recover the items that already exist on the recovery destination

Security settings

☑ Restore access control list (ACL) permissions to the file or folder being recovered

9. Click *Next*. The Confirmation page appears.



Confirmation

From backup: 12/27/2010 12:00 PM

Recovery items:

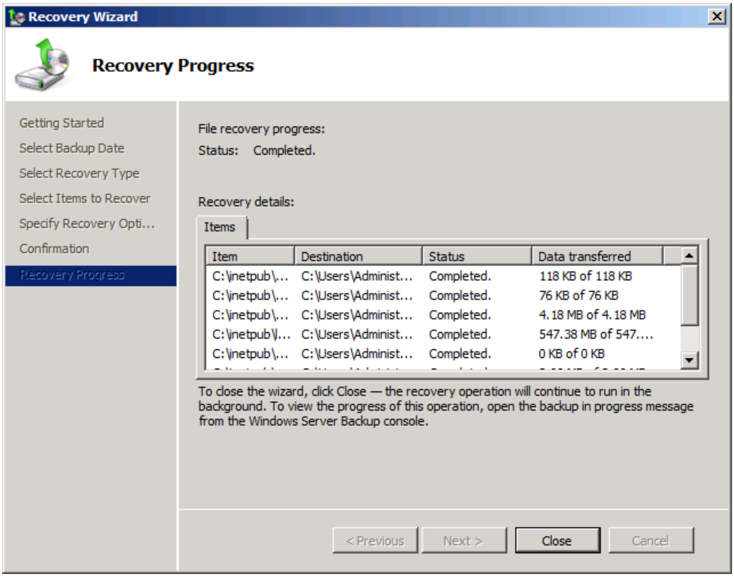
```
C:\inetpub\AdminScripts
C:\inetpub\custerr
C:\inetpub\history
C:\inetpub\logs
C:\inetpub\mailroot
C:\inetpub\temp
C:\inetpub\wwwroot
```

Recovery destination: C:\Users\Administrator\Documents

Recovery option: Create copies of recovered files

Security settings: Recover

10. Click *Recover*. The Recovery Progress page appears, as the wizard restores the items you selected and places them in your specified destination.



File recovery progress:

Status: Completed.

Recovery details:

Item	Destination	Status	Data transferred
C:\inetpub\...	C:\Users\Administ...	Completed.	118 KB of 118 KB
C:\inetpub\...	C:\Users\Administ...	Completed.	76 KB of 76 KB
C:\inetpub\...	C:\Users\Administ...	Completed.	4.18 MB of 4.18 MB
C:\inetpub\...	C:\Users\Administ...	Completed.	547.38 MB of 547....
C:\inetpub\...	C:\Users\Administ...	Completed.	0 KB of 0 KB

To close the wizard, click Close — the recovery operation will continue to run in the background. To view the progress of this operation, open the backup in progress message from the Windows Server Backup console.

11. Click *Close*. The wizard closes and a File Recovery message appears in the Windows Server Backup Console.

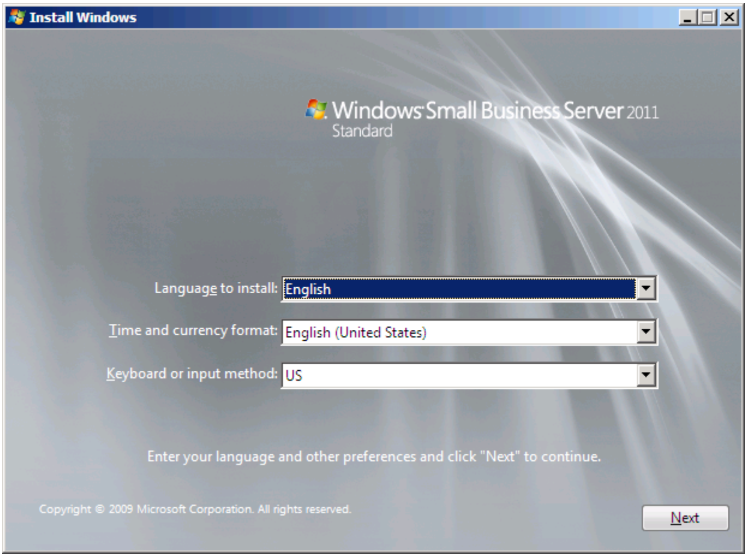
Recovering an Entire System

Because your backup job includes the system volume by default, along with the system recovery elements, you can recover an entire server if the internal hard disk or the computer containing it is lost or destroyed. Because all the system data, including the boot files, has been lost, you must start the computer using your Windows SBS 2011 installation disk. However, you do not have to perform a complete reinstallation of the operating system. Your Windows SBS 2011 disk includes the Windows Recovery Environment (RE), a bare-bones version of the operating system that provides you with tools you can use to diagnose and repair system problems, as well as the ability to perform a full restore from a backup located on an external hard drive.

To perform a complete restore of your primary server, do the following:

1. Start your computer and insert the Windows SBS 2011 installation disk into the DVD-ROM drive.

2. If necessary, press a key to boot from the DVD rather than the internal hard disk. The Install Windows page appears.



Language to install: English

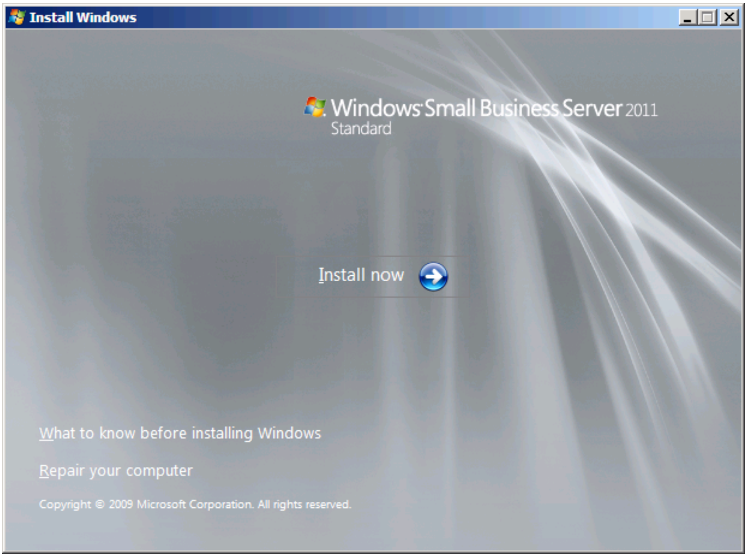
Time and currency format: English (United States)

Keyboard or input method: US

Enter your language and other preferences and click "Next" to continue.

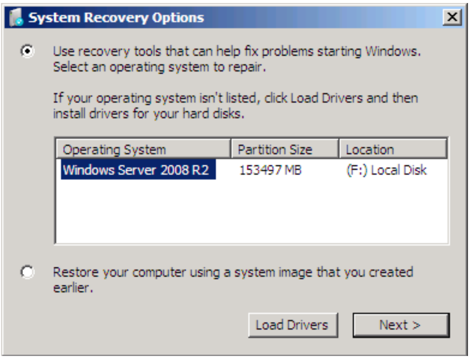
Copyright © 2009 Microsoft Corporation. All rights reserved.

3. Select the appropriate language, time, currency, and keyboard or input method values and then click *Next*. The Install Now page appears.


Install Windows
Windows Small Business Server 2011
Standard
Install now
What to know before installing Windows
Repair your computer

Copyright © 2009 Microsoft Corporation. All rights reserved.

4. Click *Repair your computer*. The System Recovery Options Wizard appears.



● Use recovery tools that can help fix problems starting Windows. Select an operating system to repair.

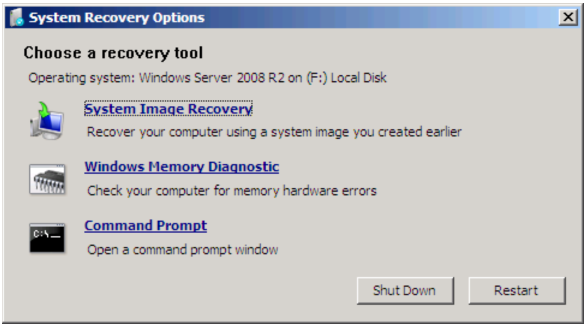
If your operating system isn't listed, click Load Drivers and then install drivers for your hard disks.

Operating System	Partition Size	Location
Windows Server 2008 R2	153497 MB	(F:) Local Disk

○ Restore your computer using a system image that you created earlier.

NOTE If your computer needs special drivers to access the hard disk drives, click *Load drivers* and insert a flash drive or other medium containing the driver installation files.

5. Select Microsoft Windows Server 2008 R2 and click *Next*. The Choose A Recovery Tool page appears.



Choose a recovery tool

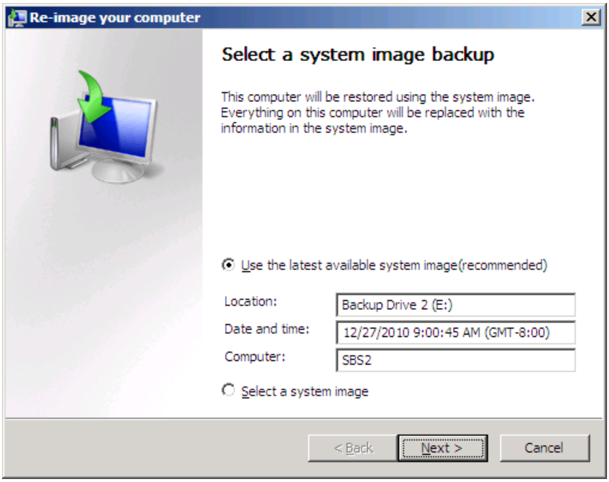
Operating system: Windows Server 2008 R2 on (F:) Local Disk

System Image Recovery
Recover your computer using a system image you created earlier

Windows Memory Diagnostic
Check your computer for memory hardware errors

Command Prompt
Open a command prompt window

6. Click *System image recovery*. The Re-Image Your Computer Wizard appears, displaying the Select A System Image Backup page.



Select a system image backup

This computer will be restored using the system image. Everything on this computer will be replaced with the information in the system image.

● Use the latest available system image(recommended)

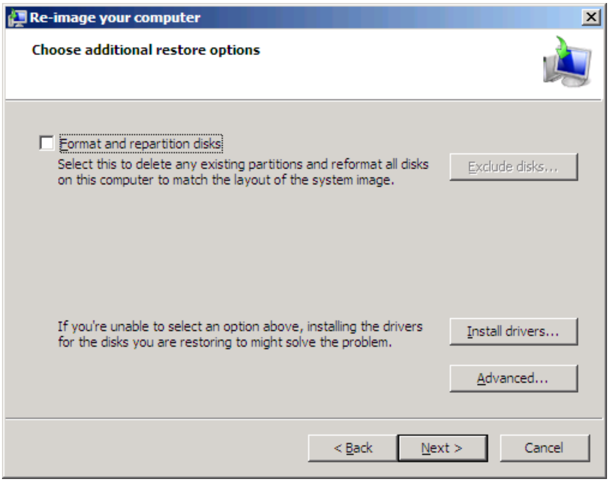
Location: Backup Drive 2 (E:)

Date and time: 12/27/2010 9:00:45 AM (GMT-8:00)

Computer: SBS2

○ Select a system image

7. Confirm that the system has located the most recent backup on your drive and click *Next*. The Choose Additional Restore Options page appears.



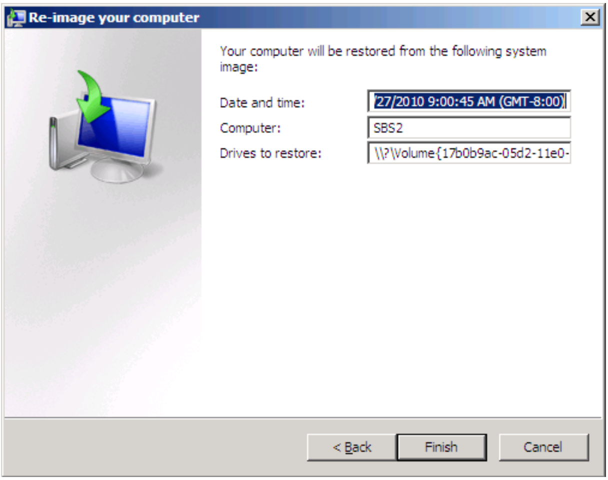
Choose additional restore options

□ Format and repartition disks

Select this to delete any existing partitions and reformat all disks on this computer to match the layout of the system image.

If you're unable to select an option above, installing the drivers for the disks you are restoring to might solve the problem.

8. Select the *Format and repartition disks* check box. If necessary, click *Exclude disks* and select any drives that you want to exclude from the restore. Then click *Next*. An Untitled Summary page appears.



Re-image your computer

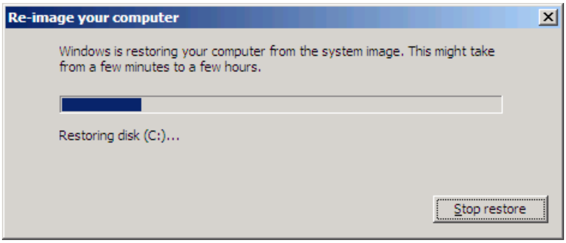
Your computer will be restored from the following system image:

Date and time: 27/2010 9:00:45 AM (GMT-8:00)

Computer: SBS2

Drives to restore: \\?\Volume{17b0b9ac-05d2-11e0-

9. Click *Finish*. A Re-Image Your Computer message box appears, prompting you to confirm your actions.
10. Click *Yes*. A progress indicator appears, displaying the progress of the restore.



Re-image your computer

Windows is restoring your computer from the system image. This might take from a few minutes to a few hours.

Restoring disk (C:)...

When the restore is finished, a Do You Want To Restart Your Computer Now? message box appears, offering you the ability to abort the default 60-second restart interval.

11. Remove the Windows SBS 2011 installation disk from the DVD-ROM drive and click *Restart now*. The computer restarts and boots from the newly restored system drive.

CHAPTER 13

Managing Windows SBS 2011

The Windows SBS Console enables you to manage many of the most important elements of Windows Small Business Server (SBS) 2011, but it does not do everything. A Windows SBS administrator must use the other tools supplied with the operating system in many situations. This chapter covers some of these tools and the tasks commonly associated with them.

Accessing Remote Computers

Depending on the layout of the network, it might be difficult, or even impossible, for administrators to physically access the computers they need to manage. Servers might be stored in a locked closet or even located in a branch office. Windows SBS 2011 includes a number of tools that enable administrators to access remote computers, as described in the following sections.

Using Remote Desktop

Remote Desktop is a client/server application that enables a user on one computer to log on to another computer and perform virtually any task possible from the local console. The Remote Desktop server capability is built into most Windows operating systems, and any Windows computer can run a Remote Desktop client program.

> ***NOTE*** **All the business-oriented versions of Windows operating systems include Remote Desktop server capabilities, including Windows 7 Professional, Windows Vista Business, and Windows XP Professional. The Home-based operating systems in the Windows 7, Windows Vista, and Windows XP lines do not include the server capability, but they do have a Remote Desktop client.**

As the name implies, the Remote Desktop client functions strictly as a terminal that controls the activities of the server from a distance. The client computer runs a program called *Remote Desktop Connection (RDC)*, which sends keystrokes and mouse commands to the server and receives output in the form of display elements. When you log on to a computer using Remote Desktop and start an application, the application actually runs on the server using the server's processor, memory, and other resources. In the same way, configuring system settings with Remote Desktop means that you are reconfiguring the server, not the client.

Remote Desktop is a limited version of Remote Desktop Services, a Windows Server role that enables multiple users to access applications running on a server instead of installing them on a local drive. Remote Desktop Services requires the purchase of additional Client Access Licenses (CALs) and cannot run on a Windows SBS 2011 primary server, but the Remote Desktop version is operable on all servers without additional licensing, although it is limited to two connections.

> ***NOTE*** **To use Remote Desktop Services on a computer running Windows Server 2008 R2, you must install the Remote Desktop Services role, but the Remote Desktop server capabilities are available by default, even on computers that do not have the role installed. This means that you can connect to your Windows SBS 2011 primary server using Remote Desktop, even though you have not installed (and should not install) the Remote Desktop Services role.**

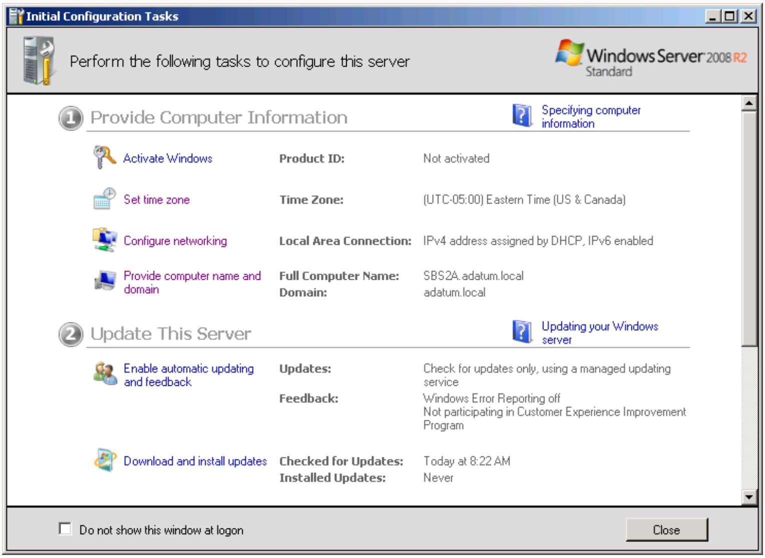
To administer a computer running Windows SBS 2011 or Windows Server 2008 R2 using Remote Desktop, you must complete two tasks:

- Enable Remote Desktop on the server.
- Establish a connection between the client and the server.

Enabling Remote Desktop

By default, computers running Windows Server 2008 R2 have their Remote Desktop server functions disabled. This is to prevent access by unauthorized users before all the computer's security precautions are in place. However, because the Windows SBS 2011 installation process secures the computer, the setup program enables Remote Desktop on the primary server. To enable Remote Desktop manually on a server running Windows Server 2008 R2, use this procedure:

1. Log on to your server, using an account with network Administrator privileges. The Initial Configuration Tasks window appears.



Initial Configuration Tasks

Perform the following tasks to configure this server

Windows Server 2008 R2 Standard

1 Provide Computer Information — Specifying computer information

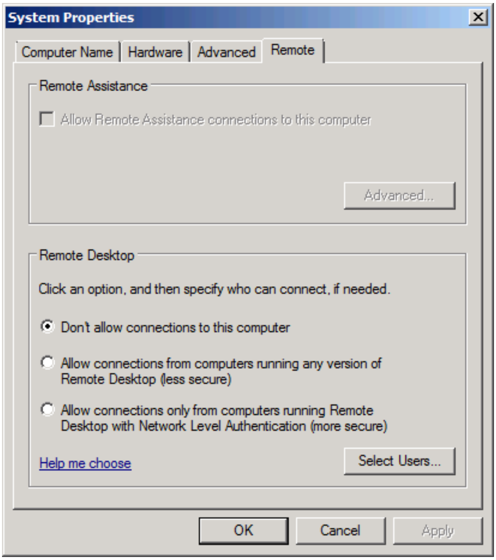
Activate Windows	**Product ID:**	Not activated
Set time zone	**Time Zone:**	(UTC-05:00) Eastern Time (US & Canada)
Configure networking	**Local Area Connection:**	IPv4 address assigned by DHCP, IPv6 enabled
Provide computer name and domain	**Full Computer Name:** **Domain:**	SBS2A.adatum.local adatum.local

2 Update This Server — Updating your Windows server

Enable automatic updating and feedback	**Updates:**	Check for updates only, using a managed updating service
	Feedback:	Windows Error Reporting off Not participating in Customer Experience Improvement Program
Download and install updates	**Checked for Updates:** **Installed Updates:**	Today at 8:22 AM Never

□ Do not show this window at logon

2. In the *Customize this server* section, click *Enable Remote Desktop*. The System Properties sheet appears.



System Properties

Remote Assistance

□ Allow Remote Assistance connections to this computer

Remote Desktop

Click an option, and then specify who can connect, if needed.

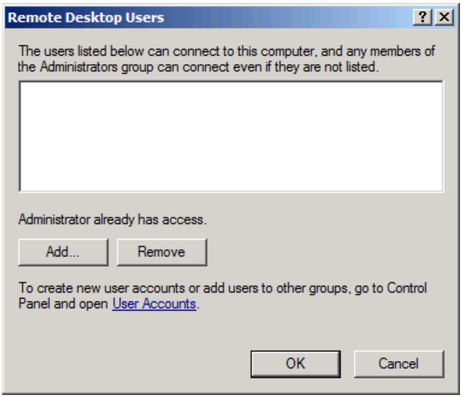
● Don't allow connections to this computer

○ Allow connections from computers running any version of Remote Desktop (less secure)

○ Allow connections only from computers running Remote Desktop with Network Level Authentication (more secure)

TIP **If the server is a domain controller, the Server Manager Console appears instead, and you can open the System Properties sheet by clicking *Configure Remote Desktop* in the *server summary* section of the Server Manager Console.**

3. In the *Remote Desktop* section, select the *Allow connections from computers running any version of Remote Desktop (less secure)*. A Remote Desktop message box appears, informing you that the system will open a firewall exception for Remote Desktop communications.
4. Click *OK*. Then click *Select users*. The Remote Desktop Users dialog box appears.



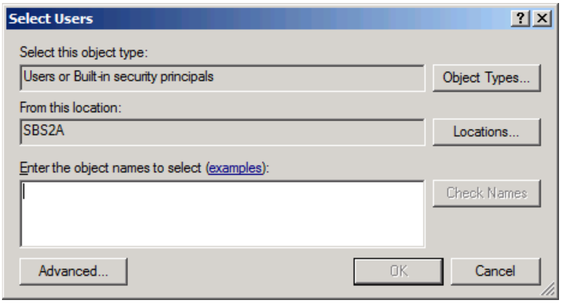
Remote Desktop Users

The users listed below can connect to this computer, and any members of the Administrators group can connect even if they are not listed.

Administrator already has access.

To create new user accounts or add users to other groups, go to Control Panel and open User Accounts.

5. Click *Add*. The Select Users dialog box appears.



Select Users

Select this object type:
Users or Built-in security principals

From this location:
SBS2A

Enter the object names to select (examples):

6. In the *Enter the object names to select* text box, type the names of the user accounts and groups to which you want to grant Remote Desktop access, and then click *OK*. The users and groups you specify appear in the Remote Desktop Users dialog box.

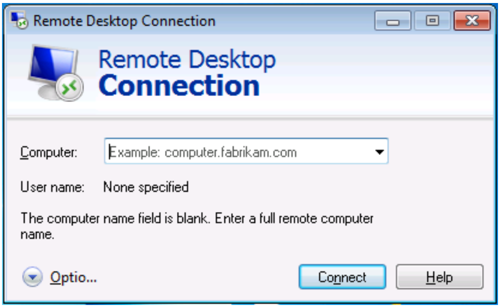
NOTE **The Remote Desktop Users dialog box adds the objects you specify to the Remote Desktop Users local group on the server, which enables them to access the server from a remote location. Administrators have Remote Desktop access by default; you do not have to add them to the Remote Desktop Users group.**

7. Click *OK* to close the Remote Desktop Users dialog box.
8. Click *OK* to close the System Properties sheet.

Using the Remote Desktop Connection Client

Once you have enabled Remote Desktop on the computer that functions as the server, you can run the Remote Desktop Connection program on the client and establish a connection to it, using these steps:

1. Log on to a Windows 7 workstation using a domain user account.
2. Click *Start*. Then click *All Programs* > *Accessories* > *Remote Desktop Connection*. The Remote Desktop Connection dialog box appears.

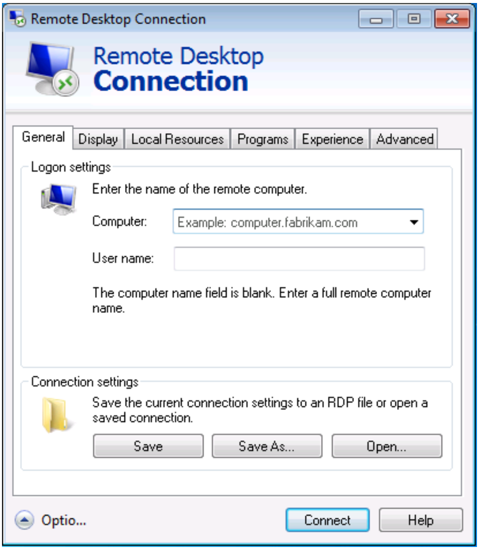


Computer: Example: computer.fabrikam.com

User name: None specified

The computer name field is blank. Enter a full remote computer name.

3. In the *Computer* text box, type the name or IP address of the computer to which you want to connect.
4. Click *Options*. The dialog box expands.



Enter the name of the remote computer.

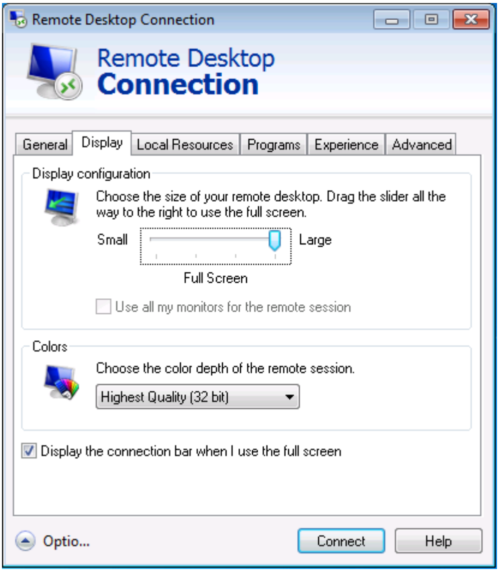
Computer: Example: computer.fabrikam.com

User name:

The computer name field is blank. Enter a full remote computer name.

Save the current connection settings to an RDP file or open a saved connection.

5. Click the *Display* tab.



Remote Desktop Connection

Remote Desktop Connection

General | Display | Local Resources | Programs | Experience | Advanced

Display configuration

Choose the size of your remote desktop. Drag the slider all the way to the right to use the full screen.

Small — Large

Full Screen

□ Use all my monitors for the remote session

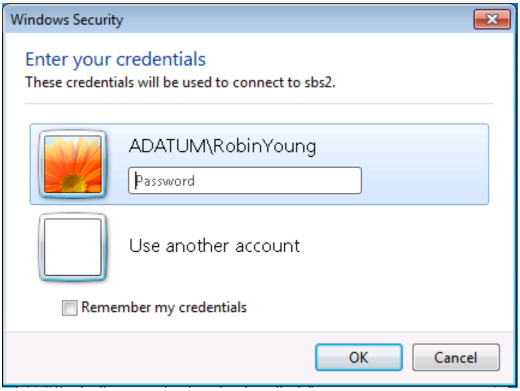
Colors

Choose the color depth of the remote session.

Highest Quality (32 bit)

☑ Display the connection bar when I use the full screen

6. Adjust the *Remote Desktop size* slider to a value smaller than that of your current screen resolution.
7. Click *Connect*. A Windows Security dialog box appears.



Windows Security

Enter your credentials

These credentials will be used to connect to sbs2.

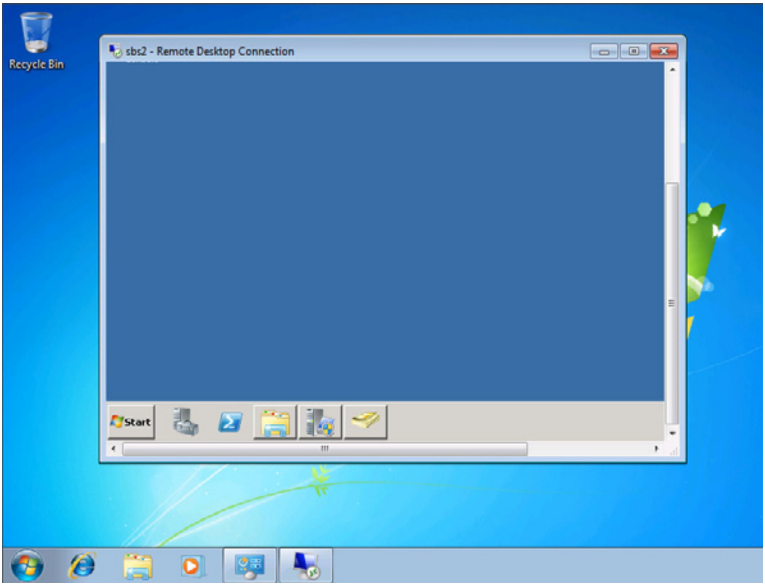
ADATUM\RobinYoung

Password

Use another account

□ Remember my credentials

8. In the *User name* and *password* text boxes, type the credentials for an account that has Remote Desktop connection privileges on the server and click *OK*. A Remote Desktop window appears, containing the server's desktop.

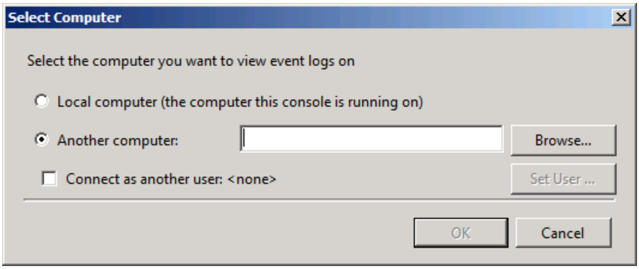


At this point, any activity you perform within the Remote Desktop window is taking place on the remote computer, using that computer's resources. The RDC client program uses the Remote Desktop Protocol (RDP) to send your keystrokes and mouse movements to the server and receive the screen display elements that appear on your monitor. Closing the Remote Desktop window disconnects the client from the server.

Using Microsoft Management Console

Microsoft Management Console (MMC) is the primary administration tool for Windows computers. The MMC program is a shell application that can load individual components called *snap-ins*. Many of the administration tools in the Windows server and workstation operating systems take the form of MMC snap-ins. For example, most of the shortcuts you see when you open the Administrative Tools program group on a computer running Windows Server 2008 R2 are preconfigured MMC consoles that contain one or more snap-ins.

One of the primary advantages of the MMC environment is the ability to direct a snap-in to another computer on the network, enabling you to administer its properties from a remote location. Many MMC consoles that connect to the local system have a default *Connect to another computer* menu item that, when clicked, displays a dialog box like the one shown in Figure 13-1, which you can use to browse to another system on the network.



Select the computer you want to view event logs on

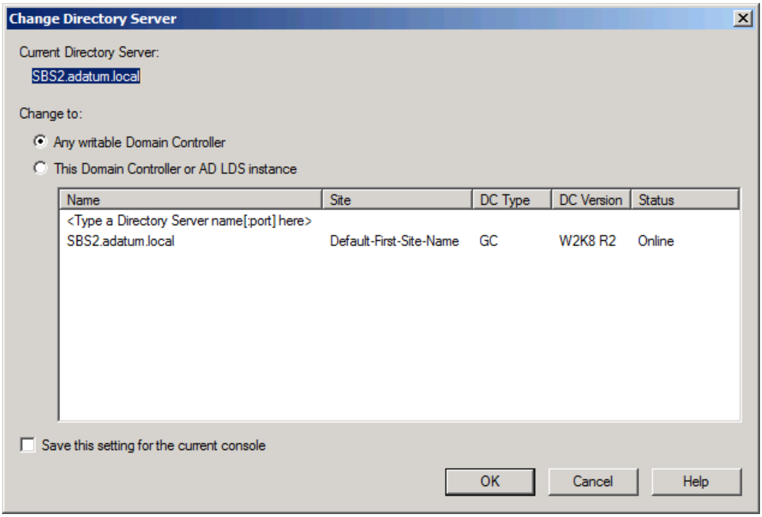
○ Local computer (the computer this console is running on)

● Another computer:

□ Connect as another user: <none>

FIGURE 13-1 The Select Computer dialog box, which enables you to direct an MMC to another computer on the network.

The ability to do this depends on the nature of the snap-in and the configuration of the console. For example, the snap-ins that you use to administer Active Directory Domain Services (AD DS), such as the Active Directory Users And Computers Console, connect to the local domain by default. However, you can point the snap-in to another domain on a network that has one, or point it to a specific domain controller in the current domain using the Change Directory Server dialog box, shown in Figure 13-2.



Current Directory Server:
SBS2.adatum.local

Change to:

● Any writable Domain Controller

○ This Domain Controller or AD LDS instance

Name	Site	DC Type	DC Version	Status
<Type a Directory Server name[:port] here>				
SBS2.adatum.local	Default-First-Site-Name	GC	W2K8 R2	Online

□ Save this setting for the current console

FIGURE 13-2 The Change Directory Server dialog box, which enables you to direct an AD DS Console to a specific domain controller.

TIP **If you want to administer a role on a remote server from a computer that is not running that role, you can install the required snap-in using the Remote Server Administration Tools feature in the Server Manager Console.**

Another powerful feature in MMC is the ability to load multiple snap-ins and create a console that performs a variety of functions. The Computer Management Console, shown in Figure 13-3, is an example of a single console that contains many snap-ins, all pointed at the local computer.

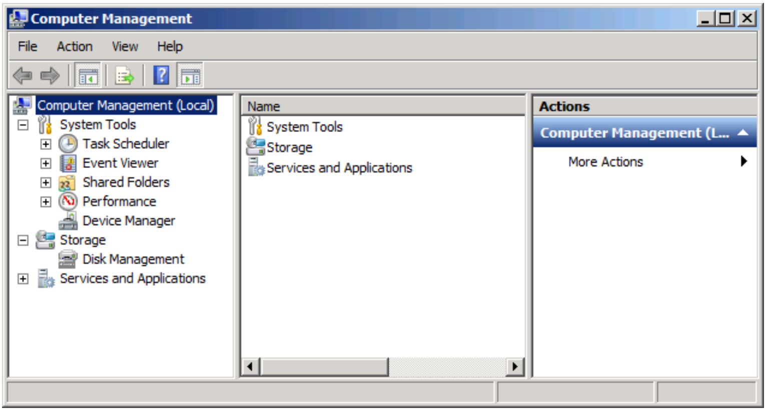


FIGURE 13-3 The Computer Management Console.

In addition to using the preconfigured consoles supplied with the operating system, you can create your own customized MMCs that contain any combination of snap-ins you want. Your custom consoles can contain a variety of snap-ins pointed at the same computer or multiple instances of the same snap-in pointed at different computers. For example, you can create a console containing an instance of the Event Viewer snap-in for each computer on your network, so you can examine all the network's system logs using one tool, as shown in Figure 13-4.

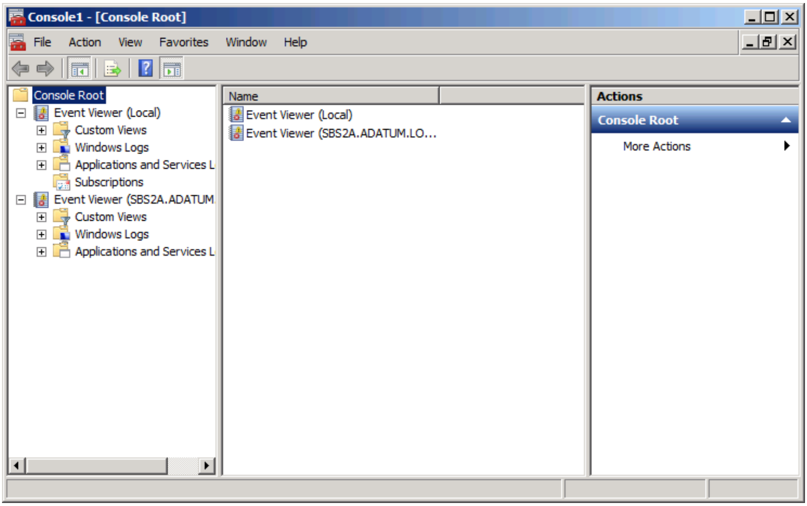
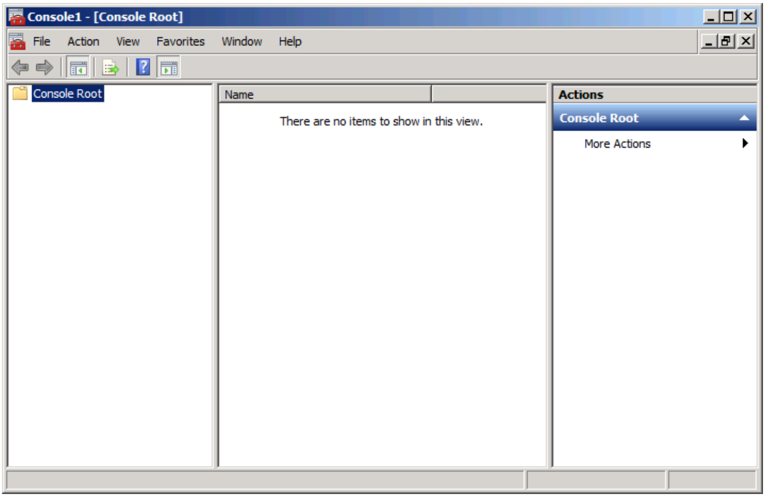


FIGURE 13-4 A custom MMC Console containing three instances of the Event Viewer snap-in.

> ***TIP*** **By default, Windows Firewall blocks the ports that most MMC snap-ins use to communicate with other computers on the network. You might have to open the Remote Service Management firewall exception before you can direct a snap-in to another computer.**

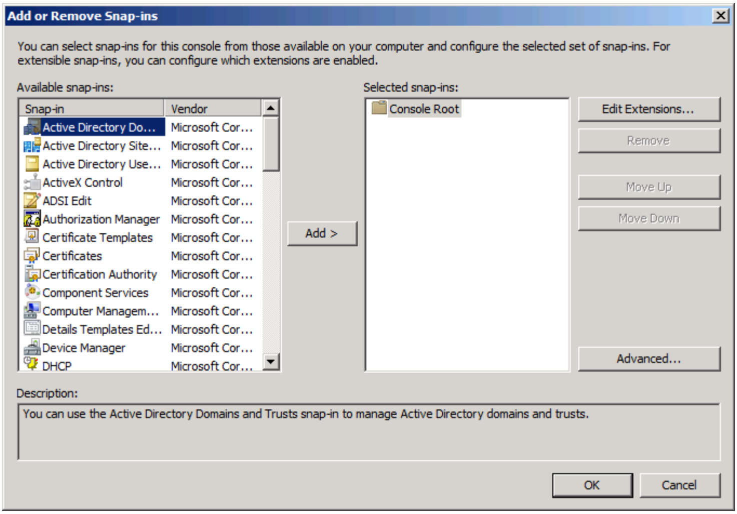
To create a custom MMC Console on a computer running Windows SBS 2011 or Windows Server 2008 R2, take the following steps:

1. Log on to the server using a domain account with administrative privileges.
2. Click *Start*, and then click *Run*. The Run dialog box appears.
3. In the *Open* text box, type **mmc** and click *OK*. When the User Account Control dialog box appears, click *Continue*. A blank MMC Console appears.



There are no items to show in this view.

4. Click *File* > *Add/Remove Snap-In*. The Add Or Remove Snap-Ins dialog box appears.



You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

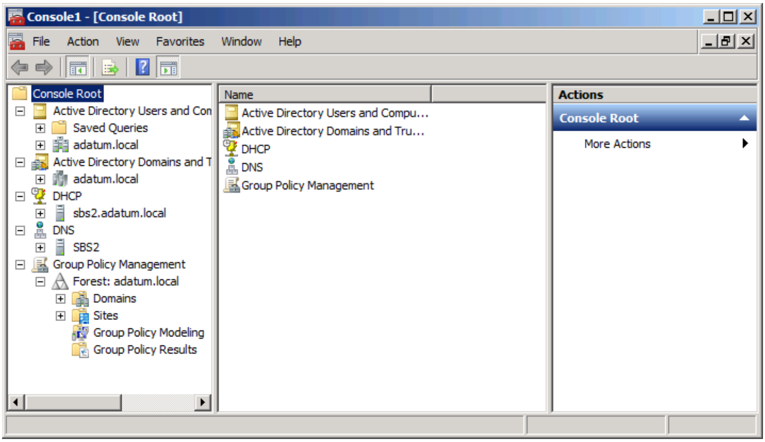
Snap-in	Vendor
Active Directory Do...	Microsoft Cor...
Active Directory Site...	Microsoft Cor...
Active Directory Use...	Microsoft Cor...
ActiveX Control	Microsoft Cor...
ADSI Edit	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificate Templates	Microsoft Cor...
Certificates	Microsoft Cor...
Certification Authority	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Details Templates Ed...	Microsoft Cor...
Device Manager	Microsoft Cor...
DHCP	Microsoft Cor...

You can use the Active Directory Domains and Trusts snap-in to manage Active Directory domains and trusts.

5. In the *Available snap-ins* list, select the snap-in you want to add to the console and click *Add*.

   Depending on the snap-in, a dialog box might appear, prompting you to select the computer or user account you want to manage. The snap-in then appears in the *Selected snap-ins* list.

6. Repeat step 5 to select additional snap-ins for the console (if desired) and click *OK*. The snap-ins appear in the console.

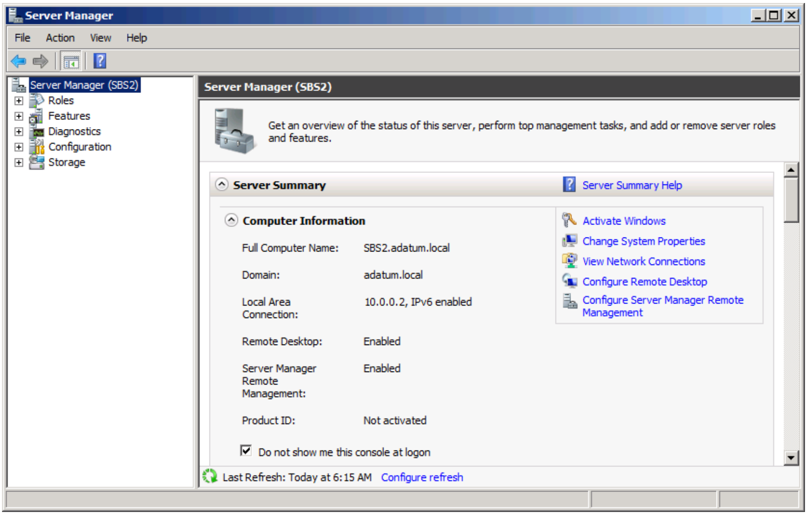


7. Click *File* > *Save As*. The *Save as* combo box appears.

8. Type a name for the console and click *Save*. MMC adds the new console to the Administrative Tools program group.

Using Server Manager

Windows SBS 2011 and Windows Server 2008 R2 use elements called *roles* and *features* to implement their various applications and services. During the installation of a Windows SBS 2011 primary server, the setup program adds a number of roles and features by default. The default Windows Server 2008 R2 installation includes no roles or features, however. The primary tool that Windows SBS 2011 and Windows Server 2008 R2 administrators use to install, remove, and manage roles and features is called Server Manager, shown in Figure 13-5.



Server Manager (SBS2)

Get an overview of the status of this server, perform top management tasks, and add or remove server roles and features.

Computer Information

Full Computer Name: SBS2.adatum.local

Domain: adatum.local

Local Area Connection: 10.0.0.2, IPv6 enabled

Remote Desktop: Enabled

Server Manager Remote Management: Enabled

Product ID: Not activated

☑ Do not show me this console at logon

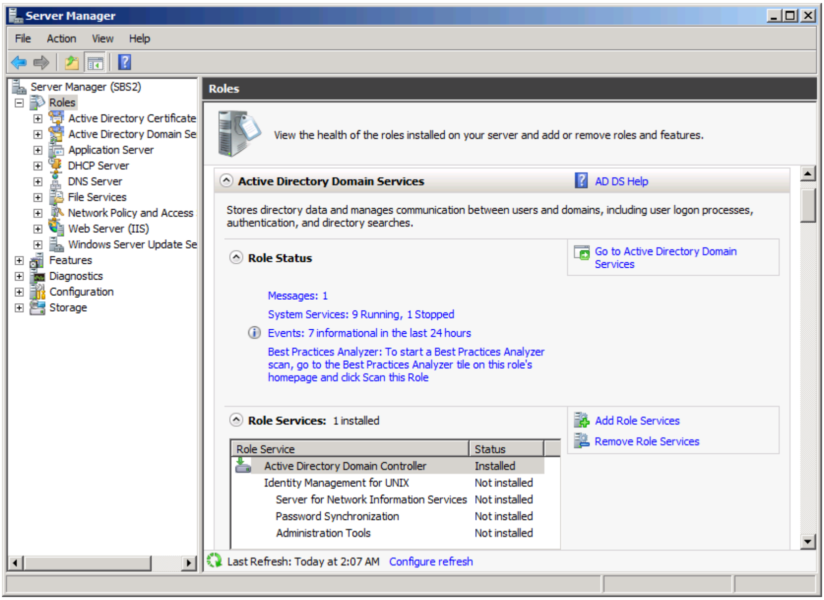
Last Refresh: Today at 6:15 AM

FIGURE 13-5 The Server Manager Console.

Server Manager is an MMC console that provides access to a variety of snap-ins, system configuration controls, and diagnostic tools. In addition, Server Manager includes wizards that enable you to install and remove roles and features. When you install a role that includes its own administration snap-ins, Server Manager, in most cases, provides access to those snap-ins.

Managing Roles

When you open the Server Manager Console on your Windows SBS 2011 primary server and expand the *Roles* node, the Scope (left) pane contains all the roles that the setup program added during the operating system installation, as shown in Figure 13-6. The Detail (right) pane contains a section for each role that displays its status.



View the health of the roles installed on your server and add or remove roles and features.

Active Directory Domain Services

Stores directory data and manages communication between users and domains, including user logon processes, authentication, and directory searches.

Role Status

Messages: 1

System Services: 9 Running, 1 Stopped

Events: 7 informational in the last 24 hours

Best Practices Analyzer: To start a Best Practices Analyzer scan, go to the Best Practices Analyzer tile on this role's homepage and click Scan this Role

Role Services: 1 installed

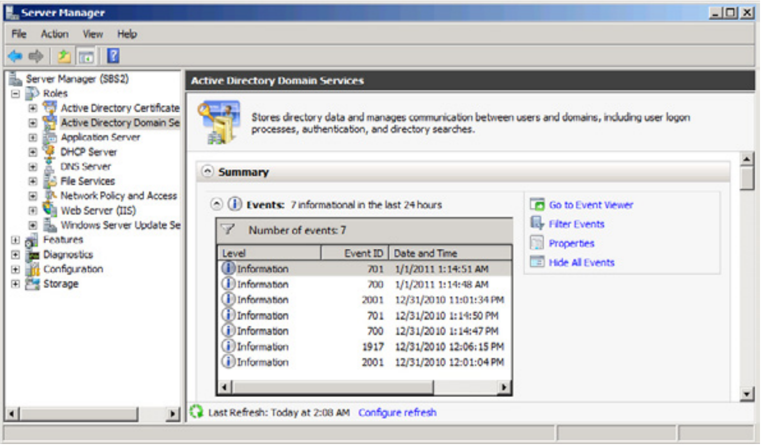
Role Service	Status
Active Directory Domain Controller	Installed
Identity Management for UNIX	Not installed
Server for Network Information Services	Not installed
Password Synchronization	Not installed
Administration Tools	Not installed

Last Refresh: Today at 2:07 AM

FIGURE 13-6 The *Roles* node in the Server Manager Console.

When you select one of the installed roles, the Scope pane contains a more detailed status display that contains some or all of the following items:

- **Events** Contains a list of the events pertaining to the role from the last 24 hours, derived from the Windows logs and linking to the Event Viewer Console.



Stores directory data and manages communication between users and domains, including user logon processes, authentication, and directory searches.

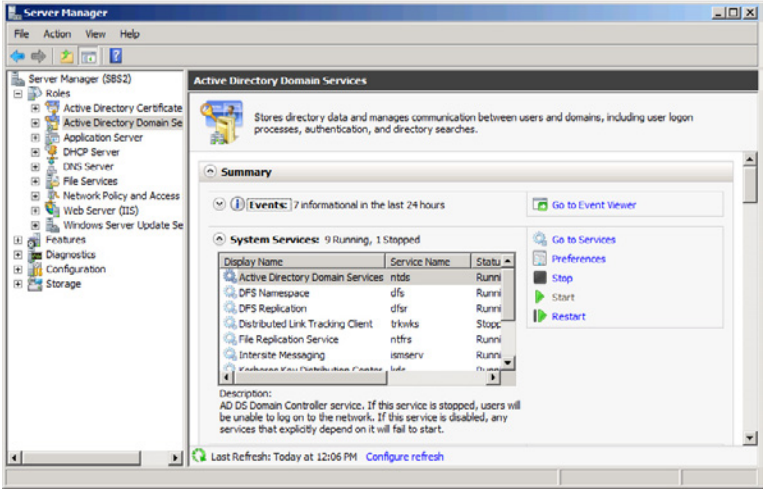
Events: 7 informational in the last 24 hours

Number of events: 7

Level	Event ID	Date and Time
Information	701	1/1/2011 1:14:51 AM
Information	700	1/1/2011 1:14:48 AM
Information	2001	12/31/2010 11:01:34 PM
Information	701	12/31/2010 1:14:50 PM
Information	700	12/31/2010 1:14:47 PM
Information	1917	12/31/2010 12:06:15 PM
Information	2001	12/31/2010 12:01:04 PM

Last Refresh: Today at 2:08 AM

- **System services** Contains a list of the services associated with the role, and enables you to stop, start, and configure them, just as you can from the Services Console.



Stores directory data and manages communication between users and domains, including user logon processes, authentication, and directory searches.

Events: 7 informational in the last 24 hours

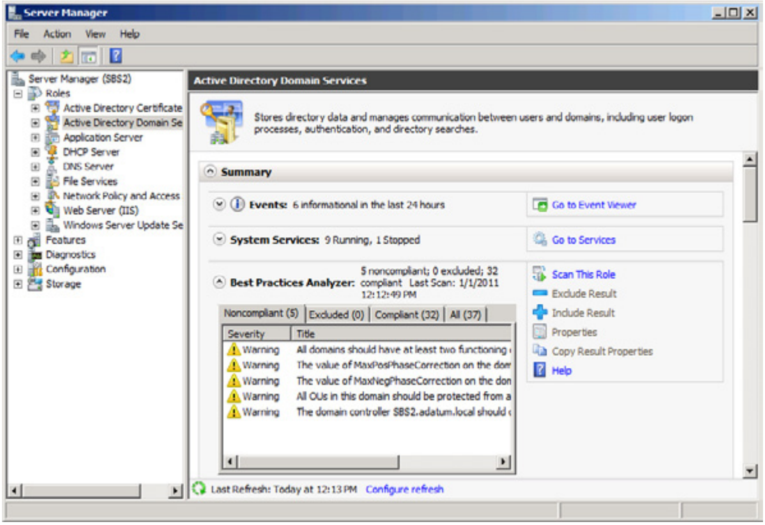
System Services: 9 Running, 1 Stopped

Display Name	Service Name	Statu
Active Directory Domain Services	ntds	Runni
DFS Namespace	dfs	Runni
DFS Replication	dfsr	Runni
Distributed Link Tracking Client	trkwks	Stopp
File Replication Service	ntfrs	Runni
Intersite Messaging	ismserv	Runni
Kerberos Key Distribution Center	kdc	Runn

Description:
AD DS Domain Controller service. If this service is stopped, users will be unable to log on to the network. If this service is disabled, any services that explicitly depend on it will fail to start.

Last Refresh: Today at 12:06 PM

- **Best practices analyzer (BPA)** For some roles, by initiating a BPA analysis, Windows Server 2008 R2 compares the role's current configuration to a set of predefined rules specifying its recommended parameters. Any failures to meet the recommendations appear as noncompliance warnings.



Stores directory data and manages communication between users and domains, including user logon processes, authentication, and directory searches.

Events: 6 informational in the last 24 hours

System Services: 9 Running, 1 Stopped

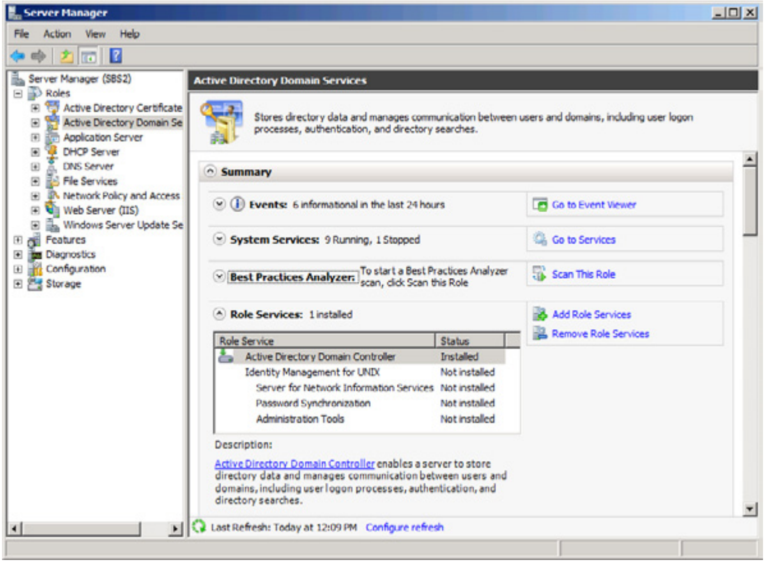
Best Practices Analyzer: 5 noncompliant; 0 excluded; 32 compliant Last Scan: 1/1/2011 12:12:49 PM

Severity	Title
Warning	All domains should have at least two functioning
Warning	The value of MaxPosPhaseCorrection on the dom
Warning	The value of MaxNegPhaseCorrection on the don
Warning	All OUs in this domain should be protected from a
Warning	The domain controller SBS2.adatum.local should

Last Refresh: Today at 12:13 PM

NOTE **The rules that the *Best practices analyzer* uses for its analysis are those for a standard Windows Server 2008 R2 installation; they are not specific to Windows SBS 2011. The default Windows SBS server configuration is therefore not compliant with all the recommended best practices.**

- **Role services** Contains a list of the role's subcomponents, and specifies which ones are currently installed. You can also add or remove role services using wizards.



Active Directory Domain Services

Stores directory data and manages communication between users and domains, including user logon processes, authentication, and directory searches.

Summary

Events: 6 informational in the last 24 hours

System Services: 9 Running, 1 Stopped

Best Practices Analyzer: To start a Best Practices Analyzer scan, click Scan this Role

Role Services: 1 installed

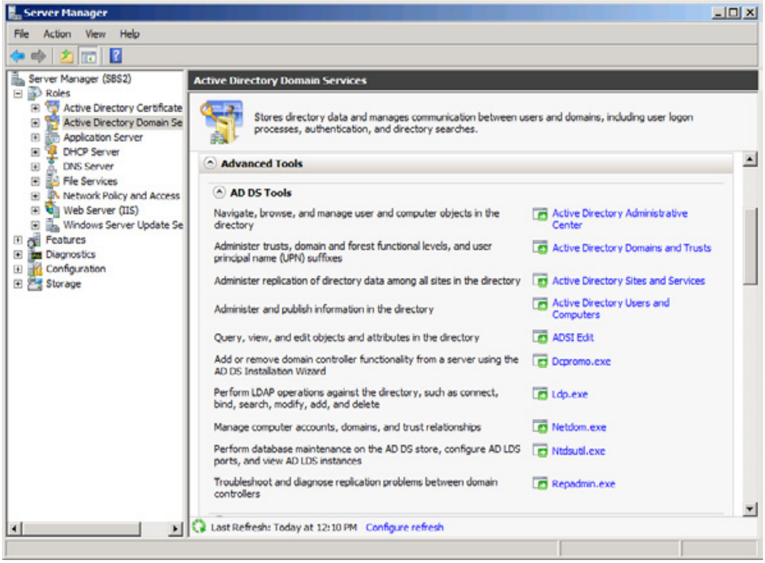
Role Service	Status
Active Directory Domain Controller	Installed
Identity Management for UNIX	Not installed
Server for Network Information Services	Not installed
Password Synchronization	Not installed
Administration Tools	Not installed

Description:

Active Directory Domain Controller enables a server to store directory data and manages communication between users and domains, including user logon processes, authentication, and directory searches.

Last Refresh: Today at 12:09 PM

- **Advanced tools** For roles with a large number of additional consoles or command prompt utilities, this section contains links to those tools and descriptions of their functions.



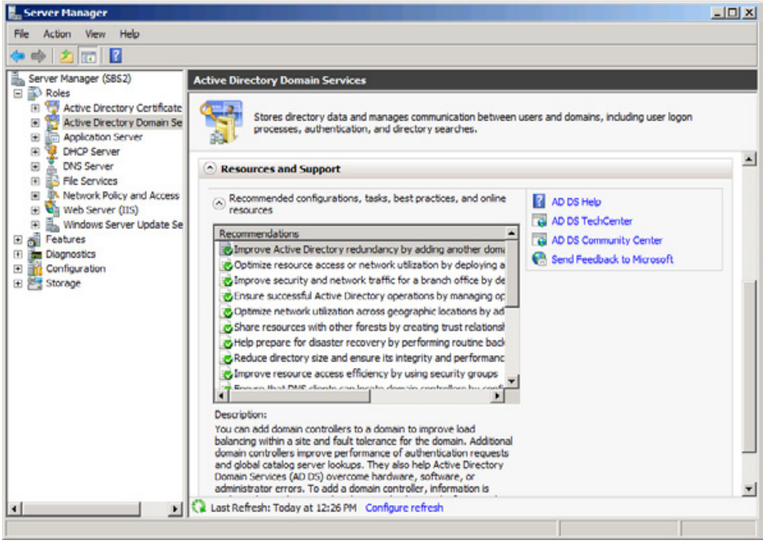
Active Directory Domain Services

Stores directory data and manages communication between users and domains, including user logon processes, authentication, and directory searches.

Navigate, browse, and manage user and computer objects in the directory	Active Directory Administrative Center
Administer trusts, domain and forest functional levels, and user principal name (UPN) suffixes	Active Directory Domains and Trusts
Administer replication of directory data among all sites in the directory	Active Directory Sites and Services
Administer and publish information in the directory	Active Directory Users and Computers
Query, view, and edit objects and attributes in the directory	ADSI Edit
Add or remove domain controller functionality from a server using the AD DS Installation Wizard	Dcpromo.exe
Perform LDAP operations against the directory, such as connect, bind, search, modify, add, and delete	Ldp.exe
Manage computer accounts, domains, and trust relationships	Netdom.exe
Perform database maintenance on the AD DS store, configure AD LDS ports, and view AD LDS instances	Ntdsutil.exe
Troubleshoot and diagnose replication problems between domain controllers	Repadmin.exe

Last Refresh: Today at 12:10 PM Configure refresh

- **Resources and support** Contains links to help files, Web resources, best practices, and recommended procedures.



Active Directory Domain Services

Stores directory data and manages communication between users and domains, including user logon processes, authentication, and directory searches.

Recommended configurations, tasks, best practices, and online resources

Recommendations
Improve Active Directory redundancy by adding another dom
Optimize resource access or network utilization by deploying a
Improve security and network traffic for a branch office by de
Ensure successful Active Directory operations by managing op
Optimize network utilization across geographic locations by ad
Share resources with other forests by creating trust relations
Help prepare for disaster recovery by performing routine back
Reduce directory size and ensure its integrity and performanc
Improve resource access efficiency by using security groups

Description:
You can add domain controllers to a domain to improve load balancing within a site and fault tolerance for the domain. Additional domain controllers improve performance of authentication requests and global catalog server lookups. They also help Active Directory Domain Services (AD DS) overcome hardware, software, or administrator errors. To add a domain controller, information is

Last Refresh: Today at 12:26 PM Configure refresh

In addition to these resources, Server Manager incorporates many of the MMC snap-ins associated with a role into the console. When you expand a role in the Scope pane, the snap-ins appear underneath, as shown in Figure 13-7.

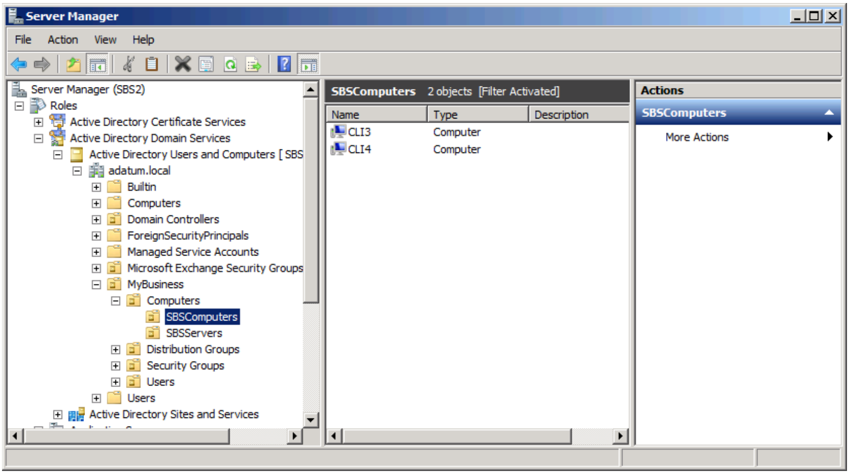


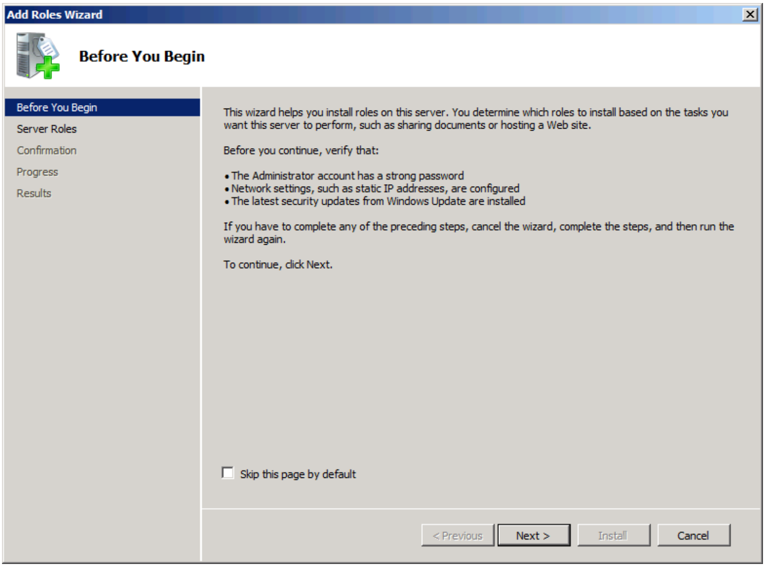
FIGURE 13-7 The Active Directory Users and Computers snap-in, incorporated into the Server Manager Console.

> ***NOTE*** **The Server Manager Console does not necessarily provide access to all the snap-ins associated with a particular role. You might find additional consoles in the Administrative Tools program group and others that are accessible only by adding them to a custom MMC.**

Adding Roles and Features

Windows SBS 2011 primary servers run a large number of roles by default, and administrators should be cautious about installing additional ones. However, if you have additional computers running Windows Server 2008 R2 on your network, you will most likely have to install some roles on it yourself. To install a role with the Server Manager Console, use the following procedure:

1. Log on to the server using a domain account with administrative privileges.
2. Click *Start*. Then click *Administrative Tools* > *Server Manager*. The Server Manager Console appears.
3. Select the *Roles* node.
4. In the Detail pane, click *Add roles*. The Add Roles Wizard appears, displaying the Before You Begin page.



This wizard helps you install roles on this server. You determine which roles to install based on the tasks you want this server to perform, such as sharing documents or hosting a Web site.

Before you continue, verify that:

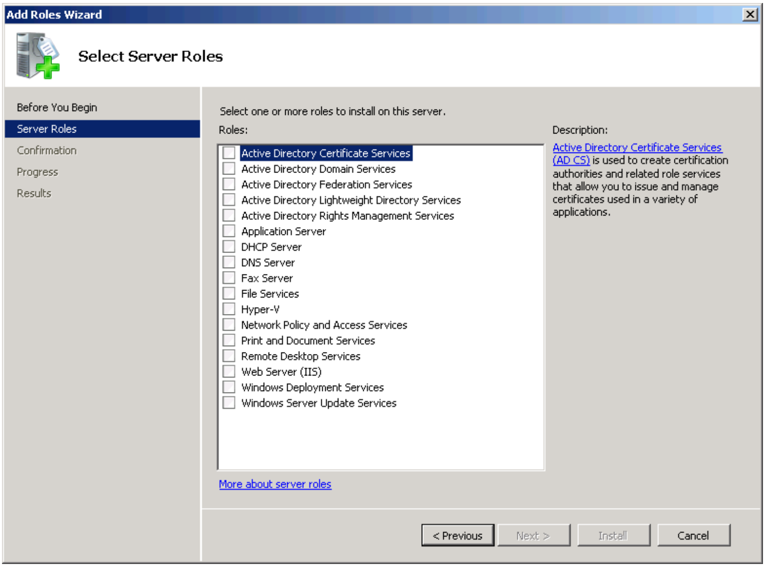
- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The latest security updates from Windows Update are installed

If you have to complete any of the preceding steps, cancel the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

□ Skip this page by default

5. Click *Next*. The Select Server Roles page appears.



Select one or more roles to install on this server.

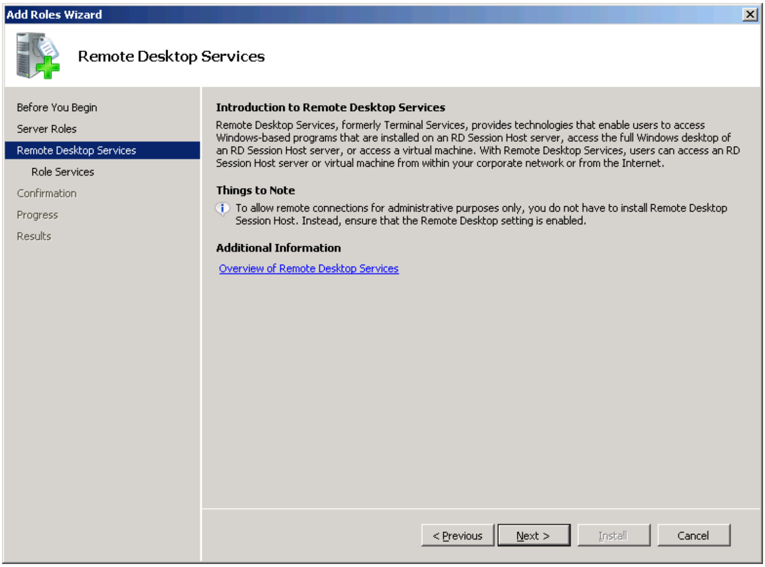
Roles:

- □ Active Directory Certificate Services
- □ Active Directory Domain Services
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Application Server
- □ DHCP Server
- □ DNS Server
- □ Fax Server
- □ File Services
- □ Hyper-V
- □ Network Policy and Access Services
- □ Print and Document Services
- □ Remote Desktop Services
- □ Web Server (IIS)
- □ Windows Deployment Services
- □ Windows Server Update Services

Description:

Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.

6. Select the check box for the role you want to install and click *Next*. An Introduction page appears.



Introduction to Remote Desktop Services

Remote Desktop Services, formerly Terminal Services, provides technologies that enable users to access Windows-based programs that are installed on an RD Session Host server, access the full Windows desktop of an RD Session Host server, or access a virtual machine. With Remote Desktop Services, users can access an RD Session Host server or virtual machine from within your corporate network or from the Internet.

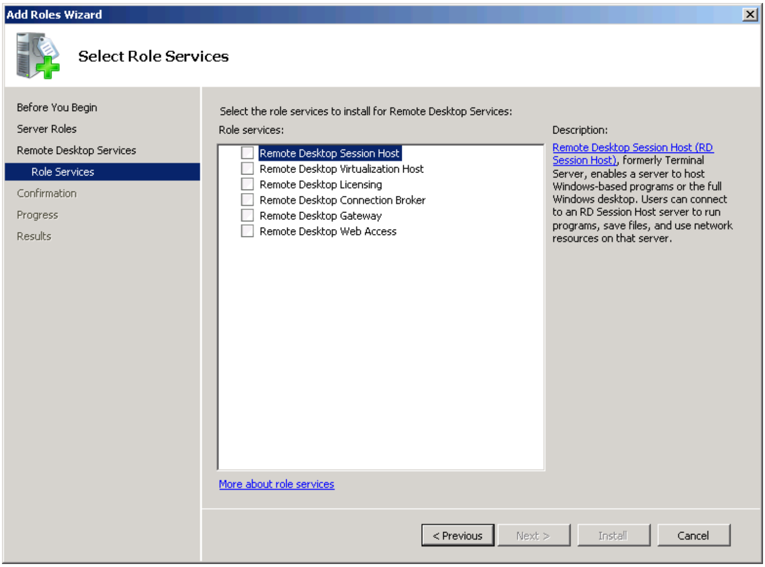
Things to Note

To allow remote connections for administrative purposes only, you do not have to install Remote Desktop Session Host. Instead, ensure that the Remote Desktop setting is enabled.

Additional Information

Overview of Remote Desktop Services

7. Click *Next*. For roles that include role services, the Select Role Services page appears, like the one shown here.



Select the role services to install for Remote Desktop Services:

Role services:

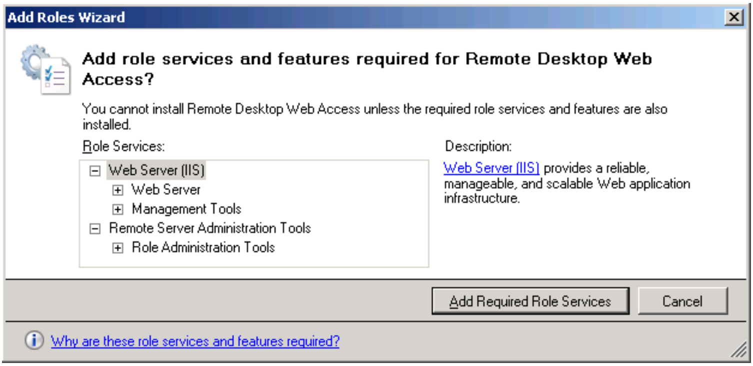
□ Remote Desktop Session Host
□ Remote Desktop Virtualization Host
□ Remote Desktop Licensing
□ Remote Desktop Connection Broker
□ Remote Desktop Gateway
□ Remote Desktop Web Access

Description:

Remote Desktop Session Host (RD Session Host), formerly Terminal Server, enables a server to host Windows-based programs or the full Windows desktop. Users can connect to an RD Session Host server to run programs, save files, and use network resources on that server.

8. Select the check boxes for the role services you want to install.

   Many roles and role services depend on other roles or features to function. For example, the Remote Desktop Web Access role service in the Remote Desktop Services role requires a web server, so an Add Role Services And Features Required For Remote Desktop Web Access dialog box appears, listing the dependent modules and offering to install them for you. Click *Add required role services* to select the dependent modules.



Add role services and features required for Remote Desktop Web Access?

You cannot install Remote Desktop Web Access unless the required role services and features are also installed.

Role Services:

- ⊟ Web Server (IIS)
  - ⊞ Web Server
  - ⊞ Management Tools
- ⊟ Remote Server Administration Tools
  - ⊞ Role Administration Tools

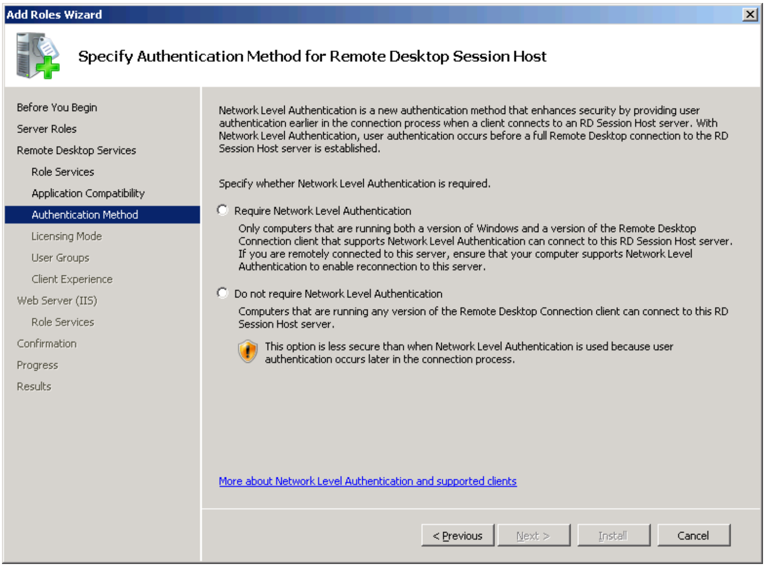
Description:

Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.

Why are these role services and features required?

9. Click *Next*. The next role-specific page appears.

   In most cases, the roles and role services you select for installation add pages to the wizard, like the one shown here, which you can use to configure role-specific parameters. Dependent roles and features can add their own configuration pages as well.



Specify Authentication Method for Remote Desktop Session Host

Network Level Authentication is a new authentication method that enhances security by providing user authentication earlier in the connection process when a client connects to an RD Session Host server. With Network Level Authentication, user authentication occurs before a full Remote Desktop connection to the RD Session Host server is established.

Specify whether Network Level Authentication is required.

○ Require Network Level Authentication

Only computers that are running both a version of Windows and a version of the Remote Desktop Connection client that supports Network Level Authentication can connect to this RD Session Host server. If you are remotely connected to this server, ensure that your computer supports Network Level Authentication to enable reconnection to this server.

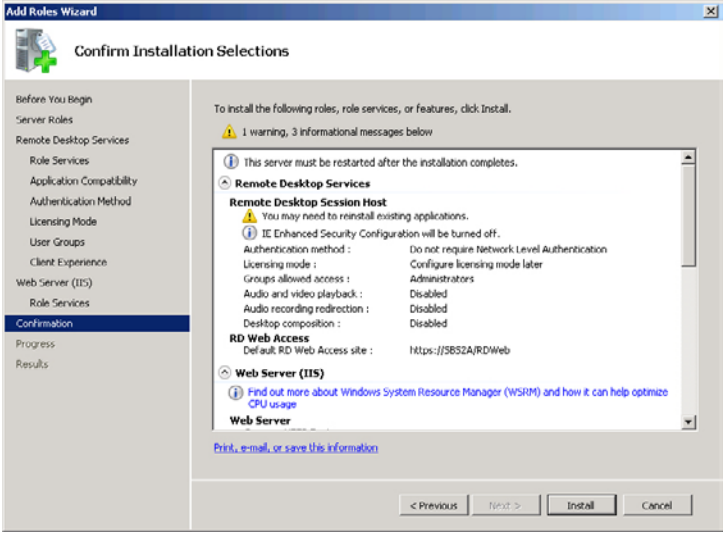
○ Do not require Network Level Authentication

Computers that are running any version of the Remote Desktop Connection client can connect to this RD Session Host server.

This option is less secure than when Network Level Authentication is used because user authentication occurs later in the connection process.

More about Network Level Authentication and supported clients

10. Complete all the role-specific pages in the wizard and click *Next*. The Confirm Installation Selections page appears, listing all the actions the wizard performs.



Confirm Installation Selections

To install the following roles, role services, or features, click Install.

⚠ 1 warning, 3 informational messages below

ⓘ This server must be restarted after the installation completes.

Remote Desktop Services

Remote Desktop Session Host

⚠ You may need to reinstall existing applications.

ⓘ IE Enhanced Security Configuration will be turned off.

```
Authentication method :        Do not require Network Level Authentication
Licensing mode :               Configure licensing mode later
Groups allowed access :        Administrators
Audio and video playback :     Disabled
Audio recording redirection :  Disabled
Desktop composition :          Disabled
```

RD Web Access

```
Default RD Web Access site :   https://SBS2A/RDWeb
```

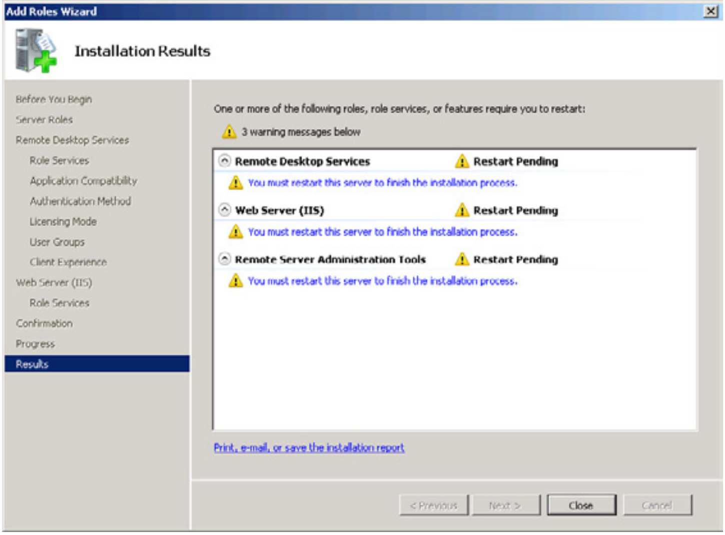
Web Server (IIS)

ⓘ Find out more about Windows System Resource Manager (WSRM) and how it can help optimize CPU usage

Web Server

Print, e-mail, or save this information

11. Click *Install*. The wizard displays an Installation Progress page as it installs and configures the selected modules. Then an Installation Results page appears, which might inform you that you must restart the server.



Installation Results

One or more of the following roles, role services, or features require you to restart:

⚠ 3 warning messages below

Remote Desktop Services ⚠ **Restart Pending**

⚠ You must restart this server to finish the installation process.

Web Server (IIS) ⚠ **Restart Pending**

⚠ You must restart this server to finish the installation process.

Remote Server Administration Tools ⚠ **Restart Pending**

⚠ You must restart this server to finish the installation process.

Print, e-mail, or save the installation report

12. Click *Close* and restart the server, if necessary.

Using Windows Server 2008 R2 Tools

Much of this book has been devoted to the administration and configuration tools specific to Windows SBS 2011, and especially the Windows SBS Console. However, Windows SBS 2011 is a superset of Windows Server 2008 R2 and includes all the tools normally supplied with the operating system. While the Windows SBS Console enables administrators to perform many of the basic functions required for everyday network maintenance, it is typical for them to move on to the more powerful Windows Server tools eventually. The following sections contain brief descriptions of the most commonly used Windows Server 2008 R2 administration tools.

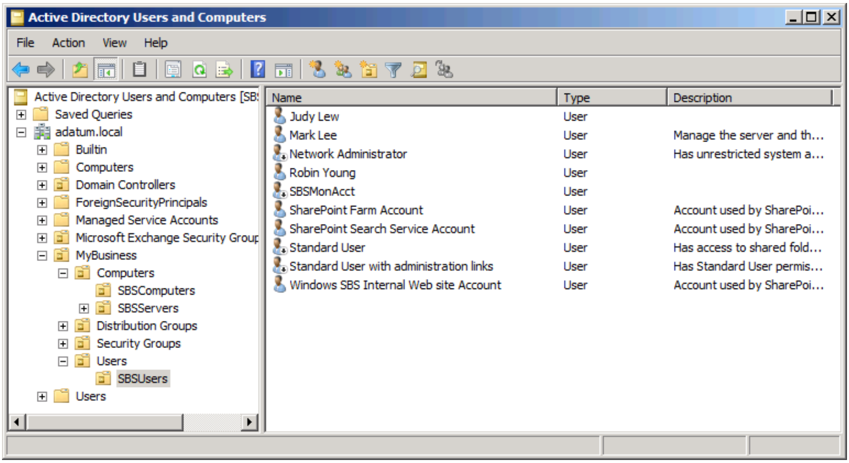
Using Active Directory Users and Computers

The Active Directory Users And Computers Console is the primary administration tool for AD DS. The console provides access to all the objects in the AD DS hierarchy and most of the attributes in each object. If you want to work with objects or attributes that do not appear in the Windows SBS Console, Active Directory Users and Computers provides a more comprehensive view.

> ***MORE INFO*** **For more information about AD DS objects and attributes, see the section entitled "An Active Directory Primer" in Chapter 6, "Working with Users, Computers, and Groups."**

Windows Server 2008 R2 installs the console on all domain controllers automatically; to run it on a computer that is not a domain controller, you can install the console using the Remote Server Administration Tools.

The Active Directory Users And Computers Console displays a hierarchical view of the AD DS domain to which you are currently attached, as shown in Figure 13-8. You can browse through the organizational units (OUs) in the domain to find and manage existing objects or create new ones. Double-clicking an object opens its Properties sheet, which, depending on the object type, can be simple or quite complex, and which provides access to the object's attributes.

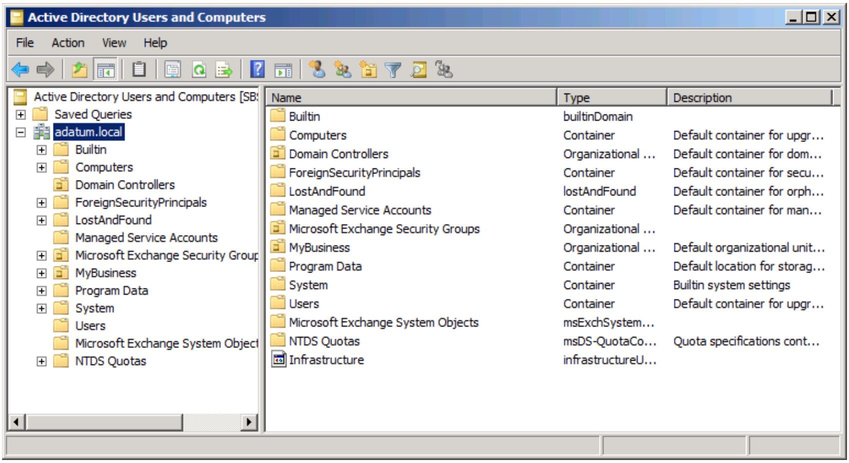


- Active Directory Users and Computers [SB
  - Saved Queries
  - adatum.local
    - Builtin
    - Computers
    - Domain Controllers
    - ForeignSecurityPrincipals
    - Managed Service Accounts
    - Microsoft Exchange Security Grour
    - MyBusiness
      - Computers
        - SBSComputers
        - SBSServers
      - Distribution Groups
      - Security Groups
      - Users
        - SBSUsers
    - Users

Name	Type	Description
Judy Lew	User	
Mark Lee	User	Manage the server and th...
Network Administrator	User	Has unrestricted system a...
Robin Young	User	
SBSMonAcct	User	
SharePoint Farm Account	User	Account used by SharePoi...
SharePoint Search Service Account	User	Account used by SharePoi...
Standard User	User	Has access to shared fold...
Standard User with administration links	User	Has Standard User permis...
Windows SBS Internal Web site Account	User	Account used by SharePoi...

FIGURE 13-8 The Active Directory Users And Computers Console.

To display all the objects and attributes in an AD DS domain, you must select *View > Advanced Features* in the console to display the interface shown in Figure 13-9.



- Active Directory Users and Computers [SB
  - Saved Queries
  - adatum.local
    - Builtin
    - Computers
    - Domain Controllers
    - ForeignSecurityPrincipals
    - LostAndFound
    - Managed Service Accounts
    - Microsoft Exchange Security Grour
    - MyBusiness
    - Program Data
    - System
    - Users
    - Microsoft Exchange System Object
    - NTDS Quotas

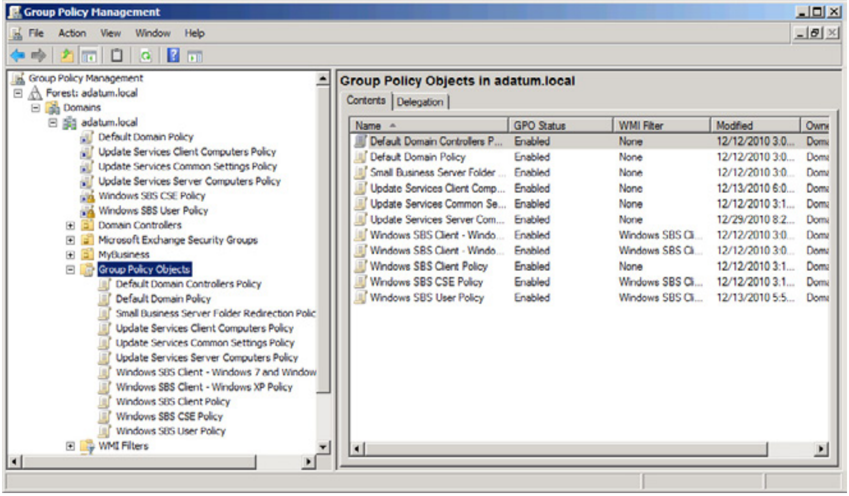
Name	Type	Description
Builtin	builtinDomain	
Computers	Container	Default container for upgr...
Domain Controllers	Organizational ...	Default container for dom...
ForeignSecurityPrincipals	Container	Default container for secu...
LostAndFound	lostAndFound	Default container for orph...
Managed Service Accounts	Container	Default container for man...
Microsoft Exchange Security Groups	Organizational ...	
MyBusiness	Organizational ...	Default organizational unit...
Program Data	Container	Default location for storag...
System	Container	Builtin system settings
Users	Container	Default container for upgr...
Microsoft Exchange System Objects	msExchSystem...	
NTDS Quotas	msDS-QuotaCo...	Quota specifications cont...
Infrastructure	infrastructureU...	

FIGURE 13-9 The Advanced Features display of the Active Directory User And Computers Console.

Using Group Policy Management

Group Policy is one of the most powerful and useful administrative tools provided with Windows SBS 2011 and Windows Server 2008 R2. Group Policy is essentially a method for deploying Windows registry settings to large numbers of users or computers on a network. Windows SBS 2011 uses Group Policy settings to configure several critical functions on your network workstations, including folder redirection, Windows Firewall, and the Windows Update client.

The Group Policy Management Console, shown in Figure 13-10, enables you to control the links between Group Policy objects (GPOs) and AD DS objects. GPOs contain the actual Group Policy settings, and linking them to AD DS domain, site, or OU objects deploys those settings to all the users and computers contained by those objects.


Group Policy Management
File
Action
View
Window
Help
Group Policy Management
Forest: adatum.local
Domains
adatum.local
Default Domain Policy
Update Services Client Computers Policy
Update Services Common Settings Policy
Update Services Server Computers Policy
Windows SBS CSE Policy
Windows SBS User Policy
Domain Controllers
Microsoft Exchange Security Groups
MyBusiness
Group Policy Objects
Default Domain Controllers Policy
Default Domain Policy
Small Business Server Folder Redirection Polic
Update Services Client Computers Policy
Update Services Common Settings Policy
Update Services Server Computers Policy
Windows SBS Client - Windows 7 and Window
Windows SBS Client - Windows XP Policy
Windows SBS Client Policy
Windows SBS CSE Policy
Windows SBS User Policy
WMI Filters
Contents
Delegation

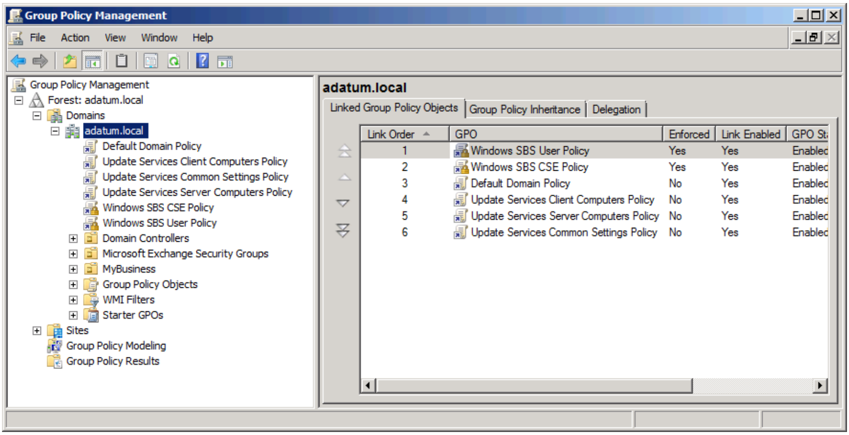
Group Policy Objects in adatum.local

Name	GPO Status	WMI Filter	Modified	Own
Default Domain Controllers P...	Enabled	None	12/12/2010 3:0...	Dom
Default Domain Policy	Enabled	None	12/12/2010 3:0...	Dom
Small Business Server Folder ...	Enabled	None	12/12/2010 3:0...	Dom
Update Services Client Comp...	Enabled	None	12/13/2010 6:0...	Dom
Update Services Common Se...	Enabled	None	12/12/2010 3:1...	Dom
Update Services Server Com...	Enabled	None	12/29/2010 8:2...	Dom
Windows SBS Client - Windo...	Enabled	Windows SBS Cli...	12/12/2010 3:0...	Dom
Windows SBS Client - Windo...	Enabled	Windows SBS Cli...	12/12/2010 3:0...	Dom
Windows SBS Client Policy	Enabled	None	12/12/2010 3:1...	Dom
Windows SBS CSE Policy	Enabled	Windows SBS Cli...	12/12/2010 3:1...	Dom
Windows SBS User Policy	Enabled	Windows SBS Cli...	12/13/2010 5:5...	Dom

FIGURE 13-10 The Group Policy Management Console.

Windows SBS 2011 creates a number of GPOs for its own use, including the Default Domain Policy and Default Domain Controllers Policy objects. Although you can modify the settings in these GPOs for your own use, the best practice is to create your own GPOs and link them to your domain or OU objects as needed. You can link multiple GPOs to a single AD DS object, and the users and computers receiving the settings apply them in the order you specify.

For example, by default Windows SBS 2011 links six different GPOs to your AD DS domain, which are numbered 1 to 6 in the Group Policy Management Console, as shown in Figure 13-11. Each user and computer in the domain applies the settings in the number 6 GPO, Update Services Common Settings Policy, followed by the settings in GPO number 5, number 4, and so forth. If two GPOs contain different values for the same settings, the settings applied later overwrite the existing ones. This way, the settings in the number 1 GPO, which the users and computers apply last, always take precedence over those with higher numbers.



- Group Policy Management
  - Forest: adatum.local
    - Domains
      - adatum.local
        - Default Domain Policy
        - Update Services Client Computers Policy
        - Update Services Common Settings Policy
        - Update Services Server Computers Policy
        - Windows SBS CSE Policy
        - Windows SBS User Policy
        - Domain Controllers
        - Microsoft Exchange Security Groups
        - MyBusiness
        - Group Policy Objects
        - WMI Filters
        - Starter GPOs
    - Sites
    - Group Policy Modeling
    - Group Policy Results

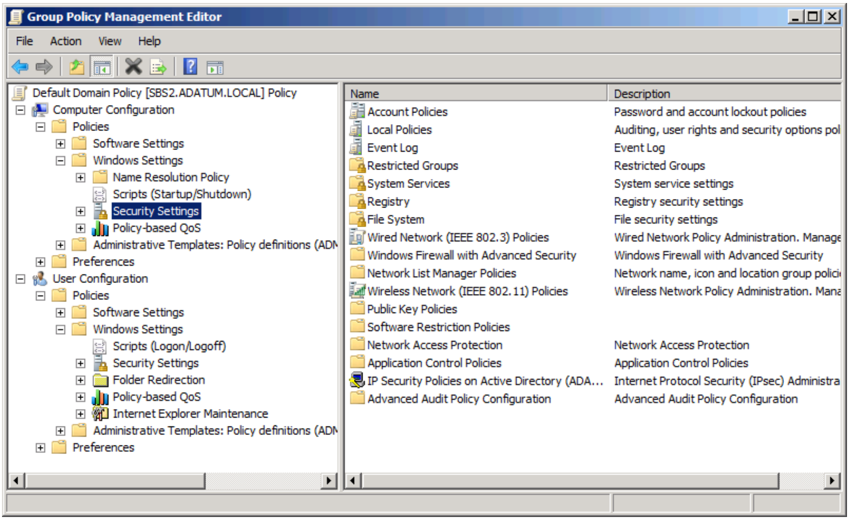
adatum.local

Linked Group Policy Objects | Group Policy Inheritance | Delegation

Link Order	GPO	Enforced	Link Enabled	GPO St
1	Windows SBS User Policy	Yes	Yes	Enabled
2	Windows SBS CSE Policy	Yes	Yes	Enabled
3	Default Domain Policy	No	Yes	Enabled
4	Update Services Client Computers Policy	No	Yes	Enabled
5	Update Services Server Computers Policy	No	Yes	Enabled
6	Update Services Common Settings Policy	No	Yes	Enabled

FIGURE 13-11 The GPOs linked to a Windows SBS 2011 domain.

To modify the settings in a GPO, or to create settings in a new GPO, you use the Group Policy Management Editor Console, as shown in Figure 13-12. Each GPO has separate settings for computers, which clients apply when the computer starts, and users, which apply when a user logs on to the domain. Each of the hundreds of settings has a dialog box that contains the controls you use to configure its value. In many cases, settings have three possible values: enabled, which explicitly activates the setting; disabled, which explicitly deactivates it; and undefined, which does nothing to modify the setting's existing value, if any.



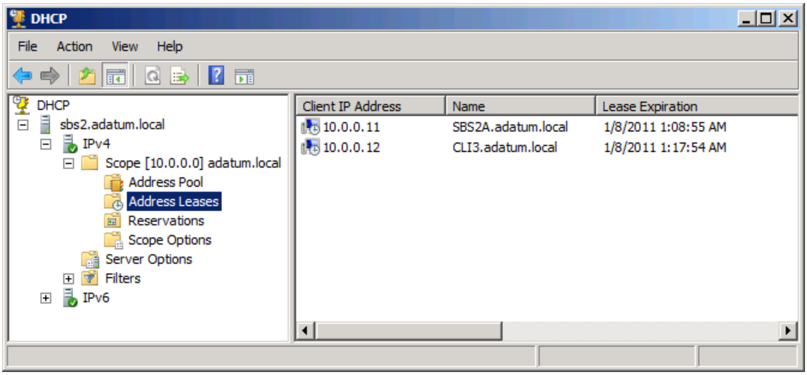
- Default Domain Policy [SBS2.ADATUM.LOCAL] Policy
  - Computer Configuration
    - Policies
      - Software Settings
      - Windows Settings
        - Name Resolution Policy
        - Scripts (Startup/Shutdown)
        - Security Settings
        - Policy-based QoS
      - Administrative Templates: Policy definitions (ADM
    - Preferences
  - User Configuration
    - Policies
      - Software Settings
      - Windows Settings
        - Scripts (Logon/Logoff)
        - Security Settings
        - Folder Redirection
        - Policy-based QoS
        - Internet Explorer Maintenance
      - Administrative Templates: Policy definitions (ADM
    - Preferences

Name	Description
Account Policies	Password and account lockout policies
Local Policies	Auditing, user rights and security options pol
Event Log	Event Log
Restricted Groups	Restricted Groups
System Services	System service settings
Registry	Registry security settings
File System	File security settings
Wired Network (IEEE 802.3) Policies	Wired Network Policy Administration. Manage
Windows Firewall with Advanced Security	Windows Firewall with Advanced Security
Network List Manager Policies	Network name, icon and location group polici
Wireless Network (IEEE 802.11) Policies	Wireless Network Policy Administration. Mana
Public Key Policies	
Software Restriction Policies	
Network Access Protection	Network Access Protection
Application Control Policies	Application Control Policies
IP Security Policies on Active Directory (ADA...	Internet Protocol Security (IPsec) Administra
Advanced Audit Policy Configuration	Advanced Audit Policy Configuration

FIGURE 13-12 The Group Policy Management Editor Console.

Using DHCP

When you run the Connect To The Internet Wizard on your Windows SBS 2011 primary server, the wizard configures the Dynamic Host Configuration Protocol (DHCP) server to provide Internet Protocol (IP) addresses and other Transmission Control Protocol/Internet Protocol (TCP/IP) settings to the computers on your network. You should not have to modify DHCP server settings manually unless you expand your network by installing additional DHCP servers on other computers. If this is the case, however, you can configure the DHCP Server service using the DHCP Console, as shown in Figure 13-13.



Client IP Address	Name	Lease Expiration
10.0.0.11	SBS2A.adatum.local	1/8/2011 1:08:55 AM
10.0.0.12	CLI3.adatum.local	1/8/2011 1:17:54 AM

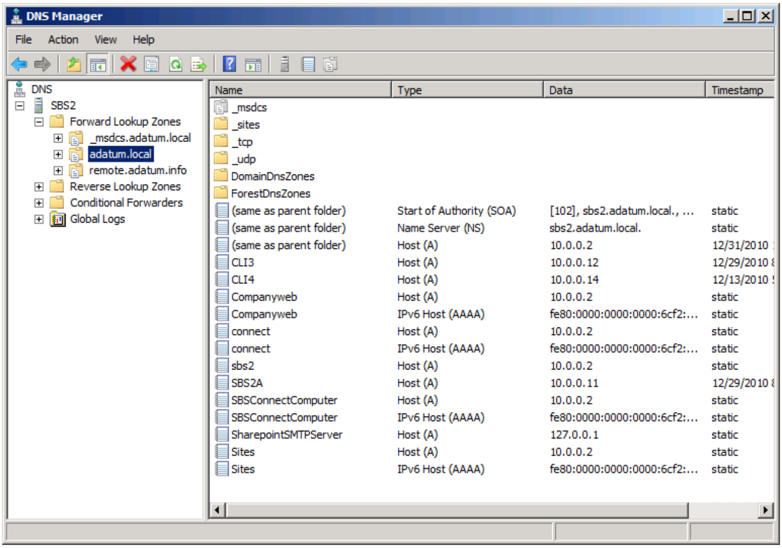
FIGURE 13-13 The DHCP Console.

> ***MORE INFO*** **For more information on DHCP, see the section entitled "Connecting to the Internet" in Chapter 4, "Getting Started."**

If your network includes remote sites with servers, you might want to configure them to function as additional DHCP servers. To do this, you must install the DHCP Server role using the Server Manager Console and create a scope using a different IP subnet than the one on your primary server. You can create the scope using the Add Roles Wizard in Server Manager or the New Scope Wizard in the DHCP Console. You must also add scope options to configure other TCP/IP settings, such as the Router and DNS Servers options, which provide your clients with their Default Gateway and Preferred DNS Server values.

Using DNS Manager

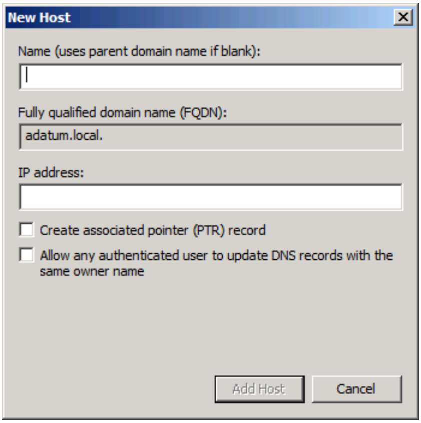
Windows SBS 2011 installs the Domain Name System (DNS) service on your primary server, as is required for AD DS, and automatically creates resource records for the computers on your network. To modify existing resource records or create new ones, you use the DNS Manager Console, as shown in Figure 13-14.



Name	Type	Data	Timestamp
_msdcs			
_sites			
_tcp			
_udp			
DomainDnsZones			
ForestDnsZones			
(same as parent folder)	Start of Authority (SOA)	[102], sbs2.adatum.local., ...	static
(same as parent folder)	Name Server (NS)	sbs2.adatum.local.	static
(same as parent folder)	Host (A)	10.0.0.2	12/31/2010
CLI3	Host (A)	10.0.0.12	12/29/2010
CLI4	Host (A)	10.0.0.14	12/13/2010
Companyweb	Host (A)	10.0.0.2	static
Companyweb	IPv6 Host (AAAA)	fe80:0000:0000:0000:6cf2:...	static
connect	Host (A)	10.0.0.2	static
connect	IPv6 Host (AAAA)	fe80:0000:0000:0000:6cf2:...	static
sbs2	Host (A)	10.0.0.2	static
SBS2A	Host (A)	10.0.0.11	12/29/2010
SBSConnectComputer	Host (A)	10.0.0.2	static
SBSConnectComputer	IPv6 Host (AAAA)	fe80:0000:0000:0000:6cf2:...	static
SharepointSMTPServer	Host (A)	127.0.0.1	static
Sites	Host (A)	10.0.0.2	static
Sites	IPv6 Host (AAAA)	fe80:0000:0000:0000:6cf2:...	static

FIGURE 13-14 The DNS Manager Console.

A DNS server is essentially a database of resource records, most of which contain computer names and their equivalent IP addresses. In Windows SBS 2011, the DNS server stores the records as part of the AD DS database. Creating a new resource record is a matter of choosing a record type and supplying the information required for that type, using a dialog box like the one shown in Figure 13-15. For example, if you want to create a new website on your server, you can assign it a unique name by creating a new Host (A) resource record pointing to the server's IP address and then using the name from the resource record as the host header value when you create the site in Internet Information Services (IIS).



Name (uses parent domain name if blank):

Fully qualified domain name (FQDN):
adatum.local.

IP address:

□ Create associated pointer (PTR) record

□ Allow any authenticated user to update DNS records with the same owner name

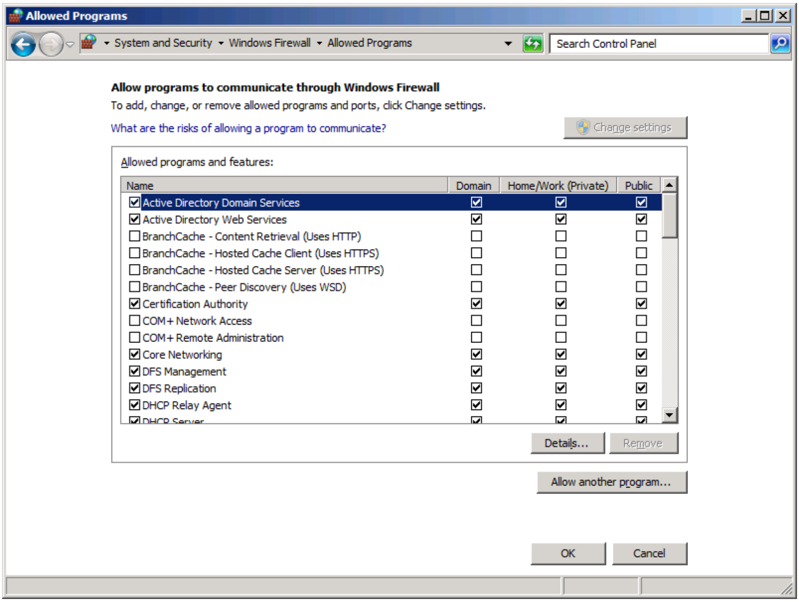
FIGURE 13-15 The New Host dialog box in the DNS Manager Console.

MORE INFO **For more information on the Domain Name System, see the section entitled "Understanding Domains" in Chapter 2, "A Networking Primer."**

Using Windows Firewall

During the operating system installation, the Windows SBS 2011 setup program configures Windows Firewall to open the ports that the system's various applications and services require. However, if you install or enable additional software on the server, you might have to open additional ports. For example, as noted earlier in this chapter, you might have to modify the firewall configuration to use an MMC Console to administer another computer.

You can use two tools to configure Windows Firewall. The first is the Windows Firewall Control panel, which enables you to open the Allowed Programs Control panel, as shown in Figure 13-16. By selecting programs in this dialog box, you can open ports that enable specific types of traffic to pass through the firewall.



Allow programs to communicate through Windows Firewall

To add, change, or remove allowed programs and ports, click Change settings.

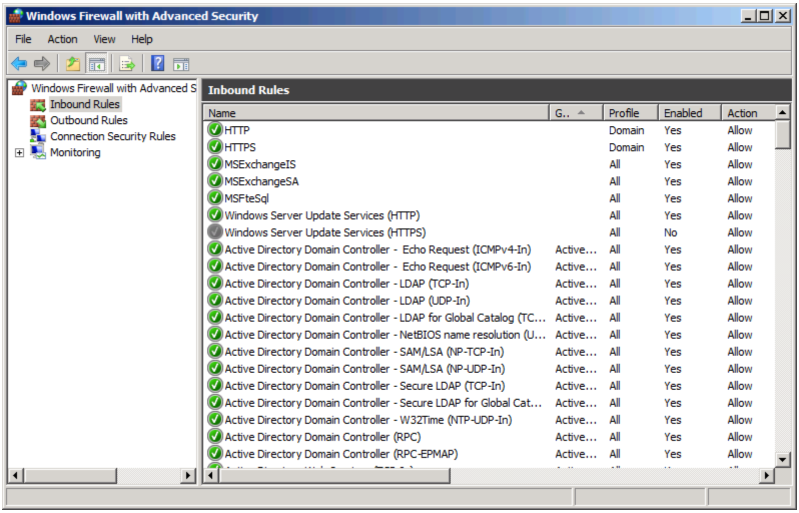
What are the risks of allowing a program to communicate?

Allowed programs and features:

Name	Domain	Home/Work (Private)	Public
☑ Active Directory Domain Services	☑	☑	☑
☑ Active Directory Web Services	☑	☑	☑
□ BranchCache - Content Retrieval (Uses HTTP)	□	□	□
□ BranchCache - Hosted Cache Client (Uses HTTPS)	□	□	□
□ BranchCache - Hosted Cache Server (Uses HTTPS)	□	□	□
□ BranchCache - Peer Discovery (Uses WSD)	□	□	□
☑ Certification Authority	☑	☑	☑
□ COM+ Network Access	□	□	□
□ COM+ Remote Administration	□	□	□
☑ Core Networking	☑	☑	☑
☑ DFS Management	☑	☑	☑
☑ DFS Replication	☑	☑	☑
☑ DHCP Relay Agent	☑	☑	☑
☑ DHCP Server	☑	☑	☑

FIGURE 13-16 The Allowed Programs Control panel.

For more detailed control over the firewall, you can use the Windows Firewall With Advanced Security Console, as shown in Figure 13-17. This console presents firewall settings as rules, which you can apply to inbound or outbound traffic. The allowed programs in the Windows Firewall Control panel are actually collections of rules.


Windows Firewall with Advanced Security
File
Action
View
Help
Windows Firewall with Advanced S
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring

Inbound Rules

Name	G..	Profile	Enabled	Action
HTTP		Domain	Yes	Allow
HTTPS		Domain	Yes	Allow
MSExchangeIS		All	Yes	Allow
MSExchangeSA		All	Yes	Allow
MSFteSql		All	Yes	Allow
Windows Server Update Services (HTTP)		All	Yes	Allow
Windows Server Update Services (HTTPS)		All	No	Allow
Active Directory Domain Controller - Echo Request (ICMPv4-In)	Active...	All	Yes	Allow
Active Directory Domain Controller - Echo Request (ICMPv6-In)	Active...	All	Yes	Allow
Active Directory Domain Controller - LDAP (TCP-In)	Active...	All	Yes	Allow
Active Directory Domain Controller - LDAP (UDP-In)	Active...	All	Yes	Allow
Active Directory Domain Controller - LDAP for Global Catalog (TC...	Active...	All	Yes	Allow
Active Directory Domain Controller - NetBIOS name resolution (U...	Active...	All	Yes	Allow
Active Directory Domain Controller - SAM/LSA (NP-TCP-In)	Active...	All	Yes	Allow
Active Directory Domain Controller - SAM/LSA (NP-UDP-In)	Active...	All	Yes	Allow
Active Directory Domain Controller - Secure LDAP (TCP-In)	Active...	All	Yes	Allow
Active Directory Domain Controller - Secure LDAP for Global Cat...	Active...	All	Yes	Allow
Active Directory Domain Controller - W32Time (NTP-UDP-In)	Active...	All	Yes	Allow
Active Directory Domain Controller (RPC)	Active...	All	Yes	Allow
Active Directory Domain Controller (RPC-EPMAP)	Active...	All	Yes	Allow

FIGURE 13-17 The Windows Firewall With Advanced Security Console.

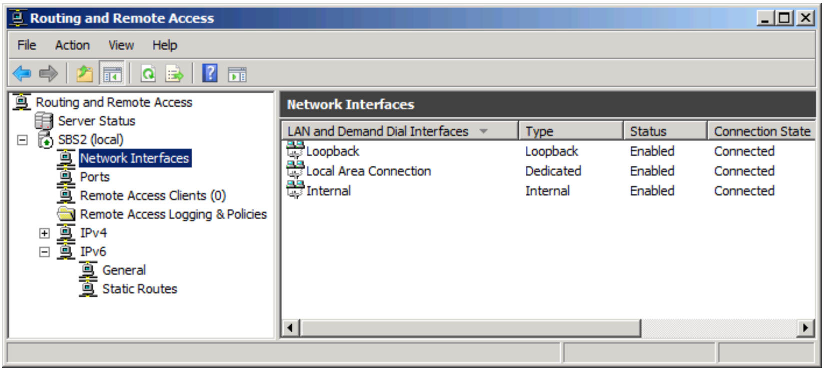
Using the Windows Firewall With Advanced Security Console, you can enable or disable the individual rules that comprise the allowed program, rather than configure the program exception as a whole. You can also create your own rules that filter traffic based on programs, services, IP addresses, and/or port numbers.

Using Routing and Remote Access

The Routing and Remote Access Service (RRAS) in Windows Server 2008 R2 enables you to configure a server's routing capabilities. You can conceivably use a server to connect two local area networks (LANs) together, but Windows SBS 2011 allows its primary server to have only one network interface adapter. The server accesses the Internet through a standalone router on the network.

However, you can use the RRAS to configure a server on your network to function as a *virtual private network (VPN)* server. A VPN is a secure remote connection to your network that uses the Internet as a network medium. For example, a user at home or on the road can connect to a local Internet service provider (ISP) and establish a VPN connection to your server. To secure the connection, the computers use a technique called *tunneling*, which encapsulates their traffic in specially encrypted packets.

To configure RRAS on your primary server, you use the Routing And Remote Access Console, shown in Figure 13-18. To enable VPN access to your network, you must configure your router to allow the traffic in from the Internet, and configure your server to respond to connection requests from remote clients by running the Routing And Remote Access Server Setup Wizard. Once a VPN client is connected to the server, the user can access network resources just as though he or she were sitting at a workstation on the network.



LAN and Demand Dial Interfaces	Type	Status	Connection State
Loopback	Loopback	Enabled	Connected
Local Area Connection	Dedicated	Enabled	Connected
Internal	Internal	Enabled	Connected

FIGURE 13-18 The Routing And Remote Access Console.

> ***TIP*** **You can configure another server running Windows Server 2008 R2 to function as a VPN server, but first you must install the Network Policy and Access Services role using the Server Manager Console, selecting the Routing and Remote Access role service in the process.**

CHAPTER 14

Monitoring Windows SBS 2011

Keeping track of how your computers are performing is part of the job of every network administrator, and Windows Small Business Server (SBS) 2011 provides many tools that enable you to monitor the activities of your network computers without having to leave your workstation.

Using Windows SBS Console Monitoring

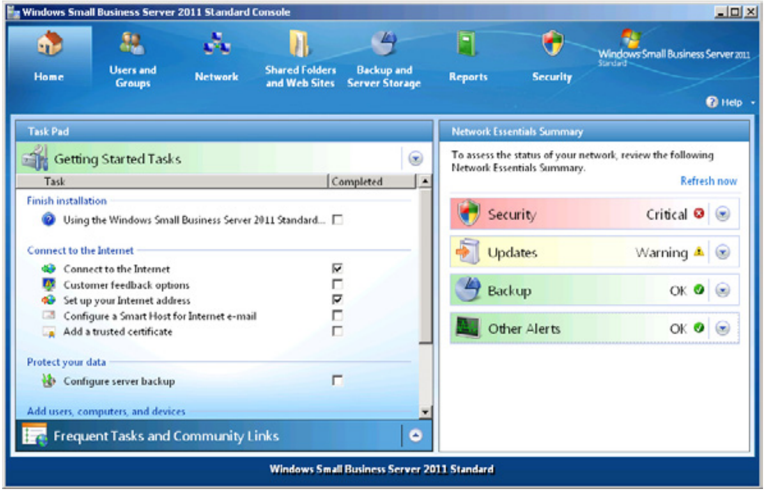
As you have seen in previous chapters, the Windows SBS Console provides administrators with many of the most vital Windows SBS controls and settings, leaving the details and comprehensive access to the standard Windows Server 2008 R2 tools. The same is true when it comes to monitoring and reporting. The console can provide administrators with basic real-time monitoring, programmed alerts, and reports that it generates on a regular basis.

Using the Network Essentials Summary

On the Home page of the Windows SBS Console, as shown in Figure 14-1, the Network Essentials Summary pane provides a high-level, real-time view of four basic performance areas:

- **Security** Checks for the presence of virus and spyware protection, as well as active firewalls, on both your servers and workstations
- **Updates** Makes sure that Windows Server Update Services (WSUS) is running and that all the network servers and workstations have the latest updates installed

- **Backup** Checks to see that the server is configured to perform regular backups and whether the backups are completing successfully
- **Other alerts** Checks for a variety of other conditions, including Error events in the System log, required services that are not running, and other important system status alerts


Windows Small Business Server 2011 Standard Console
Home
Users and Groups
Network
Shared Folders and Web Sites
Backup and Server Storage
Reports
Security
Windows Small Business Server 2011 Standard
Help
Task Pad
Network Essentials Summary
Refresh now
Frequent Tasks and Community Links
Windows Small Business Server 2011 Standard

Getting Started Tasks

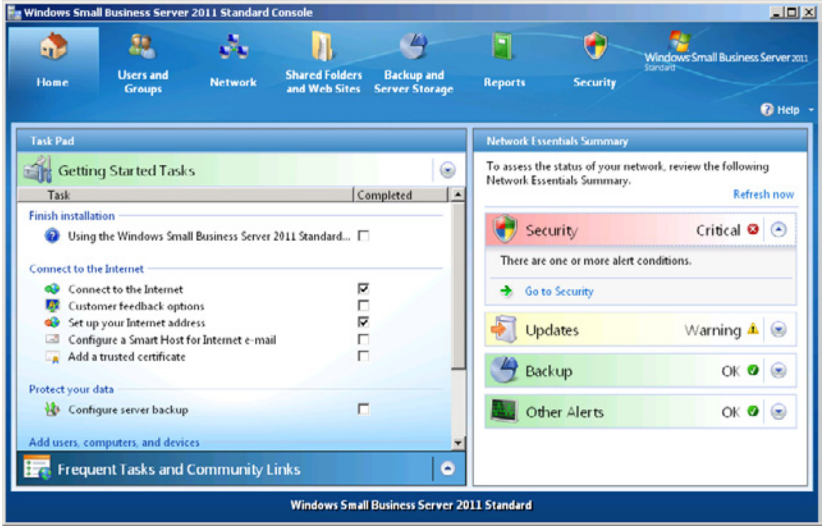
Task	Completed
Finish installation	
Using the Windows Small Business Server 2011 Standard...	□
Connect to the Internet	
Connect to the Internet	☑
Customer feedback options	□
Set up your Internet address	☑
Configure a Smart Host for Internet e-mail	□
Add a trusted certificate	□
Protect your data	
Configure server backup	□
Add users, computers, and devices	

To assess the status of your network, review the following Network Essentials Summary.

Security	Critical
Updates	Warning
Backup	OK
Other Alerts	OK

FIGURE 14-1 The Home page of the Windows SBS Console.

Each of the four areas in the Network Essentials Summary pane has a status indicator with a colored icon specifying the current status of the area: *OK* (green check mark), *Warning* (yellow exclamation point), or *Critical* (red X). There is also an arrow in each area that you can click to display more information about the network's current condition and expose a link to a console page providing more detailed information, as shown in Figure 14-2.


Windows Small Business Server 2011 Standard Console
Home
Users and Groups
Network
Shared Folders and Web Sites
Backup and Server Storage
Reports
Security
Windows Small Business Server 2011 Standard
Help
Task Pad
Getting Started Tasks
Frequent Tasks and Community Links
Network Essentials Summary
Refresh now
Go to Security
Windows Small Business Server 2011 Standard

Task	Completed
Finish installation	
Using the Windows Small Business Server 2011 Standard...	□
Connect to the Internet	
Connect to the Internet	☑
Customer feedback options	□
Set up your Internet address	☑
Configure a Smart Host for Internet e-mail	□
Add a trusted certificate	□
Protect your data	
Configure server backup	□
Add users, computers, and devices	

To assess the status of your network, review the following Network Essentials Summary.

Security	Critical
Updates	Warning
Backup	OK
Other Alerts	OK

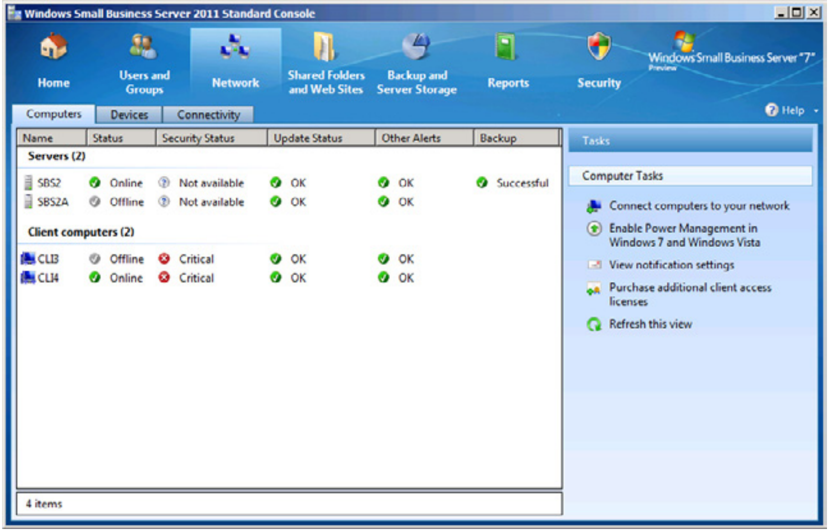
There are one or more alert conditions.

FIGURE 14-2 An expanded Networking Essentials Summary area display.

Unfortunately, the conditions that trigger a change in these status displays are not configurable. If, for example, you have deliberately stopped one of the services on your server that Windows SBS considers to be essential, the *Other alerts* status always appears as *Critical*, and clicking the arrow only tells you that one of your servers has reported an alert. You have to click the *Go to computers* link and seek more information about the problem before you can determine whether the alert concerns the stopped service you know about or a new condition.

Using Notification Settings

When you click *Network* in the Windows SBS Console and select the *Computers* tab, as shown in Figure 14-3, you see a list of the computers on your network, a column specifying whether each computer is online, and indicators providing the same four categories of information as in the Network Essentials Summary pane. The difference here is that you have a separate set of indicators for each computer, while the Network Essentials Summary pane condenses the information for the entire network into four indicators.


Windows Small Business Server 2011 Standard Console
Home
Users and Groups
Network
Shared Folders and Web Sites
Backup and Server Storage
Reports
Security
Windows Small Business Server "7" Preview
Computers
Devices
Connectivity
Help
Tasks
Computer Tasks
Connect computers to your network
Enable Power Management in Windows 7 and Windows Vista
View notification settings
Purchase additional client access licenses
Refresh this view

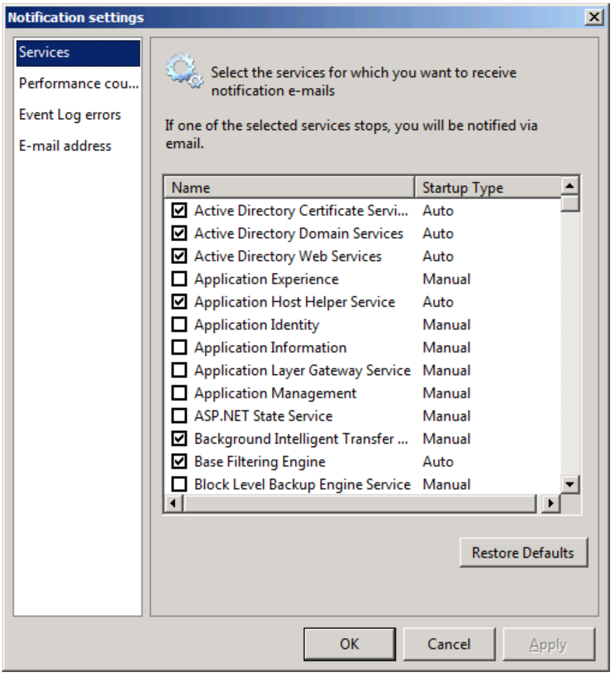
Name	Status	Security Status	Update Status	Other Alerts	Backup
Servers (2)					
SBS2	Online	Not available	OK	OK	Successful
SBS2A	Offline	Not available	OK	OK	
Client computers (2)					
CLI3	Offline	Critical	OK	OK	
CLI4	Online	Critical	OK	OK	

4 items

FIGURE 14-3 The *Network/Computers* tab in the Windows SBS Console.

From this page, you can also configure Windows SBS 2011 to send email notifications to you, or anyone else, when certain events occur. To set up email notifications, follow these steps:

1. Log on to your Windows SBS 2011 primary server, using an account with network Administrator privileges. The Windows SBS Console appears.
2. Click *Network*, and then select the *Computers* tab.
3. From the *Tasks* list, select *View notification settings*. The Notification Settings dialog box appears.
4. On the *Services* tab, select the system services that you want to trigger an email notification when they shut down.



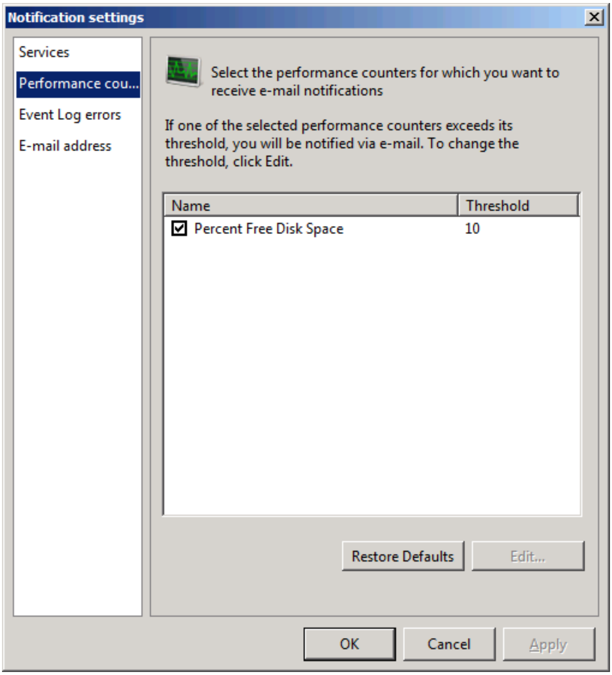
Select the services for which you want to receive notification e-mails

If one of the selected services stops, you will be notified via email.

Name	Startup Type
☑ Active Directory Certificate Servi...	Auto
☑ Active Directory Domain Services	Auto
☑ Active Directory Web Services	Auto
□ Application Experience	Manual
☑ Application Host Helper Service	Auto
□ Application Identity	Manual
□ Application Information	Manual
□ Application Layer Gateway Service	Manual
□ Application Management	Manual
□ ASP.NET State Service	Manual
☑ Background Intelligent Transfer ...	Manual
☑ Base Filtering Engine	Auto
□ Block Level Backup Engine Service	Manual

NOTE **Certain service failures can render the server unable to send any email messages at all, in which case the system sends no email notifications.**

5. Click the *Performance counters* tab, and specify whether you want the system to send an email notification when the amount of free disk space on the server drops below 10 percent of its capacity. You can also modify the default threshold by clicking *Edit* and specifying a different value in the *Change threshold to* text box.



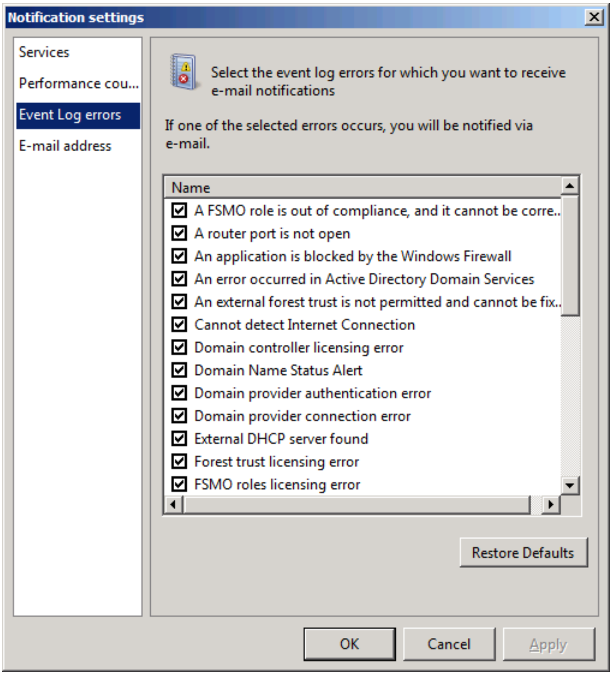
Select the performance counters for which you want to receive e-mail notifications

If one of the selected performance counters exceeds its threshold, you will be notified via e-mail. To change the threshold, click Edit.

Name	Threshold
☑ Percent Free Disk Space	10

MORE INFO In Windows, performance counters are registers that track specific statistics pertaining to certain hardware or software components. Unfortunately, this interface supports only one of the hundreds of counters available. To track other counter values, you must use the Performance Monitor Console, as described later in this chapter.

6. Click the *Event log errors* tab and specify which event types should trigger an email notification.

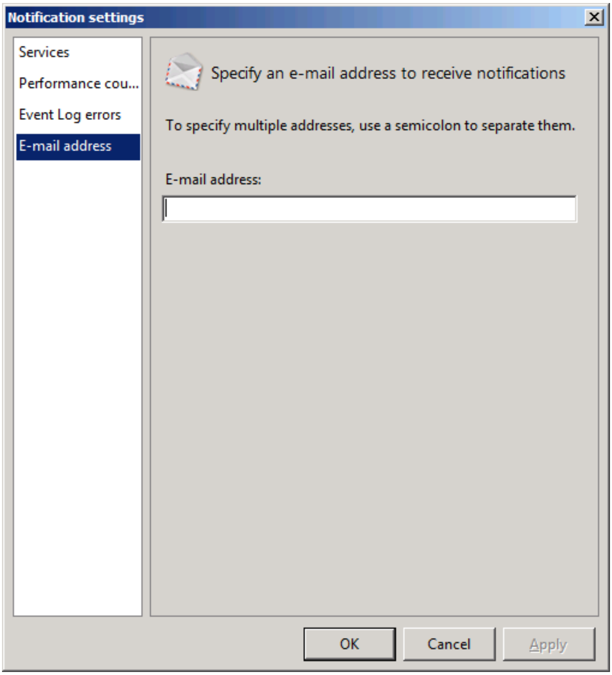


Select the event log errors for which you want to receive e-mail notifications

If one of the selected errors occurs, you will be notified via e-mail.

Name
☑ A FSMO role is out of compliance, and it cannot be corre...
☑ A router port is not open
☑ An application is blocked by the Windows Firewall
☑ An error occurred in Active Directory Domain Services
☑ An external forest trust is not permitted and cannot be fix...
☑ Cannot detect Internet Connection
☑ Domain controller licensing error
☑ Domain Name Status Alert
☑ Domain provider authentication error
☑ Domain provider connection error
☑ External DHCP server found
☑ Forest trust licensing error
☑ FSMO roles licensing error

7. Click the *E-mail address* tab, and in the *E-mail address* text box, specify the addresses of the individuals you want to receive notifications. You can use local or Internet email addresses, separating multiple addresses with semicolons.


Notification settings

Specify an e-mail address to receive notifications

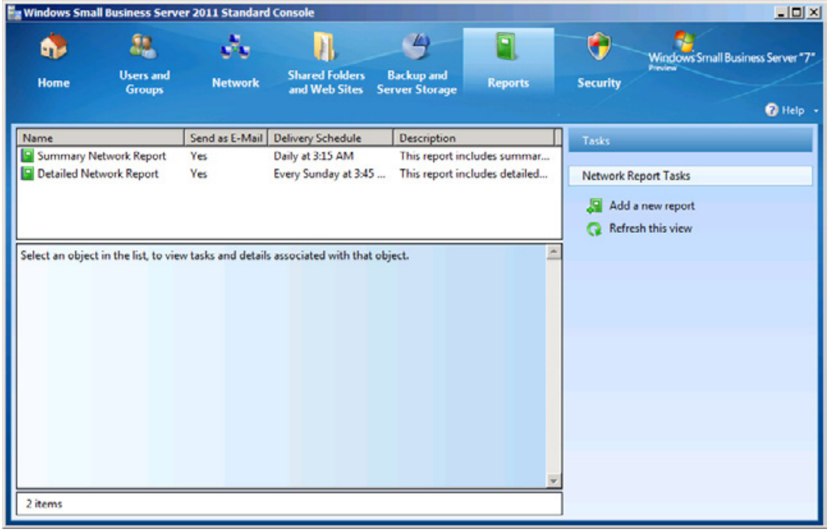
To specify multiple addresses, use a semicolon to separate them.

E-mail address:

8. Click *OK* to close the Notification Settings dialog box.

Creating and Viewing Reports

Another way to monitor Windows SBS network activity is to create reports. When you click *Reports* in the Windows SBS Console, you see the interface shown in Figure 14-4, which displays the two reports that Windows SBS 2011 creates by default.


Windows Small Business Server 2011 Standard Console
Home
Users and Groups
Network
Shared Folders and Web Sites
Backup and Server Storage
Reports
Security
Windows Small Business Server "7" Preview
Help
Tasks
Network Report Tasks
Add a new report
Refresh this view

Name	Send as E-Mail	Delivery Schedule	Description
Summary Network Report	Yes	Daily at 3:15 AM	This report includes summar...
Detailed Network Report	Yes	Every Sunday at 3:45 ...	This report includes detailed...

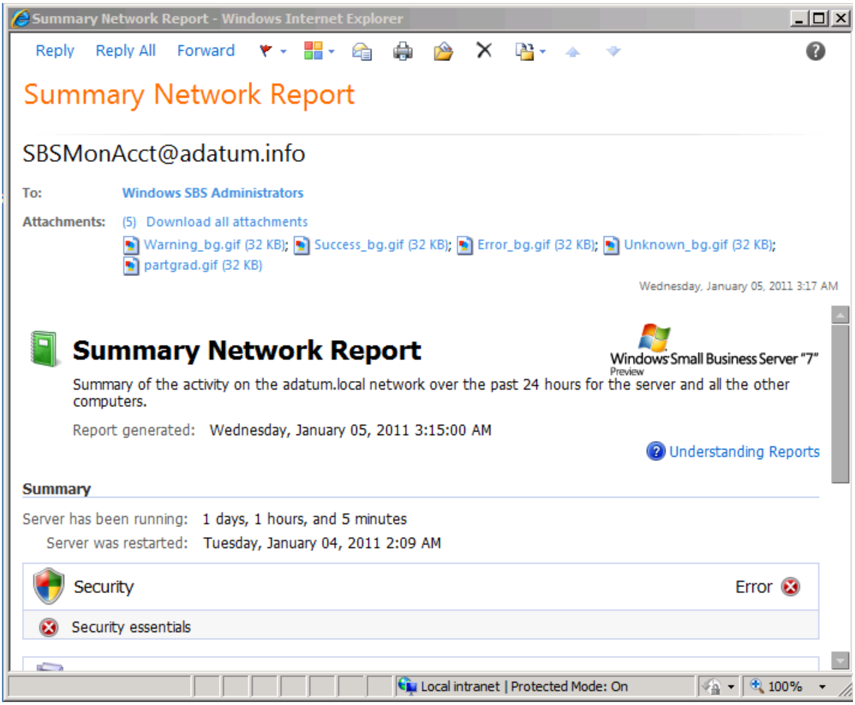
Select an object in the list, to view tasks and details associated with that object.

2 items

FIGURE 14-4 The Reports page in the Windows SBS Console.

The reports that the Windows SBS Console generates are expanded versions of the *Network essentials summary* that appears on the console's Home page, captured at a specific time. By default, Windows SBS runs a *Summary network report* each day at 3:15 A.M. and a *Detailed network report* each Sunday at 3:45 A.M., and emails them both to the Windows SBS Administrators distribution group. You can modify the schedule for these reports as needed, as well as their contents and their recipients. You can also create your own reports.

The *Summary network report*, as shown in Figure 14-5, displays the status of six system areas, which include the same *Security*, *Updates*, *Backup*, and *Other alerts* areas as the *Network essentials summary*; plus two more: *E-mail usage and mailbox sizes* and *Server event logs*. For each area that has an *Error* status, the report includes a one-line summary of the basic problem. In nearly all cases, the summary report can indicate that a problem exists, but administrators must consult other server resources to determine the source and nature of the problem.



Summary Network Report - Windows Internet Explorer
Reply
Reply All
Forward
Local intranet | Protected Mode: On
100%

Summary Network Report

SBSMonAcct@adatum.info

To: Windows SBS Administrators

Attachments: (5) Download all attachments
Warning_bg.gif (32 KB); Success_bg.gif (32 KB); Error_bg.gif (32 KB); Unknown_bg.gif (32 KB); partgrad.gif (32 KB)

Wednesday, January 05, 2011 3:17 AM

Summary Network Report

Windows Small Business Server "7" Preview

Summary of the activity on the adatum.local network over the past 24 hours for the server and all the other computers.

Report generated: Wednesday, January 05, 2011 3:15:00 AM

Understanding Reports

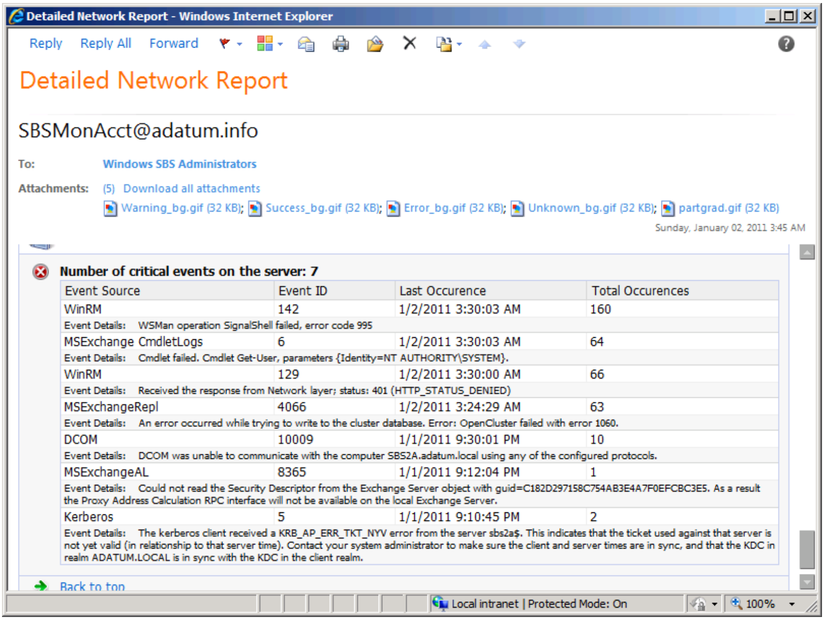
Summary

Server has been running: 1 days, 1 hours, and 5 minutes
Server was restarted: Tuesday, January 04, 2011 2:09 AM

Security — Error ☒
☒ Security essentials

FIGURE 14-5 A Summary Network Report generated by Windows SBS 2011.

The Detailed Network Report, as shown in Figure 14-6, covers the same six areas, but provides more information for each one, regardless of its status. The detailed report includes statistics, policy settings, and key error messages that can often provide administrators with enough information to diagnose a problem without having to consult other resources.


Detailed Network Report - Windows Internet Explorer
Reply
Reply All
Forward
Back to top
Local intranet | Protected Mode: On
100%

Detailed Network Report

SBSMonAcct@adatum.info

To: Windows SBS Administrators

Attachments: (5) Download all attachments
Warning_bg.gif (32 KB); Success_bg.gif (32 KB); Error_bg.gif (32 KB); Unknown_bg.gif (32 KB); partgrad.gif (32 KB)

Sunday, January 02, 2011 3:45 AM

Number of critical events on the server: 7

Event Source	Event ID	Last Occurence	Total Occurences
WinRM	142	1/2/2011 3:30:03 AM	160
Event Details: WSMan operation SignalShell failed, error code 995			
MSExchange CmdletLogs	6	1/2/2011 3:30:03 AM	64
Event Details: Cmdlet failed. Cmdlet Get-User, parameters {Identity=NT AUTHORITY\SYSTEM}.			
WinRM	129	1/2/2011 3:30:00 AM	66
Event Details: Received the response from Network layer; status: 401 (HTTP_STATUS_DENIED)			
MSExchangeRepl	4066	1/2/2011 3:24:29 AM	63
Event Details: An error occurred while trying to write to the cluster database. Error: OpenCluster failed with error 1060.			
DCOM	10009	1/1/2011 9:30:01 PM	10
Event Details: DCOM was unable to communicate with the computer SBS2A.adatum.local using any of the configured protocols.			
MSExchangeAL	8365	1/1/2011 9:12:04 PM	1
Event Details: Could not read the Security Descriptor from the Exchange Server object with guid=C182D297158C754AB3E4A7F0EFCBC3E5. As a result the Proxy Address Calculation RPC interface will not be available on the local Exchange Server.			
Kerberos	5	1/1/2011 9:10:45 PM	2
Event Details: The kerberos client received a KRB_AP_ERR_TKT_NYV error from the server sbs2a$. This indicates that the ticket used against that server is not yet valid (in relationship to that server time). Contact your system administrator to make sure the client and server times are in sync, and that the KDC in realm ADATUM.LOCAL is in sync with the KDC in the client realm.			

FIGURE 14-6 A Detailed Network Report generated by Windows SBS 2011.

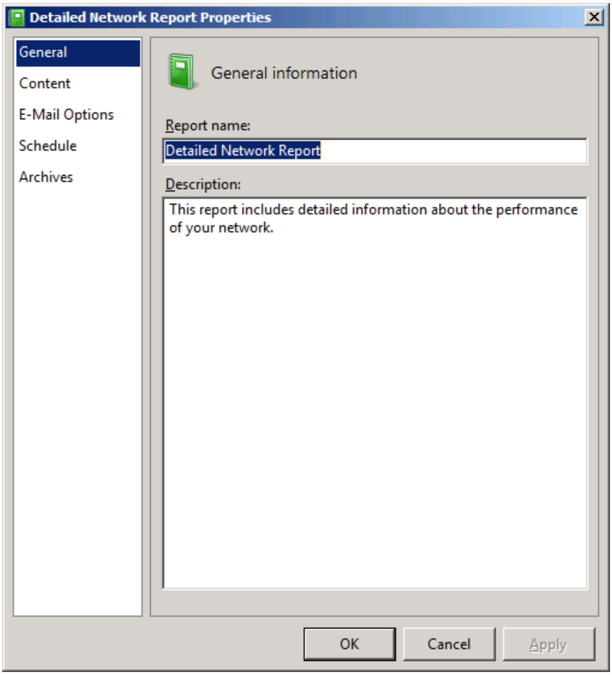
> ***CAUTION*** **Remember that both of these reports reflect the condition of the network at the time that the system generated them. By the time you read the reports, some conditions might have changed.**

Modifying the Default Reports

The Detailed Network Report begins with a *Summary* section that is identical to the Summary Network Report, followed by a *Details* section. Because the system does not take very long to generate either report, you might want to consider modifying the default schedules to generate the detailed report every day instead of once per week.

To modify the schedule of the Detailed Network Report, perform the following:

1. Log on to your Windows SBS 2011 primary server, using an account with network Administrator privileges. The Windows SBS Console appears.
2. Click *Reports*.
3. Select *Detailed network report* and, from the *Tasks* list, click *View report properties*. The Detailed Network Report Properties sheet appears.



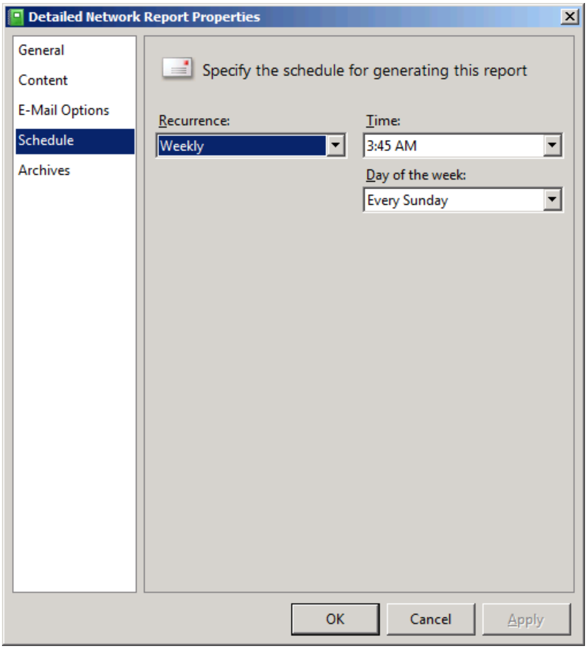
Detailed Network Report Properties

General information

Report name: Detailed Network Report

Description: This report includes detailed information about the performance of your network.

4. Click the *Schedule* tab.



Specify the schedule for generating this report

Recurrence: Weekly

Time: 3:45 AM

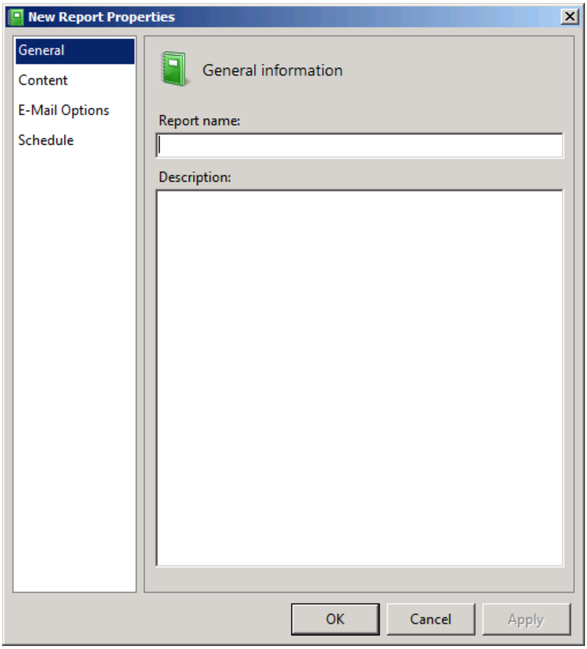
Day of the week: Every Sunday

5. From the *Recurrence* drop-down list, select *Daily*. From the *Time* drop-down list, select a different time for the report to run, if desired.
6. Click *OK*.

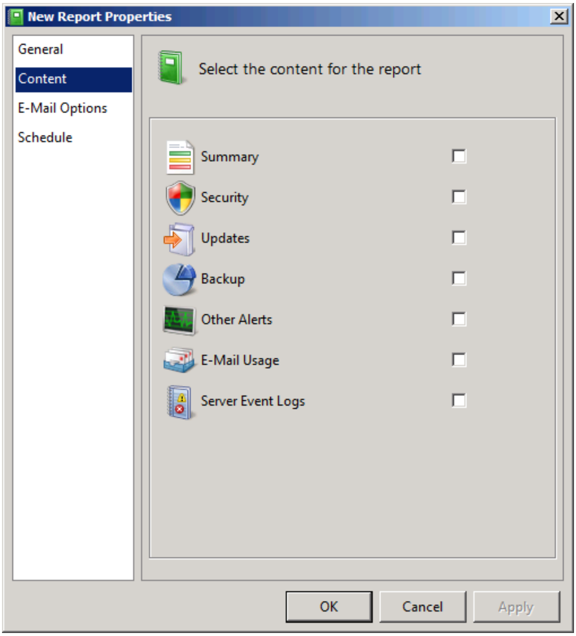
Creating New Reports

In addition to modifying the default reports, you can create new reports that contain information on specific areas and run at specified times, which the system supplies to specific users via email. To create a new report, follow this procedure:

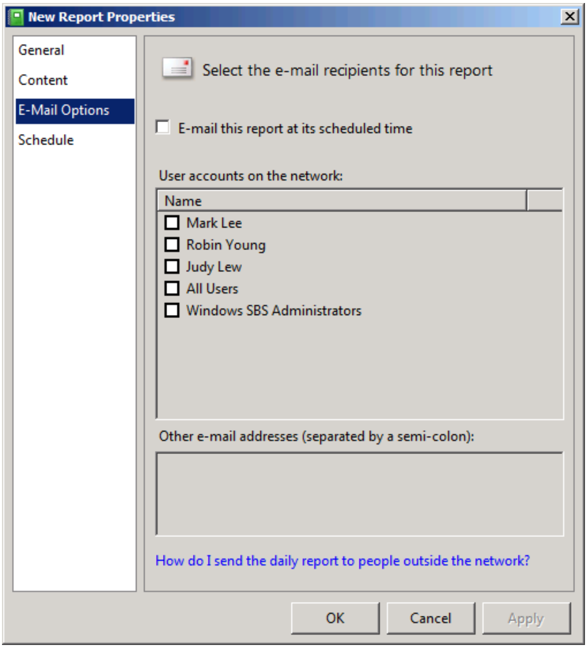
1. Log on to your Windows SBS 2011 primary server, using an account with network Administrator privileges. The Windows SBS Console appears.
2. Click *Reports*.
3. From the *Tasks* list, select *Add a new report*. The New Report Properties sheet appears.



4. In the *Report name* text box, type the name you want to assign to the report. Then click the *Content* tab.



5. Select the check boxes for the areas that you want to include in the report and click the *E-Mail options* tab.


New Report Properties

Select the e-mail recipients for this report

□ E-mail this report at its scheduled time

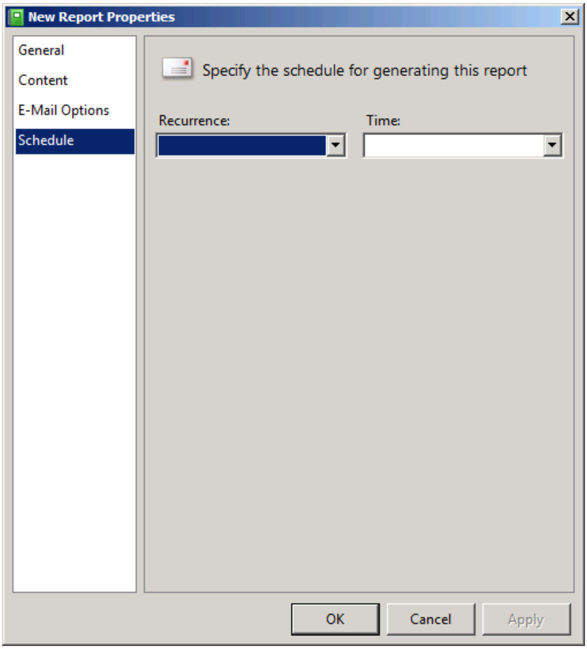
User accounts on the network:

Name
□ Mark Lee
□ Robin Young
□ Judy Lew
□ All Users
□ Windows SBS Administrators

Other e-mail addresses (separated by a semi-colon):

How do I send the daily report to people outside the network?

6. Select the *E-Mail this report at its scheduled time* check box and select the check boxes for the internal users or groups that you want to receive the report. You can also type other email addresses in the *Other e-mail addresses (separated by a semi-colon)* text box, if desired. Then, click the *Schedule* tab.



Specify the schedule for generating this report

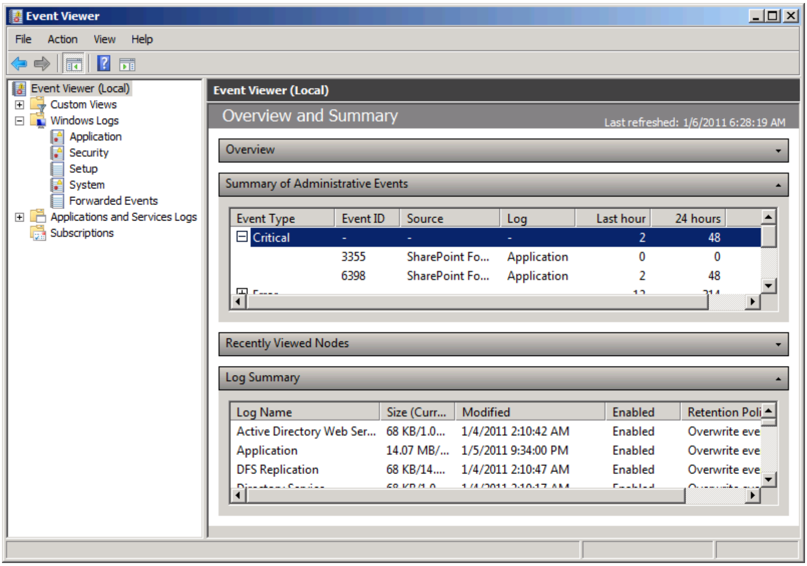
Recurence:

Time:

7. In the *Recurrence* drop-down list, specify whether you want the system to run the report daily or weekly. From the *Time* drop-down list, select the time of day that you want the system to generate the report. If you chose the *Weekly* option, select a value in the *Day of the week* drop-down list.
8. Click *OK*. The new report appears on the Reports page.

Using Event Viewer

Several Windows SBS 2011 tools, including the Windows SBS Console and the Server Manager Console, display selected entries from the Windows event logs, but to view these logs in their entirety, you must use the Event Viewer Console, shown in Figure 14-7.



Event Type	Event ID	Source	Log	Last hour	24 hours
⊟ Critical	-	-	-	2	48
	3355	SharePoint Fo...	Application	0	0
	6398	SharePoint Fo...	Application	2	48

Log Name	Size (Curr...	Modified	Enabled	Retention Poli
Active Directory Web Ser...	68 KB/1.0...	1/4/2011 2:10:42 AM	Enabled	Overwrite eve
Application	14.07 MB/...	1/5/2011 9:34:00 PM	Enabled	Overwrite eve
DFS Replication	68 KB/14....	1/4/2011 2:10:47 AM	Enabled	Overwrite eve

FIGURE 14-7 The Event Viewer Console.

Viewing Event Logs

The Windows Eventing engine is responsible for monitoring system activities on all Windows computers and recording information about those activities in various logs. Each log contains a series of entries called *events*. The Event Viewer Console is simply an application that displays those events in various formats.

To launch Event Viewer, you can use any one of the five methods:

- Click *Start*. Then click *Administrative Tools* > *Event Viewer.*
- Click *Start*. Then click *Control Panel* > *System and Security* > *Administrative Tools*, and double-click *Event viewer.*
- Open a blank Microsoft Management Console (MMC) and add the Event Viewer snap-in.
- Click *Start* and type **Event Viewer** or **Eventvwr.msc** in the search box.
- Open the Computer Management Console and expand the *Event viewer* node.

The *Overview* and *Summary* display that appears in the console by default lists the most recently occurring events by type. The Windows Eventing engine creates events of several types:

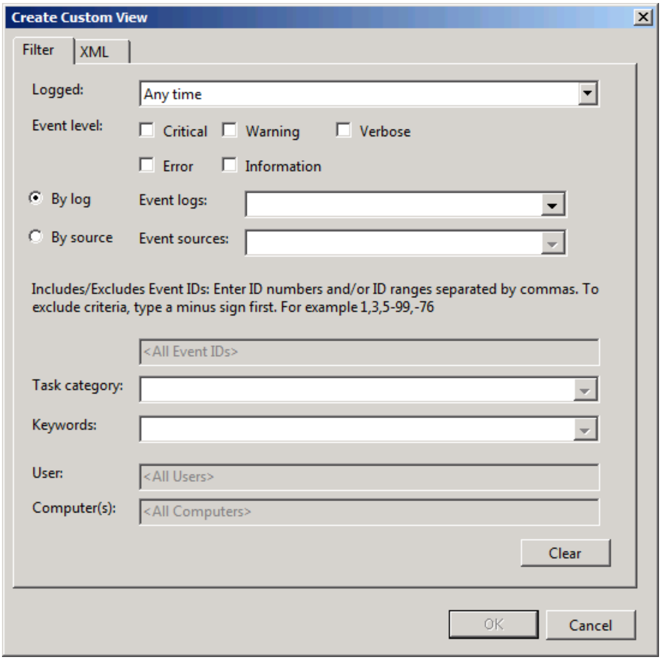
- **Critical** Warns that an incident resulting in a catastrophic loss of functionality or data in a component or process has occurred
- **Error** Warns of a problem that is not likely to affect the performance of the component or process where the problem occurred, but which could affect the performance of other system components or processes
- **Warning** Warns of a service degradation or an occurrence that can potentially cause a service degradation in the near future unless an administrator takes steps to prevent it
- **Information** Describes a change in the state of a component or process as part of a normal operation
- **Audit Success** Indicates the successful completion of a system process or activity for which an audit policy is active

In addition to a chronological display by type, Event Viewer can also display the most current events in each of the following individual logs, regardless of type:

- **Application** Contains information about specific programs running on the computer, as determined by the application developer.
- **Security** Contains information about security-related events, such as failed logons, attempts to access protected resources, and success or failure of audited events. The events recorded in this log are determined by audit policies, which you can enable using either local computer policies or Group Policy.
- **Setup** Contains information about the operating system installation and setup history.
- **System** Contains information about events generated by the operating system, such as service start and device driver load failures.
- **Forwarded vents** Contains events received from other computers on the network via subscriptions.

Using Other Event Viewer Functions

In addition to providing access to the main Windows logs, the Event Viewer Console displays logs for individual applications and services, and enables you to create custom logs containing events of specific types, from specific sources, and from specific time periods by using the Create Custom View dialog box shown in Figure 14-8.



Logged: Any time

Event level: □ Critical □ Warning □ Verbose □ Error □ Information

● By log Event logs:

○ By source Event sources:

Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

<All Event IDs>

Task category:

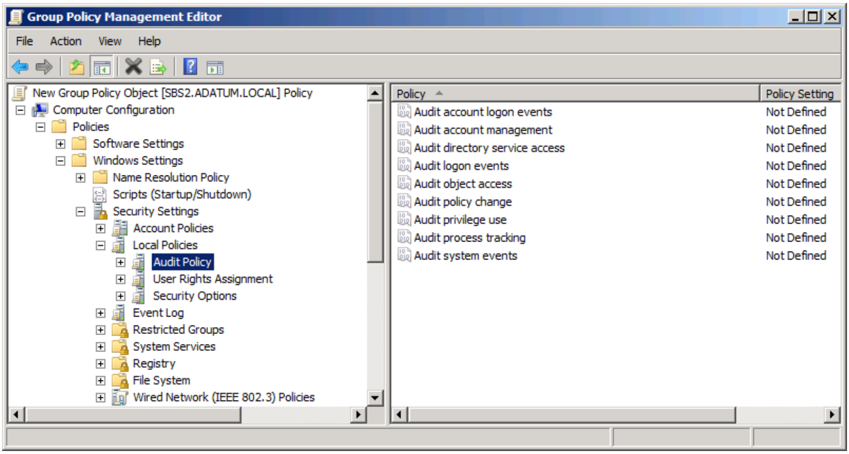
Keywords:

User: <All Users>

Computer(s): <All Computers>

FIGURE 14-8 The Create Custom View dialog box, from the Event Viewer Console.

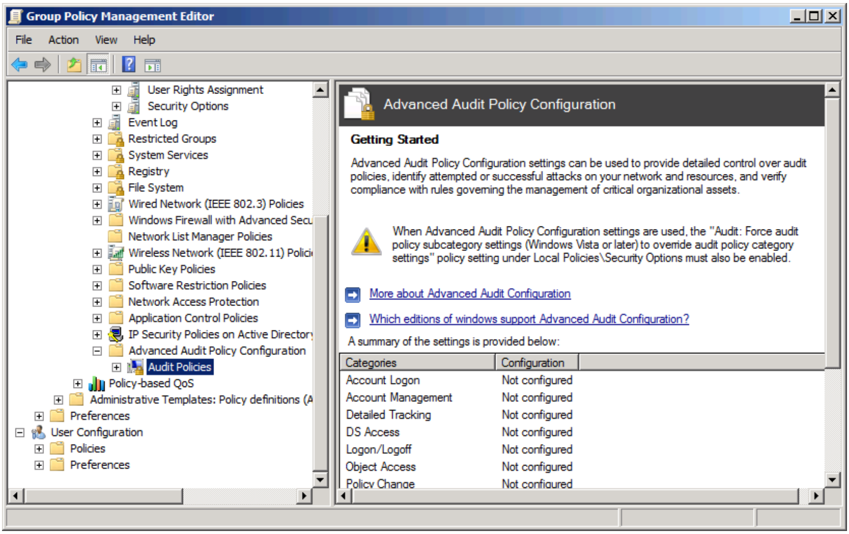
Another powerful feature of the Event Viewer Console is the ability to audit the success or failure of specific system events, such as account logons and modifications to AD DS objects. For example, you can modify logon failures to determine if someone is making repeated attempts to guess a user's password. To use auditing, you must enable specific Group Policy settings, as shown in Figure 14-9. When the system detects one of the selected events, it creates an entry in the *Security* log, which you can evaluate later.



Policy	Policy Setting
Audit account logon events	Not Defined
Audit account management	Not Defined
Audit directory service access	Not Defined
Audit logon events	Not Defined
Audit object access	Not Defined
Audit policy change	Not Defined
Audit privilege use	Not Defined
Audit process tracking	Not Defined
Audit system events	Not Defined

FIGURE 14-9 The Audit Policy settings in the Group Policy Management Editor Console.

Windows Server 2008 R2 also includes an *Advanced audit policy configuration* node in its GPOs, which enables you to monitor Windows 7 system activities on a more granular level, as shown in Figure 14-10.


Group Policy Management Editor
File Action View Help
User Rights Assignment
Security Options
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Secu
Network List Manager Policies
Wireless Network (IEEE 802.11) Polici
Public Key Policies
Software Restriction Policies
Network Access Protection
Application Control Policies
IP Security Policies on Active Director
Advanced Audit Policy Configuration
Audit Policies
Policy-based QoS
Administrative Templates: Policy definitions (A
Preferences
User Configuration
Policies
Preferences

Advanced Audit Policy Configuration

Getting Started

Advanced Audit Policy Configuration settings can be used to provide detailed control over audit policies, identify attempted or successful attacks on your network and resources, and verify compliance with rules governing the management of critical organizational assets.

When Advanced Audit Policy Configuration settings are used, the "Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings" policy setting under Local Policies\Security Options must also be enabled.

More about Advanced Audit Configuration

Which editions of windows support Advanced Audit Configuration?

A summary of the settings is provided below:

Categories	Configuration
Account Logon	Not configured
Account Management	Not configured
Detailed Tracking	Not configured
DS Access	Not configured
Logon/Logoff	Not configured
Object Access	Not configured
Policy Change	Not configured

FIGURE 14-10 The *Advanced audit policy configuration* node in the Group Policy Management Editor Console.

BEST PRACTICES **Some audit policies, such as *Audit system events*, can generate a large number of entries in a short period of time. This is one reason why auditing is not enabled by default. In most cases, the best practice is to turn auditing on for brief periods and then turn it off again, making sure that you have enough storage space for the *Security* log file.**

Using Performance Monitor

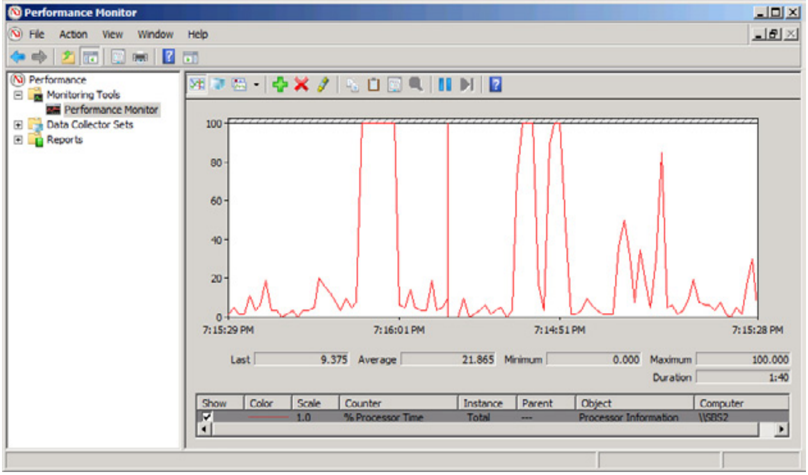
The performance level of a server running Windows SBS 2011 changes as it performs various combinations of tasks. Monitoring the performance of the computer's various components over a period of time is the only way to get a true picture of the system's capabilities. The Windows SBS Console can provide you with a snapshot of the server's condition at a specific moment in time, but the Performance Monitor snap-in enables you to view much of the same information on a continuous, real-time basis.

Like Event Viewer, Performance Monitor is an MMC snap-in that you can launch in a variety of ways, including these:

- Click *Start*. Then click *Administrative Tools > Performance Monitor*.
- Click *Start*; then click *Control Panel > System and Security > Administrative Tools* and double-click *Performance monitor*.
- Open a blank MMC console and add the Performance Monitor snap-in.
- Click *Start* and type **Perfmon.msc** in the search box.
- Open the Computer Management Console and expand the *Performance monitor* node.

Performance Monitor is a tool that can display information for hundreds of different statistics (called *performance counters*) in a variety of ways. You can use Performance Monitor to create a customized graph or report containing any statistics you choose.

When you open the Performance Monitor snap-in, expand the *Monitoring tools* node, and select *Performance monitor*, the Detail pane of the snap-in contains a line graph, updated in real time, showing the current level for the % Processor Time performance counter, as shown in Figure 14-11.



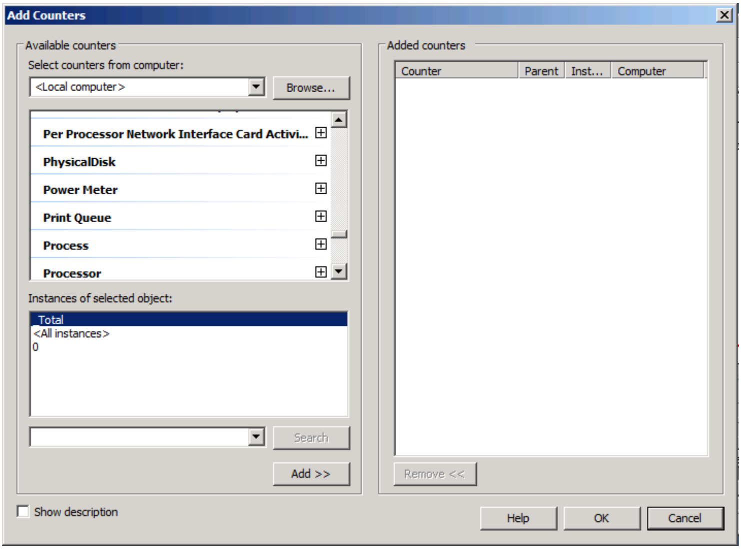
Last 9.375 Average 21.865 Minimum 0.000 Maximum 100.000
Duration 1:40

Show	Color	Scale	Counter	Instance	Parent	Object	Computer
☑	—	1.0	% Processor Time	Total	---	Processor Information	\\SBS2

FIGURE 14-11 The default display of the Performance Monitor snap-in.

Adding Counters

The % Processor Time performance counter that appears in the default Performance Monitor configuration is a useful gauge of the computer's performance, but the snap-in also includes hundreds of other counters that you can add to the display. To add counters to the Performance Monitor display, click the *Add* button in the toolbar or press Ctrl+I to display the Add Counters dialog box, as shown in Figure 14-12.



Select counters from computer: <Local computer>

Per Processor Network Interface Card Activi...
PhysicalDisk
Power Meter
Print Queue
Process
Processor

Instances of selected object:
Total
<All instances>
0

Counter	Parent	Inst...	Computer

□ Show description

FIGURE 14-12 The Add Counters dialog box.

NOTE Unlike most MMC snap-ins, Performance Monitor does not insert its most commonly used functions into the MMC Console's Action menu. The only methods for accessing Performance Monitor functions are the toolbar buttons, hotkey combinations, and the context menu that appears when you right-click the display.

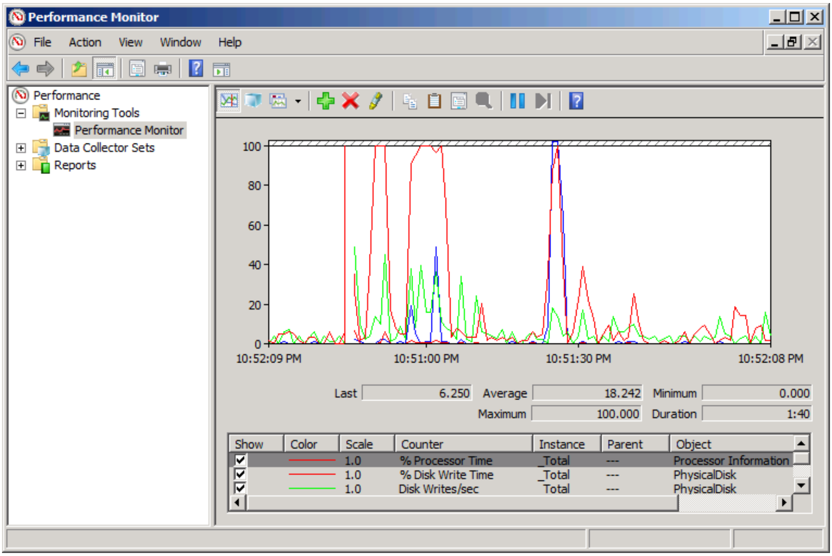
In this dialog box, you have to specify the following four pieces of information to add a counter to the display:

- **Computer** The name of the computer you want to monitor using the specified performance counter.

  NOTE Unlike most MMC snap-ins, you cannot redirect the entire focus of Performance Monitor to another computer on the network. Instead, you specify a computer name for each counter you add to the display. This enables you to create a display showing counters for various computers on the network, such as a single graph showing the processor activity for all of your workstations.

- **Performance object** A category of performance objects that represents a specific hardware or software component in the computer. Clicking the plus sign for a performance object displays the performance counters related to that component.
- **Performance counter** A statistic representing a specific aspect of the selected performance object's activities.
- **Instance** An element representing a specific occurrence of the selected performance counter. For example, on a computer with two network interface adapters, each counter in the Network Interface performance object has two instances, one for each adapter, enabling you to track the performance of each adapter individually. Some counters also have instances such as Total or Average, enabling you to track the performance of all the instances combined or the median value of all instances.

Once you have selected all of the required elements defining a performance counter instance, click *Add* to copy it to the *Added counters* list. The dialog box remains open so you can add more counters as needed. Click *OK* when you are finished to update the graph with your selected counters. When you add new counters to the Performance Monitor snap-in, they appear in the legend at the bottom of the screen, and lines representing their values are added to the display, as shown in Figure 14-13.



Last 6.250 Average 18.242 Minimum 0.000
Maximum 100.000 Duration 1:40

Show	Color	Scale	Counter	Instance	Parent	Object
☑	🟥	1.0	% Processor Time	_Total	---	Processor Information
☑	🟥	1.0	% Disk Write Time	_Total	---	PhysicalDisk
☑	🟩	1.0	Disk Writes/sec	_Total	---	PhysicalDisk

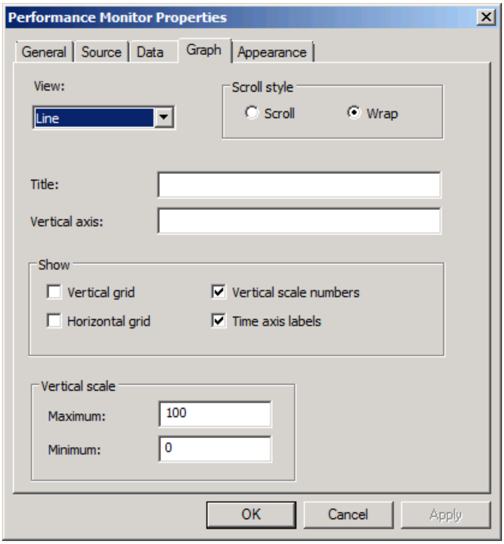
FIGURE 14-13 The additional counters in the Performance Monitor graph.

The performance objects, performance counters, and instances that are available for selection in the Add Counters dialog box depend on the computer's hardware configuration, the software installed on the computer, and the computer's role on the network. For example, the Performance Monitor snap-in on your Windows SBS 2011 primary server includes hundreds of additional counters for Microsoft Exchange, SQL Server, and SharePoint Foundation that would not appear on a computer running Windows Server 2008 R2 without those products installed.

Modifying the Graph View

The legend beneath the Performance Monitor graph specifies the line color for each counter, the scale of values for the counter, and other identifying information. When you select a counter in the legend, its current values appear in numerical form at the bottom of the graph. Click the Highlight button in the toolbar (or press Ctrl+H) to change the selected counter to a broad line that is easier to distinguish from the other lines in the graph.

On a computer that is otherwise idle, the line in the default graph tends to hover near the bottom of the scale, making it difficult to see its value. You can address this problem—or that of any graph that is difficult to see—by modifying the scale of the graph's Y (vertical) axis. Click the Properties button in the toolbar (or press Ctrl+Q) to display the Performance Monitor Properties sheet and click the *Graph* tab, as shown in Figure 14-14. In the *Vertical scale* box, you can reduce the maximum value for the Y axis, thereby using more of the graph to display the counter data.


Performance Monitor Properties

View: Line

Scroll style: ○ Scroll ● Wrap

Title:

Vertical axis:

Show

□ Vertical grid ☑ Vertical scale numbers

□ Horizontal grid ☑ Time axis labels

Vertical scale

Maximum: 100

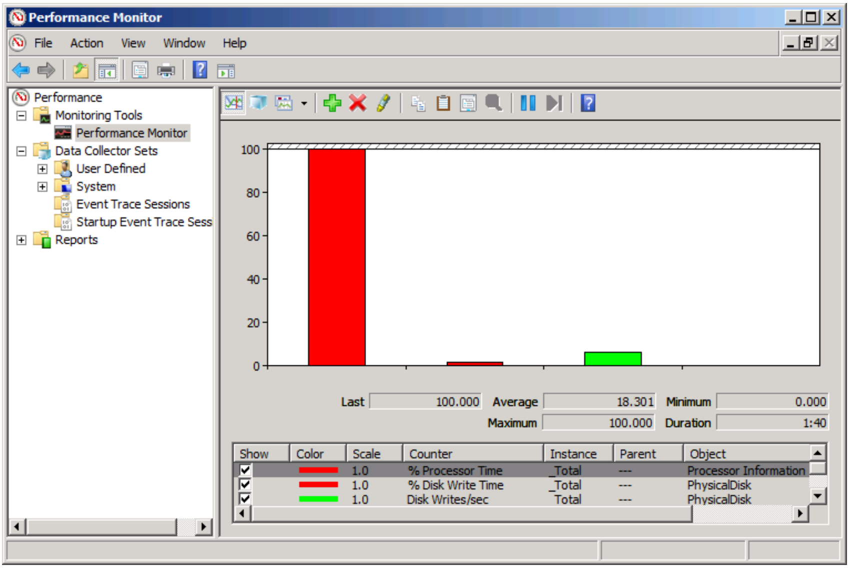
Minimum: 0

FIGURE 14-14 The *Graph* tab in the Performance Monitor Properties sheet.

On the *General* tab of the Performance Monitor Properties sheet, you can modify the sample rate of the graph. By default, Performance Monitor samples each performance counter value every one second, but you can increase this value to display data for a longer time period on a single page of the graph. This makes it easier to use Performance Monitor to display long-term trends in counter values.

Using Other Views

In addition to the line graph, Performance Monitor can display its captured data using two other views: a histogram view and a report view. You change the display to one of these views by clicking the *Change Graph Type* toolbar button. The *histogram view* is a bar graph with a separate vertical bar for each counter, as shown in Figure 14-15. In this view, it is easier to monitor large numbers of counters, because the lines do not overlap.

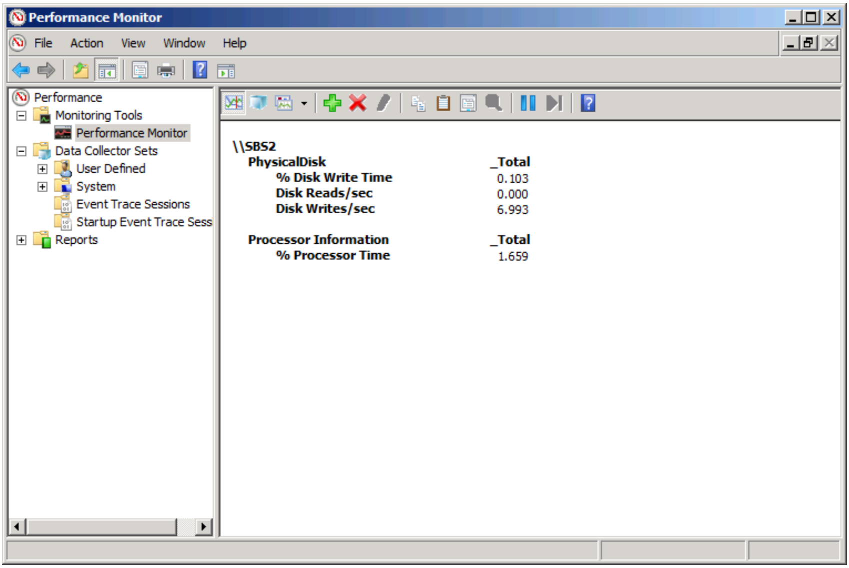


Last 100.000 Average 18.301 Minimum 0.000
Maximum 100.000 Duration 1:40

Show	Color	Scale	Counter	Instance	Parent	Object
☑	🟥	1.0	% Processor Time	_Total	---	Processor Information
☑	🟥	1.0	% Disk Write Time	_Total	---	PhysicalDisk
☑	🟩	1.0	Disk Writes/sec	_Total	---	PhysicalDisk

FIGURE 14-15 The Performance Monitor histogram view.

The *report view*, as shown in Figure 14-16, displays the numerical value for each of the performance counters.



```
\\SBS2
    PhysicalDisk                           _Total
        % Disk Write Time                   0.103
        Disk Reads/sec                      0.000
        Disk Writes/sec                     6.993

    Processor Information                  _Total
        % Processor Time                    1.659
```

FIGURE 14-16 The Performance Monitor report view.

The primary drawback of the histogram and report views is that they do not display a history of the counter values, only the current value. Each new sampling overwrites the previous one in the display, unlike the line graph, which displays the previous values as well.

Creating an Effective Display

In many cases, when users first discover the Performance Monitor tool, they see the hundreds of available performance objects and proceed to create a line graph containing dozens of different counters. In most cases, the result is an incoherent muddle of a display. The number of counters that you can display effectively depends on the size and resolution of your monitor.

Consider a few tips when selecting counters:

- **Limit the number of counters** Too many counters make the graph difficult to comprehend. To display a large number of statistics, you can open multiple windows in the console and select different counters in each window, or use the histogram or report view to display a large number of counters in a more compact form.
- **Modify the counter display properties** Depending on the size and capabilities of your monitor, the default colors and line widths that Performance Monitor uses in its graph might make it difficult to distinguish counters from each other. On the *Data* tab in the Performance Monitor Properties sheet, you can modify the color, style, and width of each counter's line in the graph to make it easier to see.
- **Choose counters with comparable values** Performance Monitor imposes no limitations on the combinations of counters you can select for a single graph, but some statistics are not practical to display together because of their disparate values. When a graph contains one counter with a typical value under 20 and another counter with a value in the hundreds, it is difficult to arrange the display so that both counters are readable. Choose counters with values that are reasonably comparable so that you can display them legibly. If you must display counters with different value ranges, the report view is often preferable to the graphs.

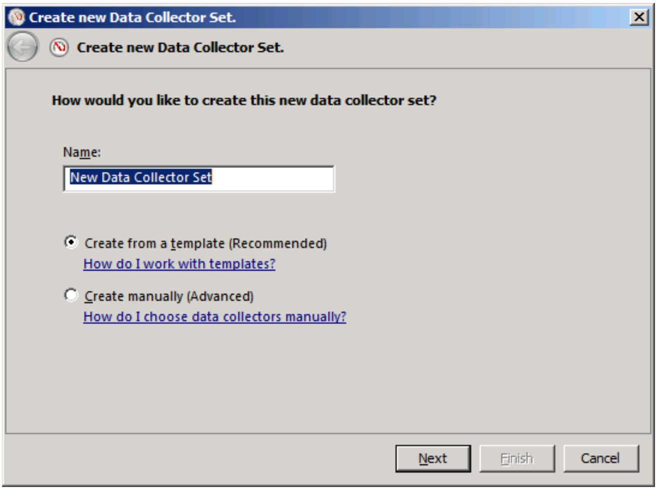
Creating Data Collector Sets

Over a period of time, server performance levels can degrade. Usually, a single component becomes overworked or insufficient; forming a bottleneck that can affect the entire computer. It is difficult to detect a bottleneck by examining a server's performance levels at a specific point in time.

This is why it is a good idea to use a tool like Performance Monitor to establish the operational baseline levels for your Windows SBS 2008 server. A *baseline* is simply a set of readings, captured under normal operating conditions, that you can save and compare to readings taken at a later time. By comparing the baseline statistics to server readings taken at regular intervals, you might be able to detect trends that eventually affect the computer's performance.

To capture counter statistics in the Performance Monitor Console for later review, you must create a *data collector set*, using the following procedure:

1. Log on to your Windows SBS 2011 primary server, using an account with network Administrator privileges. The Windows SBS Console appears.
2. Click *Start*. Then click *Administrative Tools* > *Performance Monitor*. The Performance Monitor Console appears.
3. Expand the *Data collector sets* folder. Then right-click the *User defined* folder and, from the context menu, select *New* > *Data Collector Set*. The Create New Data Collector Set Wizard appears, displaying the How Would You Like To Create This New Data Collector Set? page.


Create new Data Collector Set.
Create new Data Collector Set.

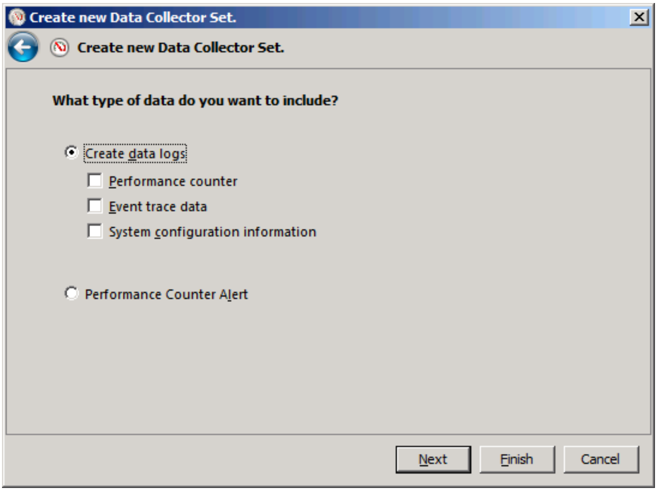
How would you like to create this new data collector set?

Name:
New Data Collector Set

● Create from a template (Recommended)
How do I work with templates?

○ Create manually (Advanced)
How do I choose data collectors manually?

4. In the *Name* text box, type a name for the data collector set. Then, select the *Create manually (advanced)* option and click *Next*. The What Type Of Data Do You Want To Include? page appears.



Create new Data Collector Set.

Create new Data Collector Set.

What type of data do you want to include?

● Create data logs

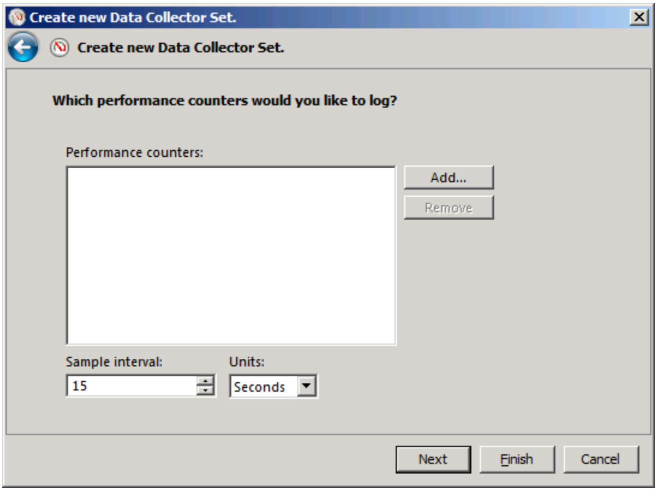
□ Performance counter

□ Event trace data

□ System configuration information

○ Performance Counter Alert

5. Select the *Performance counter* check box and click *Next*. The Which Performance Counters Would You Like To Log? page appears.



Create new Data Collector Set.

Create new Data Collector Set.

Which performance counters would you like to log?

Performance counters:

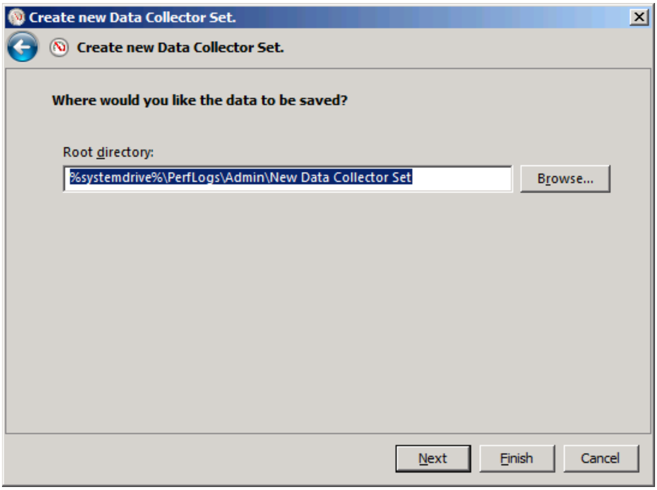
Sample interval: 15

Units: Seconds

6. Click *Add*. The standard Add Counters dialog box appears. Select the counters you want to log in the standard manner and click *OK*. The counters appear in the *Performance counters* box.

TIP You can also use the Create New Data Collector Set Wizard to create performance counter alerts, which monitor the values of specific counters and perform a task, such as sending an email to an administrator, when the counters reach a specific value.

7. Select a value for the *Sample interval spin* box, indicating how often you want the system to collect samples and click *Next*. The Where Would You Like The Data To Be Saved? page appears.

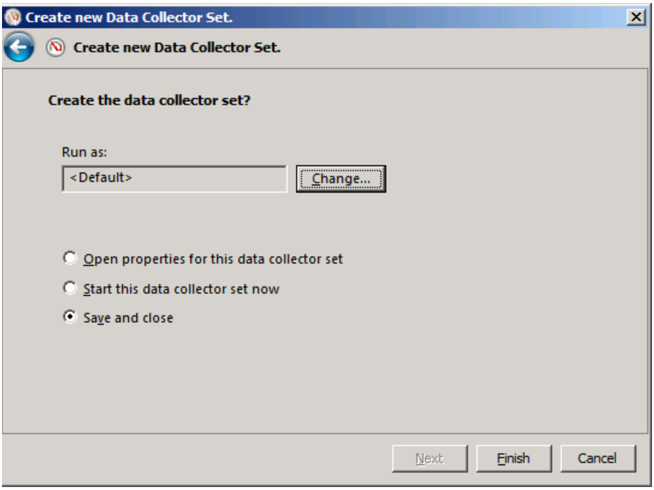


Create new Data Collector Set.

Where would you like the data to be saved?

Root directory: %systemdrive%\PerfLogs\Admin\New Data Collector Set

8. Type the name of or browse to the folder where you want to store the data collector set and click *Next*. The Create The Data Collector Set? page appears.



Create new Data Collector Set.

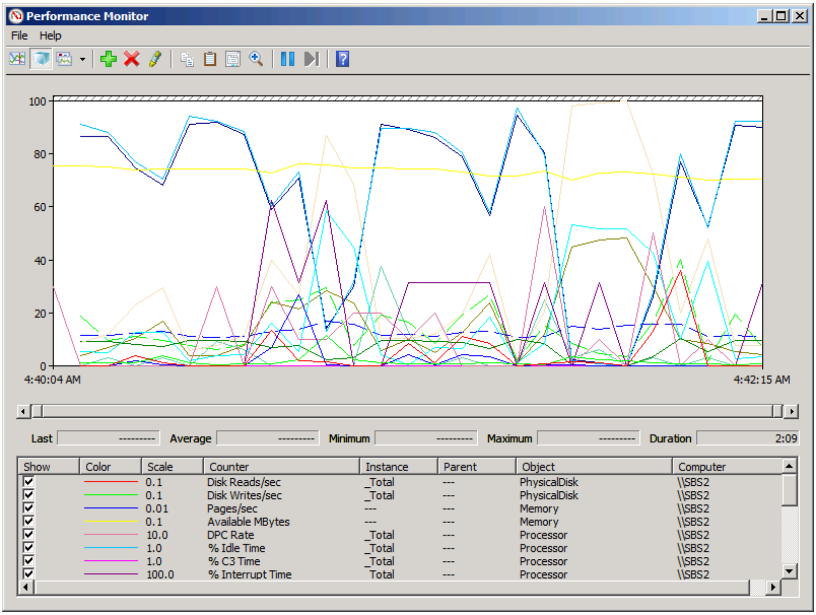
Create the data collector set?

Run as: <Default>

○ Open properties for this data collector set
○ Start this data collector set now
● Save and close

9. If the account you are currently using does not have the privileges needed to gather the log information, click *Change* to display a Performance Monitor dialog box in which you can supply alternative credentials.
10. Select one of the following options:
    - **Open properties for this data collector set** Saves the data collector set to the specified location and opens its Properties sheet for further modifications
    - **Start this data collector set now** Saves the data collector set to the specified location and starts collecting data immediately
    - **Save and close** Saves the data collector set to the specified location and closes the wizard
11. Click *Finish*. The new data collector set appears in the *User defined* folder.
12. Select the new data collector set and click *Start* in the toolbar. The console begins collecting data until you click *Stop*.

Once you have captured data using the collector set, you can display the data by double-clicking the *Performance monitor* file in the folder you specified during its creation. This opens a Performance Monitor window containing a graph of the collected data, instead of real-time activity, as shown in Figure 14-17.



Last --------- Average --------- Minimum --------- Maximum --------- Duration 2:09

Show	Color	Scale	Counter	Instance	Parent	Object	Computer
☑	🟥	0.1	Disk Reads/sec	_Total	---	PhysicalDisk	\\SBS2
☑	🟩	0.1	Disk Writes/sec	_Total	---	PhysicalDisk	\\SBS2
☑	🟦	0.01	Pages/sec	---	---	Memory	\\SBS2
☑	🟨	0.1	Available MBytes	---	---	Memory	\\SBS2
☑	▬	10.0	DPC Rate	_Total	---	Processor	\\SBS2
☑	▬	1.0	% Idle Time	_Total	---	Processor	\\SBS2
☑	▬	1.0	% C3 Time	_Total	---	Processor	\\SBS2
☑	🟪	100.0	% Interrupt Time	Total	---	Processor	\\SBS2

FIGURE 14-17 Performance Monitor information collected using a data collector set.

By repeating this process at a later time and comparing the information in the two data collector sets, you can often detect performance trends that indicate the presence of bottlenecks.

Using the Windows SBS 2011 Best Practices Analyzer

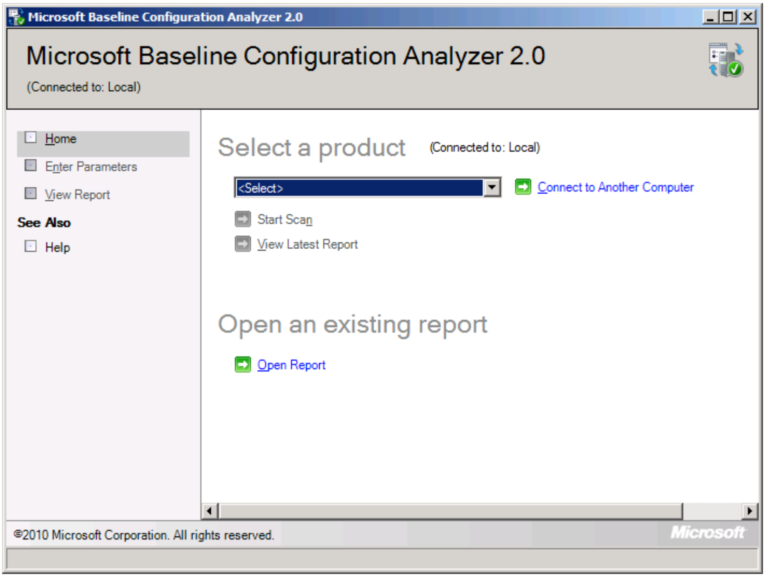
As discussed in Chapter 1, "Introducing Windows Small Business Server 2011," the designers of Windows SBS 2011 have made many of the installation and configuration decisions that Windows Server 2008 R2 administrators must make. The default server configuration implements a series of *best practices* by installing certain roles and features and configuring them to create a standard Windows SBS server configuration.

These best practices are not required to run Windows SBS 2011; you can make whatever changes to the operating system and its applications you want. However, you should be conscious of the repercussions that deviations from the standard configuration can have. The Windows SBS 2011 Best Practices Analyzer (BPA) is a tool that can examine your current system and network configurations and create a report listing the differences between it and the recommended Windows SBS 2011 settings.

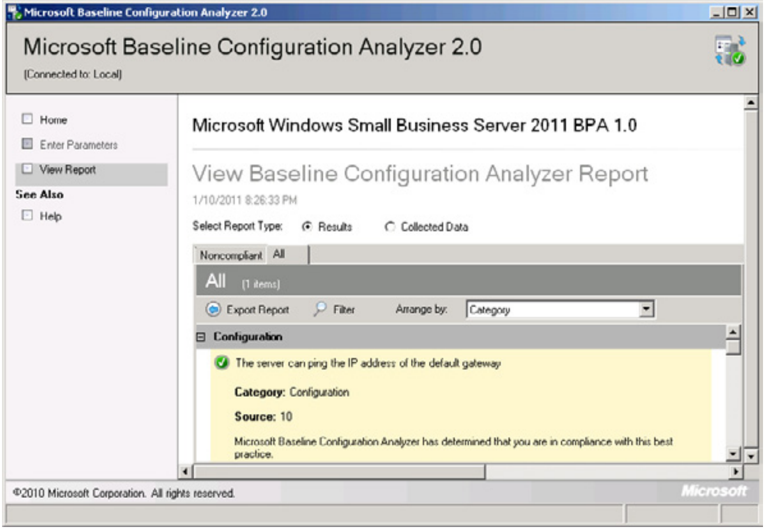
The Windows SBS 2011 BPA is not supplied with the Windows SBS 2011 product. You must download it—and the Microsoft Baseline Configuration Analyzer 2.0 (MBCA)—from the Microsoft Download Center at *http://microsoft.com/downloads* and install them on your Windows SBS primary server. The BPA and the MBCA are both packaged as Microsoft Installer (.msi) files, which you must execute on your primary server, MBCA first and then BPA. A standard installation wizard takes you through the process of approving the license agreement and specifying a location for the program. You can also choose to integrate the Windows SBS 2011 BPA into the Windows SBS Console, which enables you to view the results of the BPA scan in the Detailed Network Report.

Once you have installed the software, use the following procedure to run the Windows SBS 2011 BPA and perform your first scan:

1. Log on to your Windows SBS 2011 primary server, using an account with network Administrator privileges.
2. Click *Start*. Then click *All Programs* > *Windows Small Business Server Tools* > *Windows Small Business Server 2011 Best Practices Analyzer*. When the User Account Control dialog box appears, click *Continue*. The Microsoft Baseline Configuration Analyzer 2.0 page appears.



3. In the *Select a product* drop-down list, select *Windows Small Business Server 2011 BPA* and click *Start scan*. BPA proceeds to scan the system and displays the resulting report.



Microsoft Windows Small Business Server 2011 BPA 1.0

View Baseline Configuration Analyzer Report

1/10/2011 8:26:33 PM

Select Report Type: ● Results ○ Collected Data

✓ The server can ping the IP address of the default gateway

Category: Configuration

Source: 10

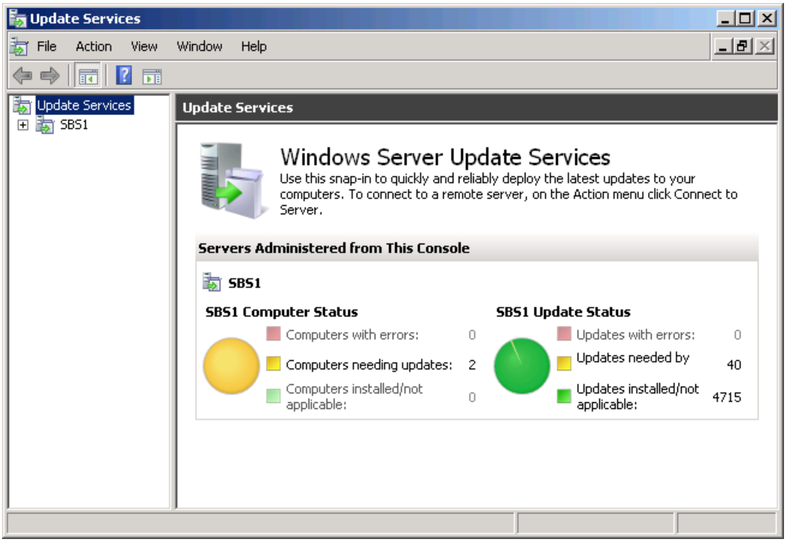
Microsoft Baseline Configuration Analyzer has determined that you are in compliance with this best practice.

Using WSUS Reports

The Windows SBS Console enables you to view a list of the updates that WSUS has furnished to each computer on your network, but it does not provide any more detailed WSUS statistics. You can obtain additional information about WSUS activities, however, by using the Update Services console.

To generate WSUS reports, follow these steps:

1. Log on to your Windows SBS 2011 primary server, using an account with network Administrator privileges.
2. Click *Start*, and then click *Administrative Tools* > *Windows Server Update Services*. When the User Account Control dialog box appears, click *Continue*. The Update Services Console appears.



Update Services

Windows Server Update Services

Use this snap-in to quickly and reliably deploy the latest updates to your computers. To connect to a remote server, on the Action menu click Connect to Server.

Servers Administered from This Console

SBS1

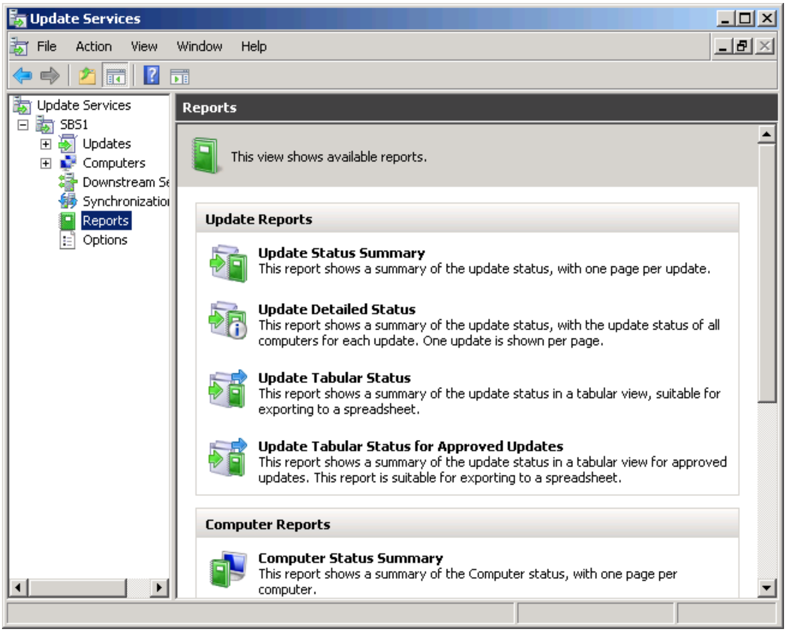
SBS1 Computer Status

🟥 Computers with errors:	0
🟨 Computers needing updates:	2
🟩 Computers installed/not applicable:	0

SBS1 Update Status

🟥 Updates with errors:	0
🟨 Updates needed by	40
🟩 Updates installed/not applicable:	4715

3. Expand the node named for your server and select *Reports*. The Reports pane appears.



Reports

This view shows available reports.

Update Reports

Update Status Summary
This report shows a summary of the update status, with one page per update.

Update Detailed Status
This report shows a summary of the update status, with the update status of all computers for each update. One update is shown per page.

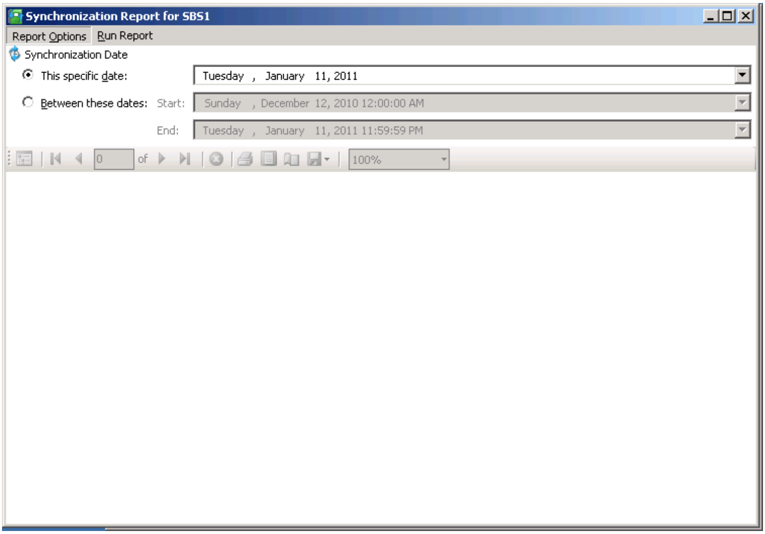
Update Tabular Status
This report shows a summary of the update status in a tabular view, suitable for exporting to a spreadsheet.

Update Tabular Status for Approved Updates
This report shows a summary of the update status in a tabular view for approved updates. This report is suitable for exporting to a spreadsheet.

Computer Reports

Computer Status Summary
This report shows a summary of the Computer status, with one page per computer.

4. To check the status of your WSUS synchronizations, click *Synchronization results*. The Synchronization Report window for your server appears.



Synchronization Date

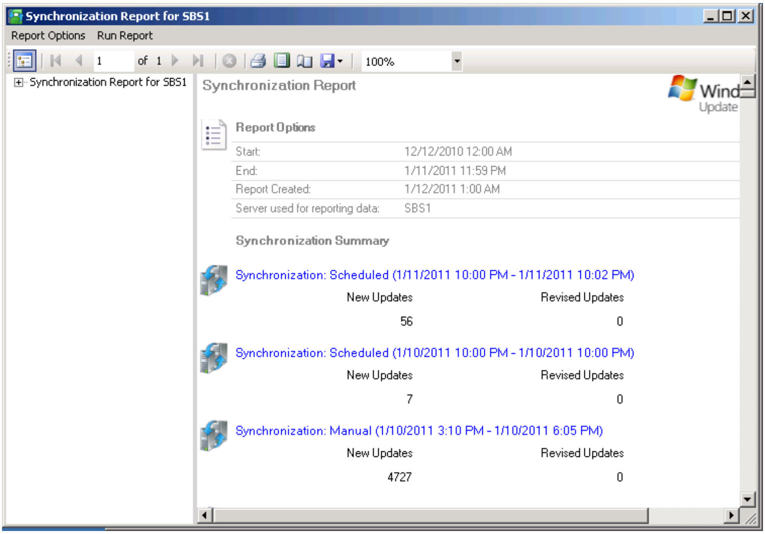
● This specific date: Tuesday , January 11, 2011

○ Between these dates: Start: Sunday , December 12, 2010 12:00:00 AM

End: Tuesday , January 11, 2011 11:59:59 PM

5. Select the *Between these dates* option, and then choose *Start* and *End* dates.

6. On the menu bar, select *Run report*. The console generates a report that begins with a summary of each synchronization performed during the selected dates.


Synchronization Report for SBS1
Report Options
Run Report
1
of 1
100%
Synchronization Report for SBS1
Windows Update

Synchronization Report

Report Options

Start:	12/12/2010 12:00 AM
End:	1/11/2011 11:59 PM
Report Created:	1/12/2011 1:00 AM
Server used for reporting data:	SBS1

Synchronization Summary

Synchronization: Scheduled (1/11/2011 10:00 PM - 1/11/2011 10:02 PM)

New Updates	Revised Updates
56	0

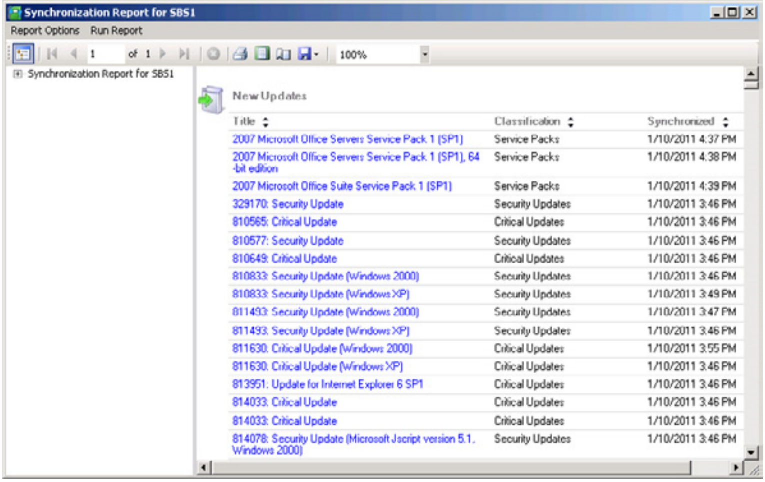
Synchronization: Scheduled (1/10/2011 10:00 PM - 1/10/2011 10:00 PM)

New Updates	Revised Updates
7	0

Synchronization: Manual (1/10/2011 3:10 PM - 1/10/2011 6:05 PM)

New Updates	Revised Updates
4727	0

7. Scroll down to see a list of new updates downloaded by WSUS.

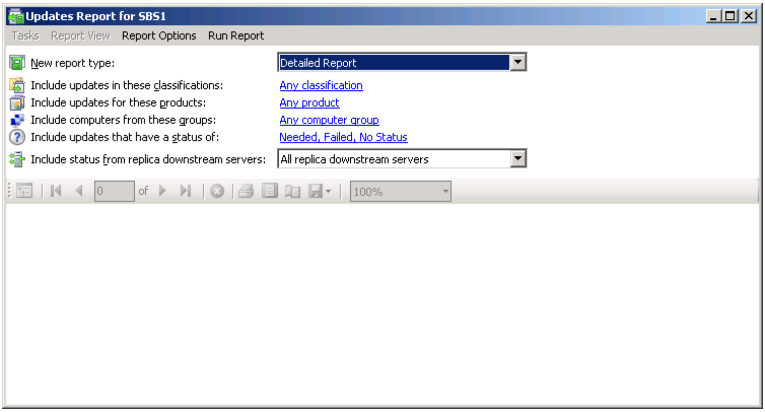

Synchronization Report for SBS1
Report Options
Run Report
1
of 1
100%
Synchronization Report for SBS1

New Updates

Title	Classification	Synchronized
2007 Microsoft Office Servers Service Pack 1 (SP1)	Service Packs	1/10/2011 4:37 PM
2007 Microsoft Office Servers Service Pack 1 (SP1), 64 -bit edition	Service Packs	1/10/2011 4:38 PM
2007 Microsoft Office Suite Service Pack 1 (SP1)	Service Packs	1/10/2011 4:39 PM
329170: Security Update	Security Updates	1/10/2011 3:46 PM
810565: Critical Update	Critical Updates	1/10/2011 3:46 PM
810577: Security Update	Security Updates	1/10/2011 3:46 PM
810649: Critical Update	Critical Updates	1/10/2011 3:46 PM
810833: Security Update (Windows 2000)	Security Updates	1/10/2011 3:46 PM
810833: Security Update (Windows XP)	Security Updates	1/10/2011 3:49 PM
811493: Security Update (Windows 2000)	Security Updates	1/10/2011 3:47 PM
811493: Security Update (Windows XP)	Security Updates	1/10/2011 3:46 PM
811630: Critical Update (Windows 2000)	Critical Updates	1/10/2011 3:55 PM
811630: Critical Update (Windows XP)	Critical Updates	1/10/2011 3:46 PM
813951: Update for Internet Explorer 6 SP1	Critical Updates	1/10/2011 3:46 PM
814033: Critical Update	Critical Updates	1/10/2011 3:46 PM
814033: Critical Update	Critical Updates	1/10/2011 3:46 PM
814078: Security Update (Microsoft Jscript version 5.1, Windows 2000)	Security Updates	1/10/2011 3:46 PM

8. Print or save the report, if needed, and close the Synchronization Report window.

9. To generate a detailed report of all WSUS updates, click *Update detailed status*. The Updates Report window for your server appears.



New report type: Detailed Report

Include updates in these classifications: Any classification

Include updates for these products: Any product

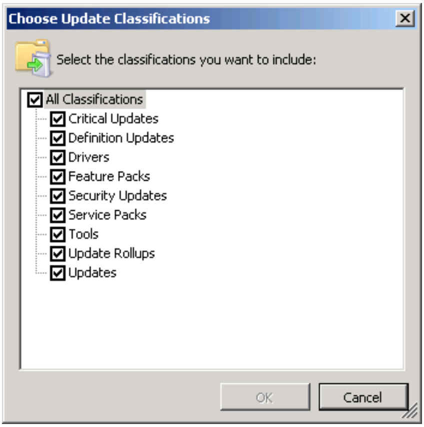
Include computers from these groups: Any computer group

Include updates that have a status of: Needed, Failed, No Status

Include status from replica downstream servers: All replica downstream servers

10. Make sure the *New report type* drop-down list is set to *Detailed report* and configure the following options as needed:

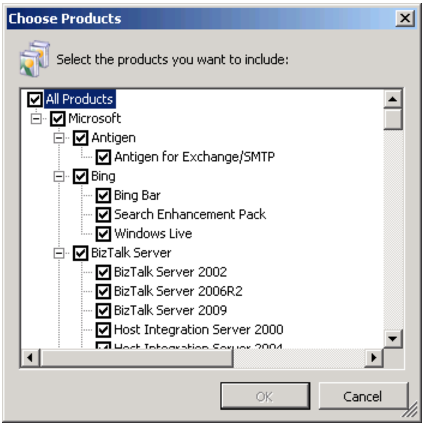
- **Include updates in these classifications** Enables you to specify the types of updates for which you want a report, using the interface shown here.



Select the classifications you want to include:

☑ All Classifications
- ☑ Critical Updates
- ☑ Definition Updates
- ☑ Drivers
- ☑ Feature Packs
- ☑ Security Updates
- ☑ Service Packs
- ☑ Tools
- ☑ Update Rollups
- ☑ Updates

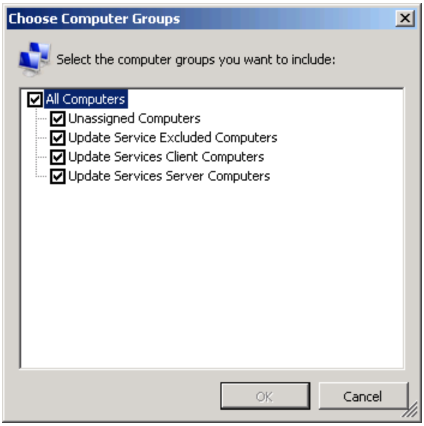
- **Include updates for these products** Enables you to specify the operating systems and applications for which you want a report, using the interface shown here.


Choose Products

Select the products you want to include:

- ☑ All Products
  - ☑ Microsoft
    - ☑ Antigen
      - ☑ Antigen for Exchange/SMTP
    - ☑ Bing
      - ☑ Bing Bar
      - ☑ Search Enhancement Pack
      - ☑ Windows Live
    - ☑ BizTalk Server
      - ☑ BizTalk Server 2002
      - ☑ BizTalk Server 2006R2
      - ☑ BizTalk Server 2009
      - ☑ Host Integration Server 2000
      - ☑ Host Integration Server 2004

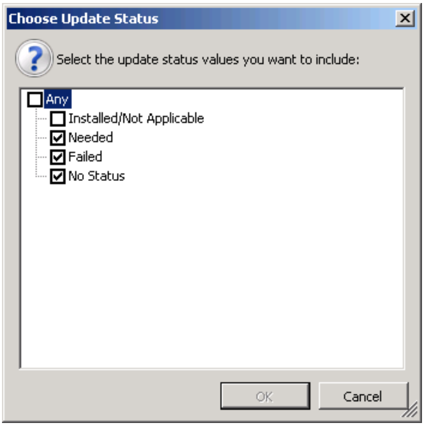
- **Include computers from these groups** Enables you to select the WSUS computer groups on which you want to report, using the interface shown here.


Choose Computer Groups

Select the computer groups you want to include:

- ☑ All Computers
  - ☑ Unassigned Computers
  - ☑ Update Service Excluded Computers
  - ☑ Update Services Client Computers
  - ☑ Update Services Server Computers

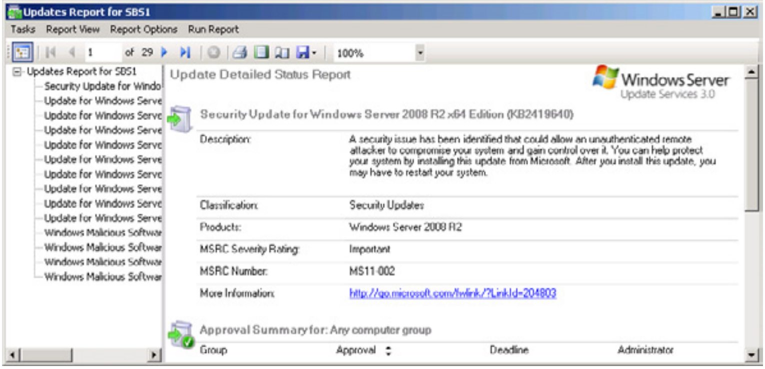
- **Include updates that have a status of** Enables you to specify which updates you want included in the report, based on their completion status, using the interface shown here.


Choose Update Status

Select the update status values you want to include:

- ☐ Any
  - ☐ Installed/Not Applicable
  - ☑ Needed
  - ☑ Failed
  - ☑ No Status

11. On the menu bar, select *Run report*. The console generates a report that lists each selected update, provides detailed metadata for it, and lists its approval and deployment history.



Update Detailed Status Report

Security Update for Windows Server 2008 R2 x64 Edition (KB2419640)

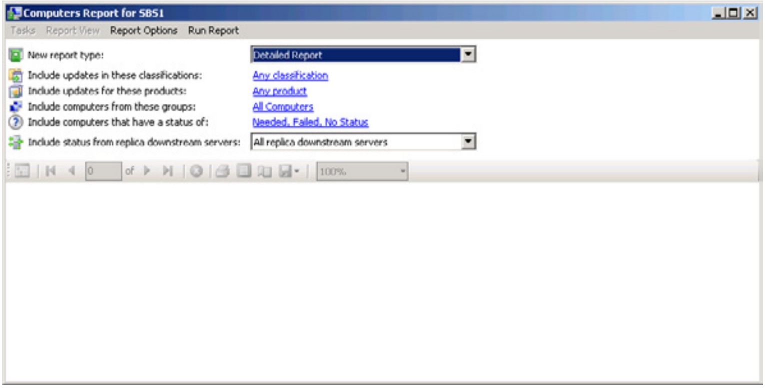
Description:	A security issue has been identified that could allow an unauthenticated remote attacker to compromise your system and gain control over it. You can help protect your system by installing this update from Microsoft. After you install this update, you may have to restart your system.
Classification:	Security Updates
Products:	Windows Server 2008 R2
MSRC Severity Rating:	Important
MSRC Number:	MS11-002
More Information:	http://go.microsoft.com/fwlink/?LinkId=204803

Approval Summary for: Any computer group

Group	Approval	Deadline	Administrator

12. Print or save the report, if needed, and close the Updates Report window.

13. To generate a detailed report for each computer, click *Computer detailed status*. The Computers Report window for your server appears.



New report type: Detailed Report

Include updates in these classifications: Any classification

Include updates for these products: Any product

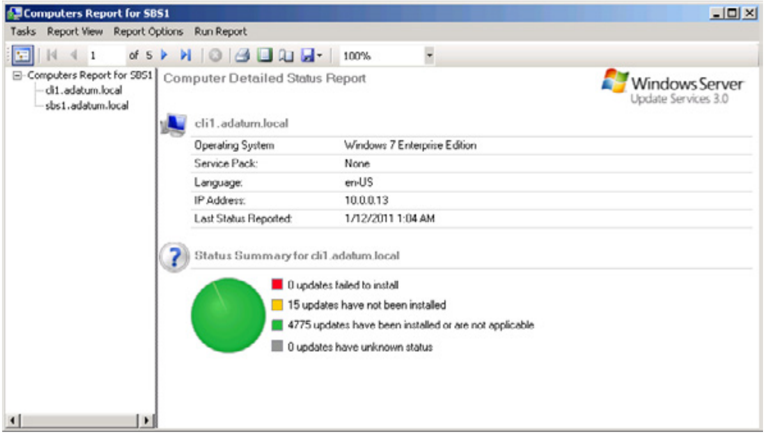
Include computers from these groups: All Computers

Include computers that have a status of: Needed, Failed, No Status

Include status from replica downstream servers: All replica downstream servers

14. Make sure the *New report type* drop-down list is set to *Detailed report* and configure the options that follow as needed.

15. On the menu bar, select *Run report*. The console generates a report that lists each selected computer and summarizes its update status.



Computer Detailed Status Report

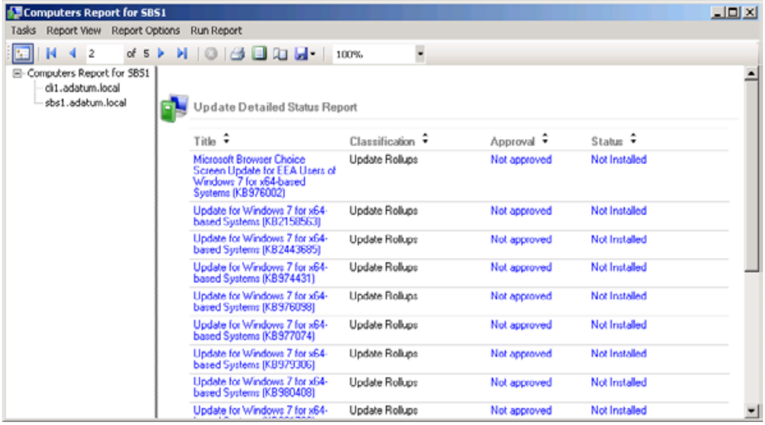
cli1.adatum.local

Operating System	Windows 7 Enterprise Edition
Service Pack:	None
Language:	en-US
IP Address:	10.0.0.13
Last Status Reported:	1/12/2011 1:04 AM

Status Summary for cli1.adatum.local

- 🟥 0 updates failed to install
- 🟨 15 updates have not been installed
- 🟩 4775 updates have been installed or are not applicable
- ⬜ 0 updates have unknown status

16. Click *Next page* to display a list of the updates corresponding to your selected options.



Update Detailed Status Report

Title	Classification	Approval	Status
Microsoft Browser Choice Screen Update for EEA Users of Windows 7 for x64-based Systems (KB976002)	Update Rollups	Not approved	Not Installed
Update for Windows 7 for x64-based Systems (KB2158563)	Update Rollups	Not approved	Not Installed
Update for Windows 7 for x64-based Systems (KB2443685)	Update Rollups	Not approved	Not Installed
Update for Windows 7 for x64-based Systems (KB974431)	Update Rollups	Not approved	Not Installed
Update for Windows 7 for x64-based Systems (KB976098)	Update Rollups	Not approved	Not Installed
Update for Windows 7 for x64-based Systems (KB977074)	Update Rollups	Not approved	Not Installed
Update for Windows 7 for x64-based Systems (KB979306)	Update Rollups	Not approved	Not Installed
Update for Windows 7 for x64-based Systems (KB980408)	Update Rollups	Not approved	Not Installed
Update for Windows 7 for x64-	Update Rollups	Not approved	Not Installed

17. Print or save the report, if needed, and close the Computers Report window.
18. Close the Update Services Console.

CHAPTER 15

Administering Email

Email is an all-but-essential tool in today's business world, and Microsoft Exchange Server 2010 Standard SP1 is one of the most powerful email server products on the market. Exchange Server is a highly flexible product, designed to support networks of virtually any size, and as a result, it can be complicated to install and configure. However, Windows Small Business Server (SBS) 2011 integrates the Exchange Server installation into its primary setup procedure and completes most of the configuration tasks for you. The Windows SBS Console enables you to configure the email settings that small businesses use most often, but you still have access to the full power of the Exchange Management Console and the other tools included with Exchange Server 2010.

An Email Primer

A basic understanding of how email works is critical to managing an email system efficiently. Email is a client/server application that enables a client to send messages to any other client with only a simple identifying address. Between the sending and receiving clients is a system of email servers that communicate with each other using specialized protocols, such as the Simple Mail Transfer Protocol (SMTP). As with most networking subjects, email communication can be extremely complicated, but the typical small business network administrator does not need to delve into the technical details too deeply. The following sections examine some of the most basic concepts, however, and describe how they pertain to Windows SBS 2011.

Understanding Email Addresses

As all email users know, an email address consists of a single user name, followed by an @ character and a domain name, as shown in Figure 15-1. The first part of the address, the part before the @ sign, is the *local part*, which needs to be understood only by the destination mail server. The part after the @ sign identifies the domain on the Internet where the destination client is located.

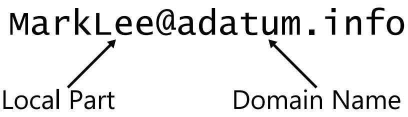


FIGURE 15-1 The parts of an email address.

In Chapter 2, "A Networking Primer," you learned that Internet Protocol (IP) addresses consist of two parts: a host identifier and a network identifier. Routers on the Internet use the network identifier to forward IP datagrams to a particular destination network and then the router on the destination network uses the host identifier to forward the datagrams to the correct computer on that network. In the same way, the Domain Name System (DNS) identifies computers using fully qualified domain names (FQDNs), which consist of two parts: a host name and a domain name. When a DNS server tries to resolve an FQDN into an IP address, it forwards the name resolution request to the authoritative server for the domain, which looks up the IP address of the specified host.

Email communications function in much the same way. The SMTP servers on the Internet read only the second part of the email address and forward the email message to the mail server for the appropriate domain. Then, the domain mail server reads the first part of the address—the part before the @ sign—and deposits the email message in the mailbox for the appropriate user.

Because the domain name of an email address must be understandable to all the servers on the Internet, it must conform to the same standards as all DNS domain names. Therefore, the domain name part of an email address is subject to the following limitations:

- The domain name can be no more than 255 characters long.
- Domain names can consist only of the letters *A* to *Z*, the numbers 0 to 9, and the hyphen (-) character.
- Domain names are not case-sensitive. The addresses *sanjays@adatum.com* and *sanjays@ADATUM.COM* are delivered to the same mail server.

Because the local part of an email address has to be read and understood only by the destination mail server, its specifications are less stringent. The local part of an email address is subject to the following limitations:

- The local part of the name can be no more than 64 characters long.

- Local part names can consist of the letters *A* to *Z*, the numbers 0 to 9, and the following characters: *! # $ % & ' * + - / = ? ^ _ ` { | } ~*.
- Local part names can also contain the period (.) character as long as it does not appear as the first or last character and as long as it does not appear twice in succession.
- Local part names can conceivably be case-sensitive, but in Exchange Server 2010, they are not. Exchange Server delivers the addresses *sanjays@adatum.com* and *SanjayS@adatum.com* to the same mailbox.

Local part names can be case-sensitive because their interpretation is left solely to the destination email server. If a particular server implementation supports case-sensitive local part names, and the destination server is running that implementation, then the distinction of two local part names that differ only in their case is possible. However, on the Internet, senders rarely know what server implementations their recipients are using, so most email servers, including Exchange Server 2010, follow the recommendation of the SMTP standard and treat all local part names as case-insensitive. Windows SBS 2011 does not allow you to create two user accounts with email addresses that differ only in case.

> ***NOTE*** **Some email servers impose other restrictions on local part name construction. For example, the Windows Live Hotmail system limits local part names to letters; numbers; and the period (.), hyphen (-), and underscore (_) characters. You cannot create a Hotmail account name using any other characters, and the Hotmail system does not send email to any address using other characters.**

Despite the limitations listed earlier, one of your primary goals when assigning email addresses should always be user-friendliness. An email address like *hknjv!fgjyc8*pi09iponi0-v665q{436y@xyucu6ysxxgfu7opm83opdx5zw56iyb.com* would be technically legal, but it would be terribly inconvenient for the individuals forced to use it or anyone trying to remember it.

Understanding Email Server Functions

Email clients have two basic messaging functions: They send outgoing mail to one kind of server and they retrieve incoming mail from another. The servers conduct the rest of the email communication process, including the transmission of messages to computers hundreds or thousands of miles away. The following sections discuss the main email server types.

> ***NOTE*** **It is critical to realize that in this discussion of email communications, the term *server* does not necessarily refer to a separate computer, but instead to a process running on a computer in the form of an application or service. A single computer can perform multiple server functions, as in the case of a computer running Exchange Server 2010, which can perform all the email server roles simultaneously.**

Simple Mail Transfer Protocol (SMTP)

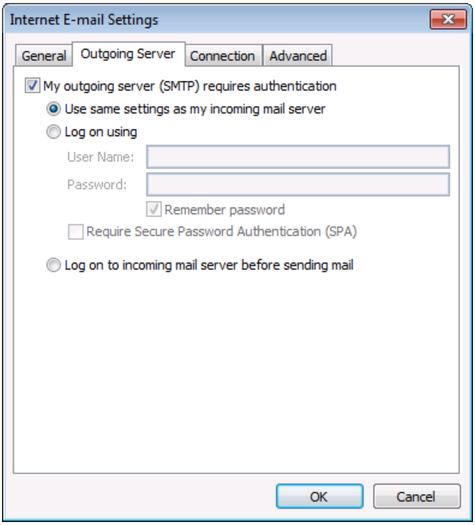
SMTP is the primary email communication protocol, responsible for the majority of email traffic on the Internet. Every email client has the name or IP address of an SMTP server in its configuration settings, to which it transmits its outgoing mail messages. Email servers can use SMTP for both incoming and outgoing traffic.

SMTP is a text-based, application layer protocol that email clients use to send their outgoing messages to a server, and email servers use it to forward the messages to other servers. Windows SBS 2011 servers function as SMTP servers, as can all computers running Exchange Server 2010. Whichever email client your users choose to run, that client sends its outgoing email messages to the Windows SBS 2011 server using SMTP. If the intended recipient of a message is another user on your network, the Windows SBS server deposits the message in the recipient's Exchange mailbox. If the message is addressed to a user in another domain, the server transmits the message to another SMTP server on the Internet.

An SMTP server is a relatively simple mechanism, but its role has been complicated over the years by the increasing prevalence on the Internet of unsolicited email traffic, also known as *spam*. In earlier days, Internet service providers (ISPs) set up SMTP servers for their customers, connected them to the Internet, and left them open for use by anyone. The well-known port number for the SMTP protocol is 25, and those servers willingly accepted anyone's outgoing SMTP email messages as long as they were addressed to that port.

However, it was not long before spammers began using these open servers to send millions of unsolicited messages. By using the SMTP servers belonging to other ISPs, the spammers made it difficult, if not impossible, to trace their spam emails back to them. As a result of the enormous amounts of bandwidth consumed by the spam, ISPs were forced to add various forms of protection to their SMTP servers.

Most Internet SMTP servers today require users to authenticate before they can submit outgoing traffic, and many of them refuse all traffic addressed to port number 25. Email clients typically enable users to specify the credentials they should use to log on to the SMTP server, as shown in Figure 15-2, as well as an alternative to port number 25. Port number 587 has been standardized as the port for authenticated outgoing mail submissions, but some ISPs use nonstandard ports instead.



Internet E-mail Settings

☑ My outgoing server (SMTP) requires authentication

● Use same settings as my incoming mail server

○ Log on using

User Name:

Password:

☑ Remember password

□ Require Secure Password Authentication (SPA)

○ Log on to incoming mail server before sending mail

FIGURE 15-2 The Outgoing Server configuration settings in Microsoft Office Outlook 2010.

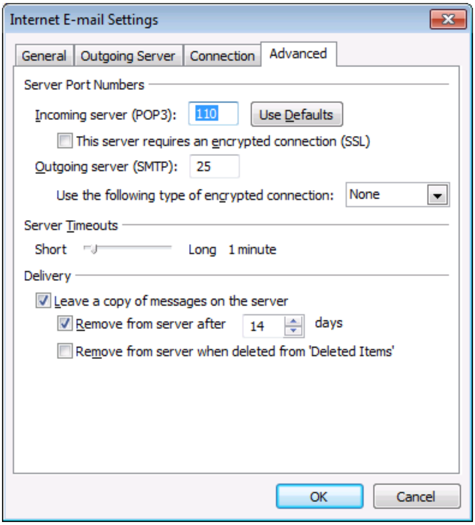
> ***NOTE*** **On a Windows SBS 2011 network, the computer functioning as the SMTP server is not accessible directly from the Internet, so it is not subject to abuse by spammers outside the local network. Therefore, it is not necessary to take these protective measures.**

Post Office Protocol Version 3 (POP3)

SMTP is strictly a "push" protocol. Email clients and other email servers send messages to SMTP servers; they do not retrieve messages from them. To retrieve their incoming messages from a server, clients use one of two "pull" protocols: *Post Office Protocol version 3 (POP3)* or *Internet Message Access Protocol version 4 (IMAP4).* POP3 is the more popular of these protocols.

> ***NOTE*** **The standard for version 3 of POP was published in 1996. POP1 and POP2 have long since become obsolete, and any reference to POP without a version identifier almost certainly refers to POP version 3. There is a Post Office Protocol version 4 (POP4) server in development, but the protocol has not yet been standardized, nor is it commercially available.**

POP3 is a relatively simple protocol that is designed to provide clients with offline access to their email messages. A POP3 server maintains a separate mailbox for each user in a particular domain, whereas the server stores the incoming email messages it receives through its SMTP connections. Email clients periodically connect to the server, authenticate the user, and download the messages in the user's mailbox. In most cases, the server deletes the messages once the client has downloaded them, but many POP3 implementations provide users with the ability to leave copies of the downloaded messages on the server, as shown in Figure 15-3.



Server Port Numbers

Incoming server (POP3): 110

□ This server requires an encrypted connection (SSL)

Outgoing server (SMTP): 25

Use the following type of encrypted connection: None

Server Timeouts

Short Long 1 minute

Delivery

☑ Leave a copy of messages on the server

☑ Remove from server after 14 days

□ Remove from server when deleted from 'Deleted Items'

FIGURE 15-3 The Advanced Configuration settings in Outlook 2010.

The design of the POP3 mechanism enables clients to connect to the server, download messages, and then disconnect, after which the user can work with the messages offline. Because of this, the client's message store is said to be authoritative in a POP3 application. When dial-up connections were the prevalent form of Internet access, POP3 provided the most bandwidth-efficient method of accessing incoming email.

POP3 is designed to keep the server side of the application as simple as possible, leaving the majority of the messaging tasks to the client. There are, however, two potential areas of server complexity. One involves the numbering of the messages in a mailbox when a user downloads and deletes some, but not all of the waiting messages. Instead of numbering the messages consecutively, and renumbering the messages when the client deletes some of them, most POP3 implementations use a technique called *Unique Identification Listing (UIDL)* to assign a permanent, unique identifier to each message in the mailbox.

The other potential problem is one of authentication security. The POP3 standard contains no provision for the use of encrypted passwords, and some implementations still require clients to transmit passwords in plain text. There are, however, a number of POP3 implementations that use security extensions to protect passwords and prevent unauthorized access to email accounts.

POP3 servers use the well-known port number 110 for client connections, and many implementations can use *Secure Sockets Layer (SSL)* or *Transport Layer Security (TLS)* to encrypt the contents of the email messages during download.

Internet Message Access Protocol 4 (IMAP4)

IMAP4 is another “pull” protocol that clients can use to obtain their email messages from a server. However, unlike POP3, IMAP4 is designed to leave the messages stored on the server and enable users to work with them there. An IMAP4 client is able to store copies of email messages on the local drive, but the authoritative message store resides on the server.

Most email clients can support both IMAP4 and POP3 connections to a server. IMAP4 connections use well-known port number 143. ISPs tend to provide their customers with POP3 mailboxes because they require fewer server resources and much less server storage. Web–based email implementations, on the other hand, often use IMAP4 to display a user’s message store in a web browser interface.

IMAP4 places a much greater burden on the server than POP3, not only because the server must maintain a message store for each user but also because the IMAP4 server provides more functions than a POP3 server. IMAP4 clients can create folders to organize email messages, move messages around between folders, and run searches for specific messages. Searching, in particular, can be a highly resource-intensive task, depending on the size of the mailbox.

IMAP4 also provides distinct advantages for the user. When a client connects to a server using IMAP4, access to the user’s message store is almost immediate because the client is displaying the contents of the mailbox as it exists on the server. By contrast, a POP3 client must check the server for new messages, download them, and integrate the messages into the client’s data store before the user can begin working with them.

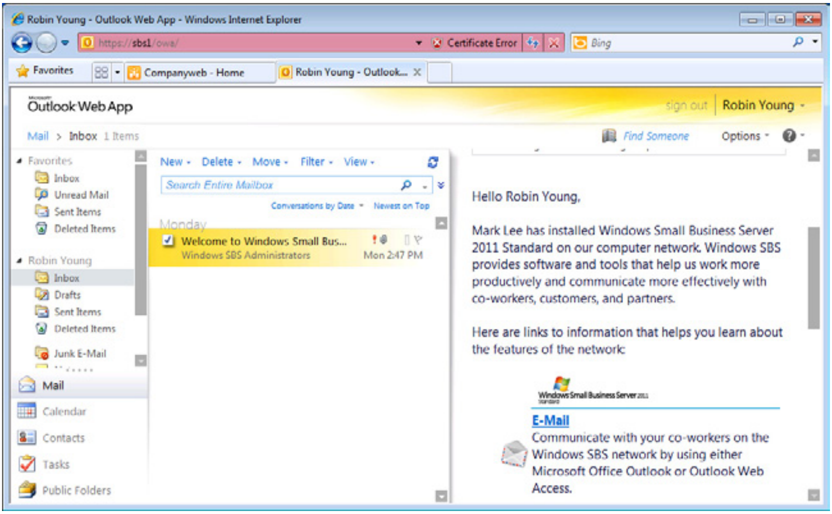
Because IMAP4 stores messages on the server, users can access their mailboxes from different locations without causing problems. For this reason, IMAP4 is a popular solution on college campuses, in which students in a computer center might use a different system each time they access their email. IMAP4 also enables multiple users to access the same mailbox simultaneously, while a POP3 mailbox can support only one connected user at a time. This can be highly useful in a business environment, such as a help desk that has several people servicing a single email help line.

Exchange Server 2010 Functions

Exchange Server 2010, although based on industry standards, is a proprietary mail and scheduling product that is designed to provide clients with access to local and Internet email, shared calendars and scheduling, task management, and a unified messaging interface that can route other types of traffic, such as voice mail and faxes, to a user's inbox. Windows SBS 2011 automatically installs Exchange Server 2010 with the Windows Server 2008 R2 operating system and configures it to provide these services to your network users.

When you run the Add A New User Account Wizard in the Windows SBS Console, the wizard creates an Exchange Server mailbox for each of your new users using the email address you specify. By default, the email address consists of the user's account name and the name of the Internet domain you specified in the Internet Address Management Wizard, as in the example *marklee@adatum.info*.

Users can access their mailboxes using the Office Outlook Web Access (OWA) site, shown in Figure 15-4, which Windows SBS 2011 creates by default. Users can also access their Exchange Server mailboxes with Microsoft Outlook, but this client is not included with Windows SBS 2011. You must purchase an appropriate edition of Microsoft Office 2010 for your client computers to obtain the Outlook client.



Hello Robin Young,

Mark Lee has installed Windows Small Business Server 2011 Standard on our computer network. Windows SBS provides software and tools that help us work more productively and communicate more effectively with co-workers, customers, and partners.

Here are links to information that helps you learn about the features of the network:

E-Mail

Communicate with your co-workers on the Windows SBS network by using either Microsoft Office Outlook or Outlook Web Access.

FIGURE 15-4 The OWA interface.

The Exchange Server 2010 implementation in Windows SBS 2011 includes POP3 and IMAP4 servers among its capabilities, but by default, the server does not start the Exchange POP3 and Exchange IMAP4 services, which prevents clients from using these protocols to access their Exchange Server mailboxes. If desired, you can start the POP3 or IMAP4 service on your Windows SBS 2011 server, enabling users to access their mailboxes using clients such as Windows Live Mail, the Windows Mail client included in Windows Vista, and the Outlook Express client in Windows XP. However, this solution provides users with email access only. These clients do not support the scheduling and task management features in Exchange Server.

Understanding Email Client Functions

An email client performs two basic functions: it sends outgoing email messages to a server, and it retrieves incoming messages from a server. Virtually all email clients are capable of sending messages to an SMTP server and accessing incoming messages using POP3, IMAP4, or both. Some clients, such as Microsoft Outlook, can also connect to proprietary mail server products, such as Exchange Server 2010.

Many email clients are available, in two major forms: standalone applications and web-based interfaces. Many of the Windows workstation operating systems include an Internet email client: Windows Vista has Windows Mail, and Windows XP and earlier versions have Outlook Express. Windows 7 does not ship with a mail client, but Windows Live Mail is now available as a free download. All these clients include support for SMTP, POP3, and IMAP4 connections, but they cannot connect to Exchange Server except by using these protocols.

To configure an email client to access Internet email, you typically have to specify settings for the following parameters:

- **User name** The name of the user that appears in the client interface.
- **Email address** The address associated with the mailbox that the client accesses.
- **Account name** The name that the client uses to log on to the POP3 or IMAP4 server maintaining the user’s mailbox. This name might or might not be the same as the local part of the email address.
- **Password** The password that the client uses to log on to the POP3 or IMAP4 server.
- **Outgoing server name** The name of the SMTP server to which the client sends outgoing Internet email messages.
- **Outgoing server port number** The port number that the SMTP server uses to receive client transmissions. The default value is 25, and the use of port number 587 is common. However, some servers use nonstandard port numbers.
- **Outgoing server user name and password** Some SMTP servers require clients to log on before they can send outgoing messages. These fields contain the client credentials for the SMTP logon and usually have an option to use the same credentials as the POP3 or IMAP4 server.
- **Incoming server name** The name of the POP3 or IMAP4 server from which the client receives incoming Internet email messages.

- **Incoming server port number** The port number that the POP3 or IMAP4 server uses to receive client transmissions. The default value for POP3 is 110; for IMAP4, the default is 143. The use of nonstandard port numbers for POP3 and IMAP4 is possible, but rare.
- **Server message retention settings** For POP3 server connections, this specifies whether the server should delete messages that the client has finished downloading.

Web-based clients are applications that run on a web server, usually a server belonging to the email service provider. ISPs often provide their customers with both POP3 access, which requires a standalone client, and a web-based interface, which runs on their own servers. Other mail providers, such as Windows Live Hotmail, provide only a web interface, although there are standalone clients that can access these web mail servers using a Hypertext Transfer Protocol (HTTP) connection and download messages to the local drive.

Proprietary clients and server mail solutions can use any communications protocol the developers want. Outlook, for example, is designed primarily to connect to Exchange Server computers on the same local network and uses a proprietary protocol called *Messaging Application Programming Interface/Remote Procedure Call (MAPI/RPC)*. However, you can also configure Outlook to access a POP3 or IMAP4 server on the Internet for incoming mail and an Internet-based SMTP server for outgoing messages.

Understanding Internet Email Communications

For internal email, clients on your Windows SBS network simply send their outgoing messages to the server, which places them in the appropriate destination mailboxes. For users connecting with OWA, the messages never actually leave the server because the OWA site and Exchange Server are running on the same computer. However, email communications involving the Internet are somewhat more complex.

An Internet email transaction consists of these steps:

1. A user on your network launches a client, creates an email message with a destination address in another domain, and sends it.
2. The client sends the email message to an SMTP server. In the case of a client on your Windows SBS 2011 network, Exchange Server 2010, running on your primary server, can provide the outgoing SMTP service.
3. The SMTP server reads the destination email address from the outgoing message.
4. The SMTP server generates a DNS request containing the destination domain name and sends it to its DNS server (on a Windows SBS 2011 network, the same computer also functions as the DNS server).
5. The DNS server forwards the request to other DNS servers on the Internet as needed until it locates the authoritative DNS server for the destination domain.

MORE INFO For more information on DNS servers and resource records, see Chapter 2.

6. The destination domain's DNS server responds by sending the Mail Exchanger (MX) record for the domain to the DNS server on your network.
7. The SMTP server receives the FQDN of the destination mail server from the DNS server.
8. The SMTP server initiates another DNS transaction, this time to resolve the destination mail server's name into an IP address.
9. The SMTP server receives the IP address of the destination mail server from its DNS server.
10. The SMTP server transmits the email message to the IP address of the mail server for the destination domain using the SMTP protocol.
11. The destination mail server, which can be another computer running Exchange Server or a POP3 or IMAP4 server, receives the message, reads the local part of the destination address, and places the message in the mailbox for the appropriate user.
12. At some future time, the recipient connects to his or her email server using a client, and accesses the message, either by downloading it or reading it in place.

Connecting an Exchange Server to the Internet

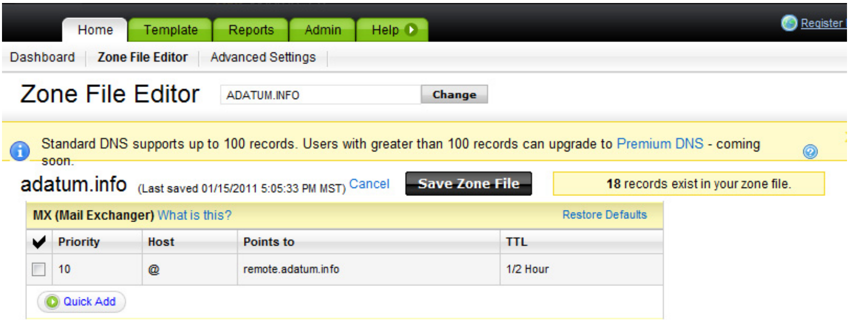
Thus far, this chapter has discussed two types of email systems that are essentially separate. SMTP, POP3, and IMAP4 servers are designed to send and receive email over the Internet, while Exchange Server 2010 is a proprietary solution that was initially designed for internal messaging on a private network. How, then, do you bring the two together so that your users can send messages to and receive them from users on both the local network and on the Internet?

There are several ways to answer this question, as Exchange Server 2010 is a highly flexible application. However, as with most of the powerful technologies it includes, Windows SBS 2011 selects and implements a configuration that is acceptable to most small business administrators.

The default Exchange Server 2010 configuration in Windows SBS 2011 is first an internal email server that enables the users on the network to communicate. When users log on to the Active Directory Domain Services (AD DS) domain, they receive access to their Exchange Server mailboxes on the primary Windows SBS server. Remote users working from home or any other location can use the Remote Web Access site to access their Exchange Server mailboxes through the Internet. This internal network access provides users with the full email, scheduling, and task management capabilities of Exchange Server.

When a network user sends an email message to an addressee on the Internet, the Windows SBS server receives the message by default and uses the SMTP server capabilities in Exchange Server 2010 to locate the destination mail server and transmit the message over the Internet. When an Internet user sends an email message to one of your network users, using an address in the Internet domain you registered with the Internet Address Management Wizard, your server receives the message and deposits it in the user's mailbox.

Your Windows SBS server is accessible to mail servers on the Internet because the Internet Address Management Wizard automatically creates an MX resource record on the DNS server that is authoritative for your domain, as shown in Figure 15-5. The MX record contains the FQDN of your server, with the host name *remote*, plus your Internet domain name, as in *remote.adatum.info*. As a result, other SMTP servers on the Internet are able to forward messages to your server.



ADATUM.INFO

Standard DNS supports up to 100 records. Users with greater than 100 records can upgrade to Premium DNS - coming soon.

adatum.info (Last saved 01/15/2011 5:05:33 PM MST) Cancel

18 records exist in your zone file.

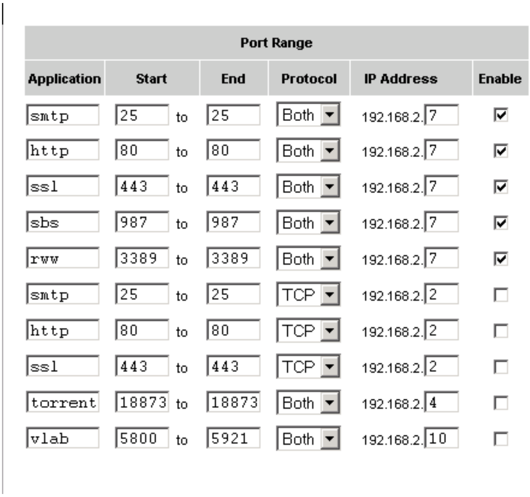
MX (Mail Exchanger) What is this?

✔	Priority	Host	Points to	TTL
□	10	@	remote.adatum.info	1/2 Hour

FIGURE 15-5 The MX resource record created by the Internet Address Management Wizard.

As noted in Chapter 2, the *Mail Exchange (MX)* record is a specialized DNS resource record that specifies the name of a mail server that is authoritative for the domain. Without an MX record, there is no way for email messages on the Internet to reach that domain. In addition to the MX record, the authoritative DNS server for the domain must also have a Host (A) record that supplies the IP address equivalent for the mail server.

The Internet Address Management Wizard also configures your router to forward the incoming SMTP traffic on port 25 to your server, as shown in Figure 15-6. These two settings (the MX record and the router configuration) complete the route from the mail servers on the Internet to your mail server on your private network.



Port Range						
Application	Start		End	Protocol	IP Address	Enable
smtp	25	to	25	Both	192.168.2.7	☑
http	80	to	80	Both	192.168.2.7	☑
ssl	443	to	443	Both	192.168.2.7	☑
sbs	987	to	987	Both	192.168.2.7	☑
rww	3389	to	3389	Both	192.168.2.7	☑
smtp	25	to	25	TCP	192.168.2.2	□
http	80	to	80	TCP	192.168.2.2	□
ssl	443	to	443	TCP	192.168.2.2	□
torrent	18873	to	18873	Both	192.168.2.4	□
vlab	5800	to	5921	Both	192.168.2.10	□

FIGURE 15-6 A typical router configuration interface.

> ***MORE INFO*** **There are situations in which you might have to configure both of these settings manually, such as when you register your domain name with a registrar not supported by the Internet Address Management Wizard, or when the wizard cannot automatically configure your router. These manual configuration tasks are not difficult, but they depend on the interfaces provided by your domain registrar and your router. For more information on the tasks performed by the Internet Address Management Wizard, see Chapter 4, "Getting Started."**

Configuring Email Settings in Windows SBS 2011

Although the Windows SBS 2011 setup program automatically installs and configures Exchange Server 2010, you might want to perform some additional configuration tasks, which are described in the following sections.

Configure a Smart Host for Internet Email

The Internet email transmission process, as described earlier in this chapter, might seem quite complicated, but it actually is quite efficient under ideal conditions. However, if a destination mail server is not available to receive messages, Exchange Server must keep retrying the transmission until it reaches its timeout interval. This means that the delivery of a single email could require the server to transmit dozens of messages over the network's Internet connection. Multiply this by the hundreds or thousands of email messages that the server sends every day, and you can see how this can bog down the server's performance and consume a significant amount of Internet bandwidth.

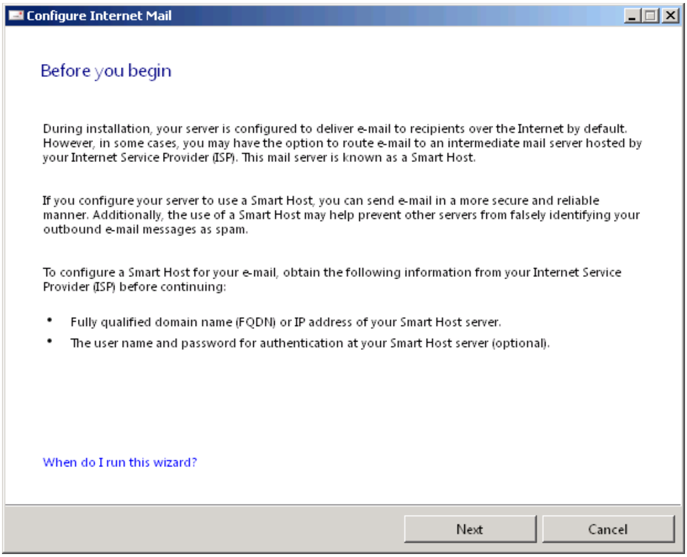
Another problem with this arrangement is the fact that many Internet servers assume that messages originating from dynamic IP addresses are spam. Most ISPs assign dynamic IP addresses to their clients, including the broadband routers that Windows SBS 2011 networks typically use to access the Internet. Therefore, you might find that some of your outgoing email messages are failing to reach their destinations because intermediate servers are discarding them as spam.

One way to overcome these problems is to use a smart host to transmit your Internet email. A *smart host* is an SMTP server, typically supplied by your ISP, that functions as an interim mail stop for your domain. You configure Exchange Server to send all its outgoing mail to the smart host, and the smart host is then responsible for transmitting and retransmitting the individual messages to their destinations as needed. In addition, because the smart host has a static IP address, its traffic is less likely to be perceived as spam.

The *Getting started tasks* list in the Windows SBS Console provides access to a wizard that configures Exchange Server 2010 to use a smart host. To run this wizard, perform the following:

1. Log on to your Windows SBS 2011 primary server using an account with network Administrator privileges. The Windows SBS Console appears.
2. On the Home page of the Windows SBS Console, click *Configure a smart host for Internet e-mail*. The Configure Internet Mail Wizard appears, displaying the Before You Begin page.

   TIP **The Configure Internet Mail Wizard is also accessible from the Network/Connectivity page of the Windows SBS Console. To start the wizard, click *Smart host for Internet e-mail* in the Internet E-Mail section.**



Configure Internet Mail

Before you begin

During installation, your server is configured to deliver e-mail to recipients over the Internet by default. However, in some cases, you may have the option to route e-mail to an intermediate mail server hosted by your Internet Service Provider (ISP). This mail server is known as a Smart Host.

If you configure your server to use a Smart Host, you can send e-mail in a more secure and reliable manner. Additionally, the use of a Smart Host may help prevent other servers from falsely identifying your outbound e-mail messages as spam.

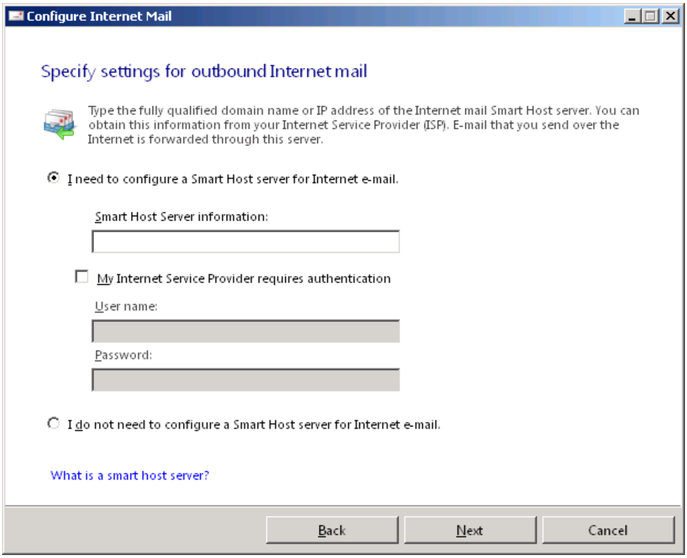
To configure a Smart Host for your e-mail, obtain the following information from your Internet Service Provider (ISP) before continuing:

- Fully qualified domain name (FQDN) or IP address of your Smart Host server.
- The user name and password for authentication at your Smart Host server (optional).

When do I run this wizard?

The Before You Begin page lists the resources you must have to complete the wizard, which include the FQDN or IP address of the smart host you intend to use. You obtain this information from your ISP or other provider. In most cases, ISPs require authentication to access the mail server, so you need a user name and password as well.

3. Click *Next*. The Specify Settings For Outbound Internet Mail page appears.



Configure Internet Mail

Specify settings for outbound Internet mail

Type the fully qualified domain name or IP address of the Internet mail Smart Host server. You can obtain this information from your Internet Service Provider (ISP). E-mail that you send over the Internet is forwarded through this server.

● I need to configure a Smart Host server for Internet e-mail.

Smart Host Server information:

□ My Internet Service Provider requires authentication

User name:

Password:

○ I do not need to configure a Smart Host server for Internet e-mail.

What is a smart host server?

4. Leave the *I need to configure a smart host server for Internet e-mail* option selected and, in the *Smart host server information* text box, type the name or IP address of the server you want to use.
5. If necessary, select the *My Internet service provider requires authentication* check box and, in the *User name* and *password* text boxes, type the credentials for the server, as supplied by your ISP.
6. Click *Next*. The Configuring Internet E-Mail Settings page appears as the wizard attempts to contact the server you specified. If the attempt succeeds, the Configure Internet Mail Settings Is Complete page appears.

   If the wizard cannot connect to the server, it specifies the nature of the problem, such as a nonexistent server or rejected credentials, allows you to correct your settings, and tries again. Keep altering your settings until the wizard connects.
7. Click *Finish*. The wizard closes.

Using the POP3 Connector

One of the byproducts of the email age is the proliferation of email addresses that people tend to gather. The Add A New User Account Wizard creates a new mailbox for each user on the network, but he or she might already have other email addresses as well, addresses from personal accounts or other affiliations. There are two ways to incorporate email from other sources into users' Exchange Server mailboxes:

- Configure the Office Outlook client on each individual workstation to access the external accounts.
- Use the POP3 Connector in Windows SBS 2011 to access the external accounts.

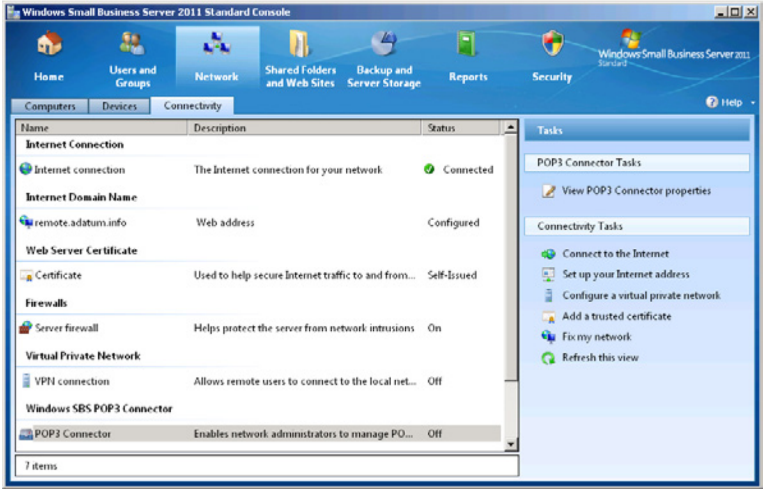
In addition to functioning as an Exchange Server client, Office Outlook is a POP3 and IMAP4 client. When you add a POP3 account to an Outlook client that is already configured to access an Exchange Server mailbox, you can integrate the messages downloaded from the POP3 server into the mailbox so that the program permanently stores them on the Exchange Server computer. With this arrangement, you must configure each individual client with the appropriate configuration settings for the POP3 account, and the system can check the POP3 server for new messages only while the client is running on the workstation.

The POP3 Connector is essentially a multiuser POP3 client that runs on Exchange Server, which you configure with the account information for each of your users. The POP3 Connector checks each of the POP3 accounts at scheduled intervals, downloads new messages, and deposits them in the correct users' mailboxes. With the

POP3 Connector, server administrators manage the account information, and the connector runs all the time, downloading new messages even when the clients are not logged on to the network.

To use the POP3 Connector, you must have the server name and user credentials for each POP3 account you want the server to access. To configure the POP3 Connector, follow these steps:

1. Log on to your Windows SBS 2011 primary server using an account with network Administrator privileges. The Windows SBS Console appears.
2. Click *Network*, and then select the *Connectivity* tab.


Windows Small Business Server 2011 Standard Console
Home
Users and Groups
Network
Shared Folders and Web Sites
Backup and Server Storage
Reports
Security
Windows Small Business Server 2011 Standard
Computers
Devices
Connectivity
Help

Name	Description	Status
Internet Connection		
Internet connection	The Internet connection for your network	Connected
Internet Domain Name		
remote.adatum.info	Web address	Configured
Web Server Certificate		
Certificate	Used to help secure Internet traffic to and from...	Self-Issued
Firewalls		
Server firewall	Helps protect the server from network intrusions	On
Virtual Private Network		
VPN connection	Allows remote users to connect to the local net...	Off
Windows SBS POP3 Connector		
POP3 Connector	Enables network administrators to manage PO...	Off

7 items

Tasks

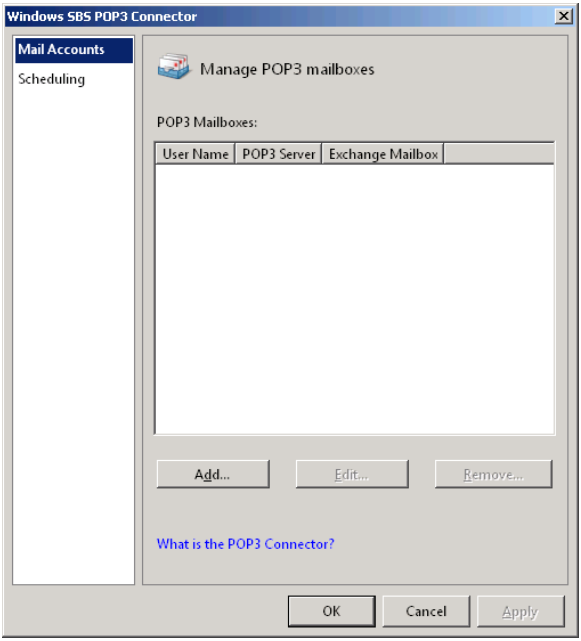
POP3 Connector Tasks

- View POP3 Connector properties

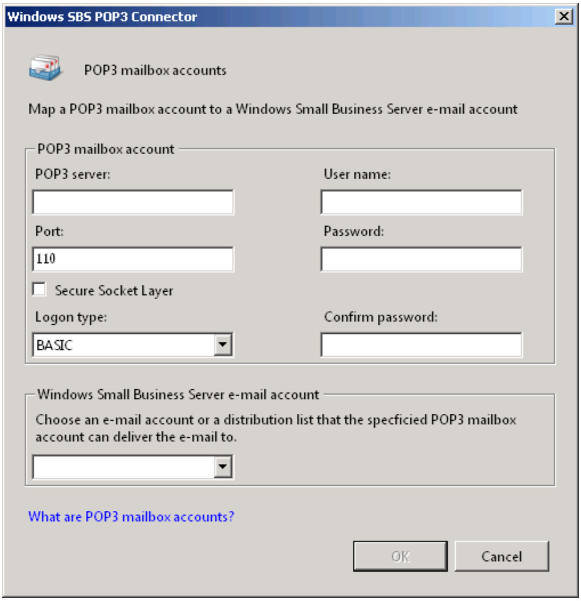
Connectivity Tasks

- Connect to the Internet
- Set up your Internet address
- Configure a virtual private network
- Add a trusted certificate
- Fix my network
- Refresh this view

3. Under Windows SBS POP3 Connector, select the *POP3 Connector* item, and in the *Tasks* list, click *View POP3 Connector properties*. The Windows SBS POP3 Connector dialog box appears. You must add each POP3 account you want the connector to access to the POP3 Mailboxes list.



4. With the *Mail accounts* tab selected, click *Add*. The Pop3 Mailbox Accounts dialog box appears.



Map a POP3 mailbox account to a Windows Small Business Server e-mail account

POP3 mailbox account

POP3 server:

User name:

Port: 110

Password:

□ Secure Socket Layer

Logon type: BASIC

Confirm password:

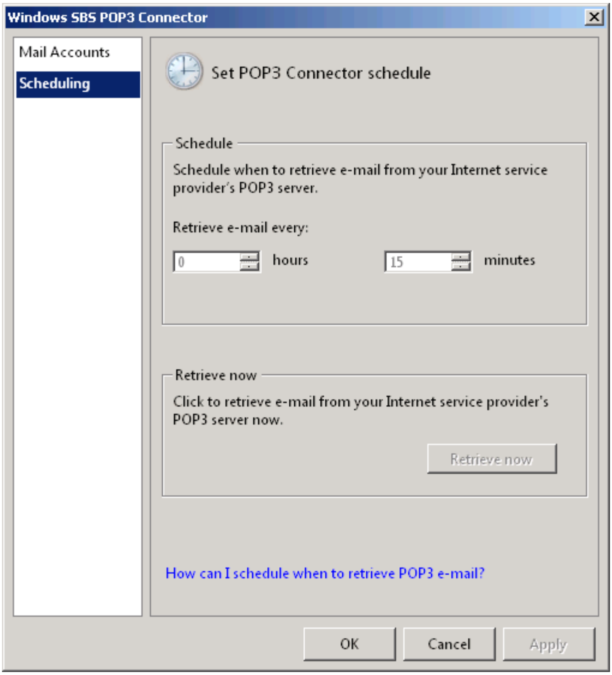
Windows Small Business Server e-mail account

Choose an e-mail account or a distribution list that the specficied POP3 mailbox account can deliver the e-mail to.

5. In the *POP3 mailbox account* box, configure the following settings:
   - **POP3 server** Specifies the name or IP address of the Internet server hosting the POP3 mailbox you want to access.
   - **Port** Specifies the port number the server is using for POP3 traffic. The default value is 110.
   - **Secure Socket Layer** Configures SSL encryption for the POP3 connection, if the server supports it.
   - **Logon type** Specifies which of the following authentication methods you want the server to use when connecting to the POP3 server: Basic, Secure Password Authentication (SPA), or Authenticated Post Office Protocol (APOP).

   NOTE **The Basic option uses plain text authentication, SPA encrypts the password before transmission, and APOP combines the password with a timestamp before encrypting it. This is done to create a unique value during each logon. APOP is more secure than SPA because it prevents potential attackers from capturing the encrypted passwords and replaying them. However, you must make sure that the POP3 server supports SPA or APOP authentication before you select these options.**

   - **User name** Specifies the account name you want the server to use when logging on to the POP3 server.
   - **Password and Confirm Password** Specify the password associated with the user name.
6. In the *Windows Small Business Server e-mail account* drop-down list, select the mailbox to which the connector should deposit the downloaded messages.
7. Click *OK*. The new account appears in the POP3 *Mailboxes* list.
8. Repeat steps 4 through 7 to configure additional POP3 mailboxes.
9. Click the *Scheduling* tab.


Windows SBS POP3 Connector
Mail Accounts
Scheduling
Set POP3 Connector schedule

Schedule

Schedule when to retrieve e-mail from your Internet service provider's POP3 server.

Retrieve e-mail every:

0 hours 15 minutes

Retrieve now

Click to retrieve e-mail from your Internet service provider's POP3 server now.

Retrieve now
How can I schedule when to retrieve POP3 e-mail?
OK
Cancel
Apply

10. In the *Schedule* box, specify the interval at which the server should check the POP3 accounts for new mail.

TIP **You can also trigger an immediate check of the POP3 accounts by clicking *Retrieve now.***

11. Click *OK*.

Setting Mailbox Quotas

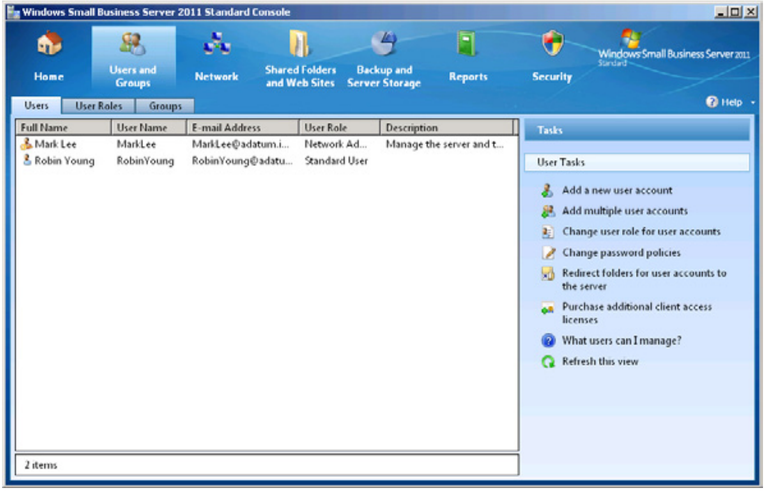
User mailboxes can grow to an enormous unwieldy size, especially when email messages carry attachments. To prevent mailboxes from growing too large, Windows SBS 2011 has the ability to impose quotas that issue warnings and ultimately stop saving incoming mail when a mailbox reaches a specified size. Windows SBS enables mailbox quotas by default and sets them to a maximum size of 2 gigabytes (GB). When a user's mailbox is within 100 megabytes (MB) of the quota limit, Exchange Server issues a warning. When the mailbox reaches the quota limit, Exchange Server stops sending and receiving mail for that user.

To reduce the size of a mailbox that has reached its quota limit, the user can delete some of the messages or archive them to another location using the capabilities of the client program. The administrator can also choose to increase the quota.

NOTE **In Windows SBS 2011, mailbox quotas are a function of Exchange Server 2010, not the File Server Resource Manager, which implements the default user share and folder redirection quotas. To modify mailbox quotas with greater precision, you must use the Exchange Management Console.**

To enable, disable, or modify quotas for specific mailboxes, use the following procedure:

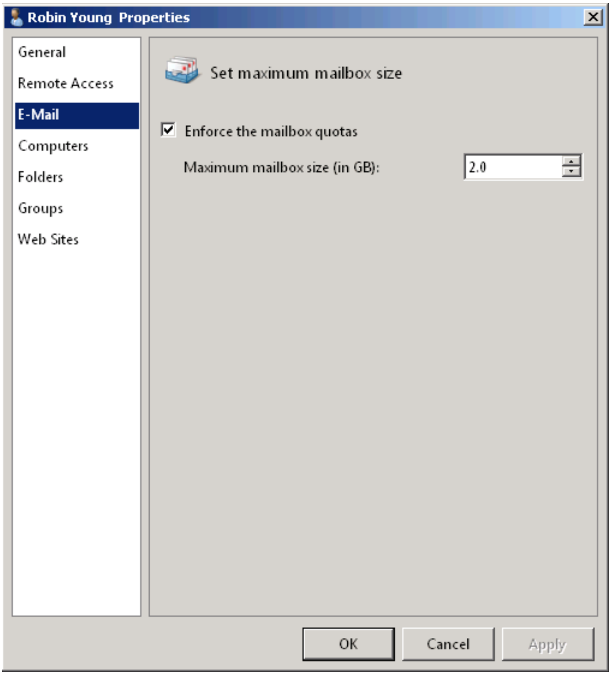
1. Log on to your Windows SBS 2011 primary server using an account with network Administrator privileges. The Windows SBS Console appears.
2. Click *Users and groups*, and then select the *Users* tab.


Windows Small Business Server 2011 Standard Console
Home
Users and Groups
Network
Shared Folders and Web Sites
Backup and Server Storage
Reports
Security
Windows Small Business Server 2011 Standard
Users
User Roles
Groups
Help
Tasks
User Tasks
Add a new user account
Add multiple user accounts
Change user role for user accounts
Change password policies
Redirect folders for user accounts to the server
Purchase additional client access licenses
What users can I manage?
Refresh this view

Full Name	User Name	E-mail Address	User Role	Description
Mark Lee	MarkLee	MarkLee@adatum.i...	Network Ad...	Manage the server and t...
Robin Young	RobinYoung	RobinYoung@adatu...	Standard User	

2 items

3. Select the user whose quota you want to modify and, from the *Tasks* list, select *Edit user account properties*. The Properties sheet for the user appears.
4. Click the *E-mail* tab.



☑ Enforce the mailbox quotas

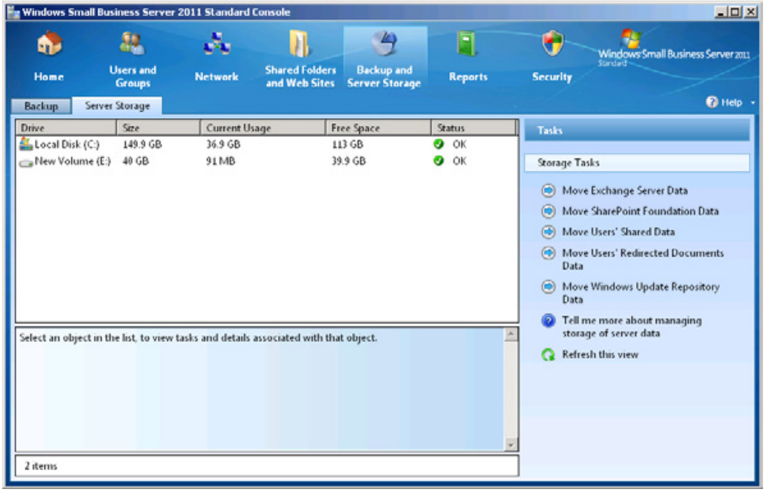
Maximum mailbox size (in GB): 2.0

5. To disable the mailbox quota, clear the *Enforce the mailbox quotas* check box. To modify the quota size, change the value in the *Maximum mailbox size* box.
6. Click *OK* to close the Properties sheet.

Moving Exchange Server Data

Because the Windows SBS 2011 setup program installs Exchange Server 2008 along with the operating system, you cannot choose the disk where Exchange Server creates its message stores. However, Windows SBS 2011 does provide a wizard that enables you to move the message stores at any time. Therefore, if you want to put the mailboxes on a fault-tolerant volume, or even if you just need more disk space for them, you can move the message stores with this procedure:

1. Log on to your Windows SBS 2011 primary server using an account with network Administrator privileges. The Windows SBS Console appears.
2. Click *Backup and server storage*, and then select the *Server storage* tab.

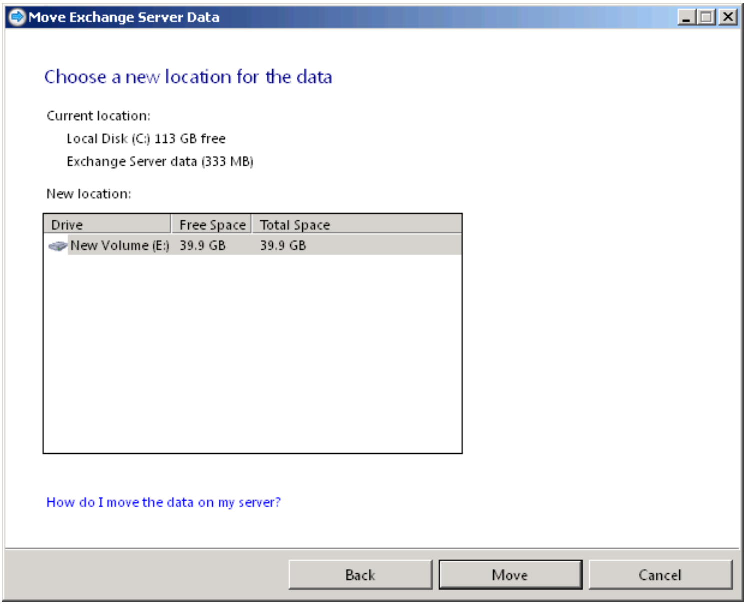

Windows Small Business Server 2011 Standard Console
Home
Users and Groups
Network
Shared Folders and Web Sites
Backup and Server Storage
Reports
Security
Windows Small Business Server 2011 Standard
Backup
Server Storage
Help
Tasks
Storage Tasks
Move Exchange Server Data
Move SharePoint Foundation Data
Move Users' Shared Data
Move Users' Redirected Documents Data
Move Windows Update Repository Data
Tell me more about managing storage of server data
Refresh this view

Drive	Size	Current Usage	Free Space	Status
Local Disk (C:)	149.9 GB	36.9 GB	113 GB	OK
New Volume (E:)	40 GB	91 MB	39.9 GB	OK

Select an object in the list, to view tasks and details associated with that object.

2 items

3. In the *Tasks* list, select *Move Exchange Server data*. The Move Exchange Server Data Wizard appears.
4. Click *Next* to bypass the Getting Started page. The wizard checks your server's backup status and searches for available volumes. If your server is not configured to perform regular backups, the Server Backup Is Not Configured dialog box appears.
5. Click *OK* to close the Server Backup Is Not Configured dialog box. The Choose A New Location For The Data page appears.



Move Exchange Server Data

Choose a new location for the data

Current location:

Local Disk (C:) 113 GB free

Exchange Server data (333 MB)

New location:

Drive	Free Space	Total Space
New Volume (E:)	39.9 GB	39.9 GB

How do I move the data on my server?

6. Select the volume where you want to move the Exchange Server data and click *Move*. The wizard moves the data to the volume you selected, and the Exchange Server Data Was Moved Successfully page appears.
7. Click *Finish*. The wizard closes.

CHAPTER 16

Working with Websites

Windows Small Business Server (SBS) 2011 relies heavily on web-based applications for many of its client communication and administration tasks. One of the biggest favors that the setup program does for you during the Windows SBS 2011 installation is to create and configure your server to host many different internal websites, tasks that would take hours if you had to perform them manually. Once created and configured, these websites need little attention from administrators, but you can customize them to accommodate the needs of your users.

Introducing Internet Information Services 7.0

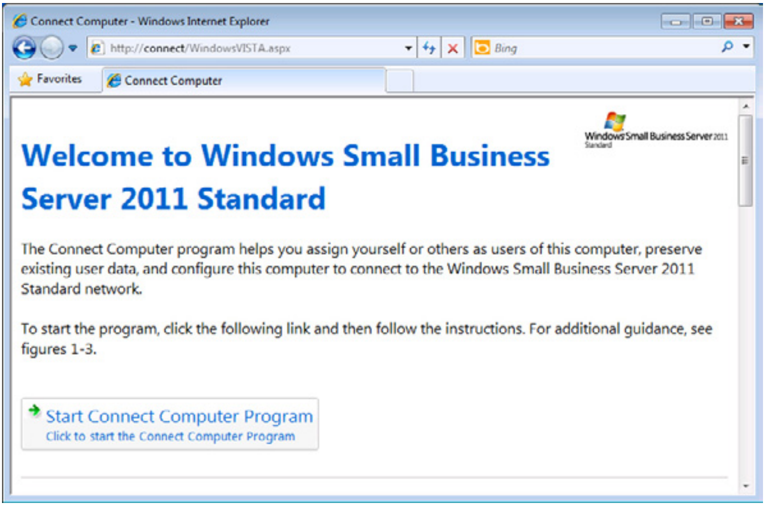
Internet Information Services (IIS) 7.0 is the web server application supplied with Windows Server 2008 R2 and Windows SBS 2011. In the early days of the Web, a web server was nothing more than an application that listened for incoming requests from browsers and responded to those requests by sending *Hypertext Markup Language (HTML)* files in return, using an application layer protocol called *Hypertext Transfer Protocol (HTTP)*. Today, however, web servers are far more complex. They can supply browsers with many other types of files, including images, audio, and video. Web servers can also host applications that are designed to use a browser as a client, communicating with a variety of protocols. Over the years, IIS has evolved into a comprehensive web server product that can host multiple websites and applications simultaneously, providing a wide variety of client and administrative services.

Introducing the Windows SBS 2011 Default Websites

Windows SBS 2011 uses IIS to provide clients with a variety of services, including the following:

- **Client deployment** When you join a client workstation to your Windows SBS 2011 network, you use Internet Explorer to access a site called *Connect*. Connect is an intranet web application hosted by IIS on your Windows SBS server. The application checks the client computer for the necessary prerequisites and enables the user to download and run a program called Launcher.exe, which starts the Connect Computer Wizard. This wizard joins the computer to the domain and performs a large number of workstation setup tasks that would otherwise require an administrator's presence.

  MORE INFO **For more information on the Connect website and the tasks performed by the Connect Computer Wizard, see the section entitled "Working with Computers," in Chapter 6, "Working with Users, Computers, and Groups."**


Connect Computer - Windows Internet Explorer
http://connect/WindowsVISTA.aspx
Bing
Favorites
Connect Computer
Windows Small Business Server 2011 Standard

Welcome to Windows Small Business Server 2011 Standard

The Connect Computer program helps you assign yourself or others as users of this computer, preserve existing user data, and configure this computer to connect to the Windows Small Business Server 2011 Standard network.

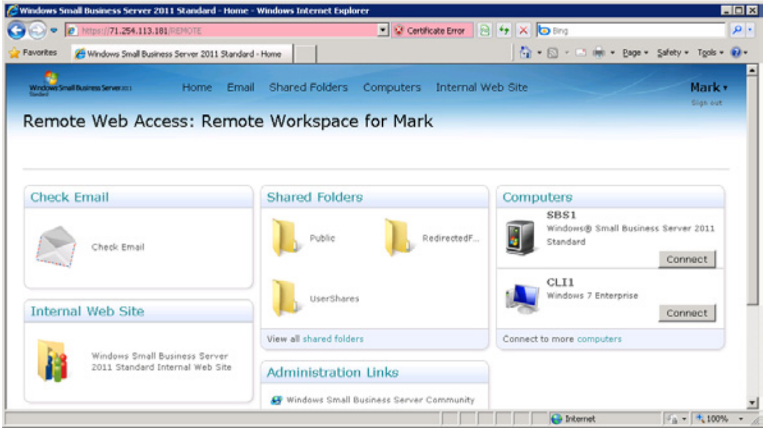
To start the program, click the following link and then follow the instructions. For additional guidance, see figures 1-3.

Start Connect Computer Program
Click to start the Connect Computer Program

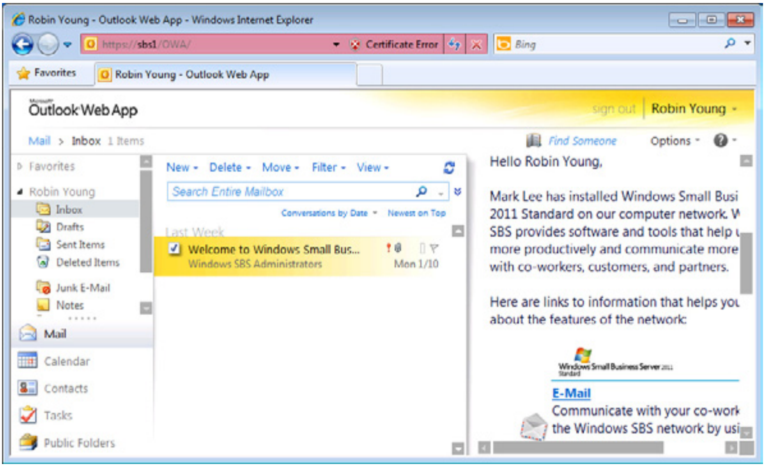
- **Windows Server Update Services (WSUS)** WSUS provides the computers on your Windows SBS network with operating system and application updates that it obtains from the Microsoft Update servers on the Internet. Although it is not visible to the network users, WSUS does this by creating an alternative to the Microsoft Updates Web site on your Windows SBS server.

MORE INFO **For more information about WSUS, see Chapter 11, "Deploying Updates."**

- **Remote Web Access (RWA)** RWA is a portal site that provides network users at remote locations with access to your Windows SBS network resources via the Internet, using the interface shown here.


Windows Small Business Server 2011 Standard - Home - Windows Internet Explorer
https://71.254.113.181/REMOTE
Certificate Error
Bing
Favorites
Windows Small Business Server 2011 Standard - Home
Page
Safety
Tools
Windows Small Business Server 2011 Standard
Home
Email
Shared Folders
Computers
Internal Web Site
Mark
Sign out
Remote Web Access: Remote Workspace for Mark
Check Email
Check Email
Shared Folders
Public
RedirectedF...
UserShares
View all shared folders
Computers
SBS1
Windows® Small Business Server 2011 Standard
Connect
CLI1
Windows 7 Enterprise
Connect
Connect to more computers
Internal Web Site
Windows Small Business Server 2011 Standard Internal Web Site
Administration Links
Windows Small Business Server Community
Internet
100%

- **Office Outlook Web Access (OWA)** OWA is a web-based client for the Microsoft Exchange Server 2010 mail server incorporated into Windows SBS 2011. Unlike earlier versions of Windows SBS, which include Microsoft Office Outlook, OWA is the only Exchange Server client supplied with the Windows SBS 2011 and Windows SBS 2008 products. Users on the internal network can access the OWA site directly, and remote users on the Internet can access it through the RWA site.



Hello Robin Young,

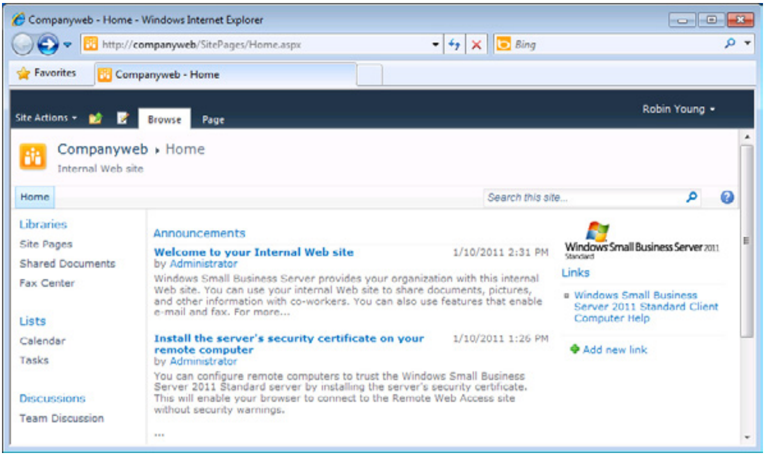
Mark Lee has installed Windows Small Busi
2011 Standard on our computer network. W
SBS provides software and tools that help u
more productively and communicate more
with co-workers, customers, and partners.

Here are links to information that helps you
about the features of the network:

E-Mail

Communicate with your co-work
the Windows SBS network by usi

- **SharePoint Foundation 2010** The Companyweb site is a database-enabled web application implemented by SharePoint Foundation Services 2010, which provides Windows SBS users with several collaboration tools, such as document storage, discussion groups, shared calendars, and task lists. Using the host name *companyweb*, this is the main internal website for Windows SBS 2011 users.



Welcome to your Internal Web site 1/10/2011 2:31 PM
by Administrator

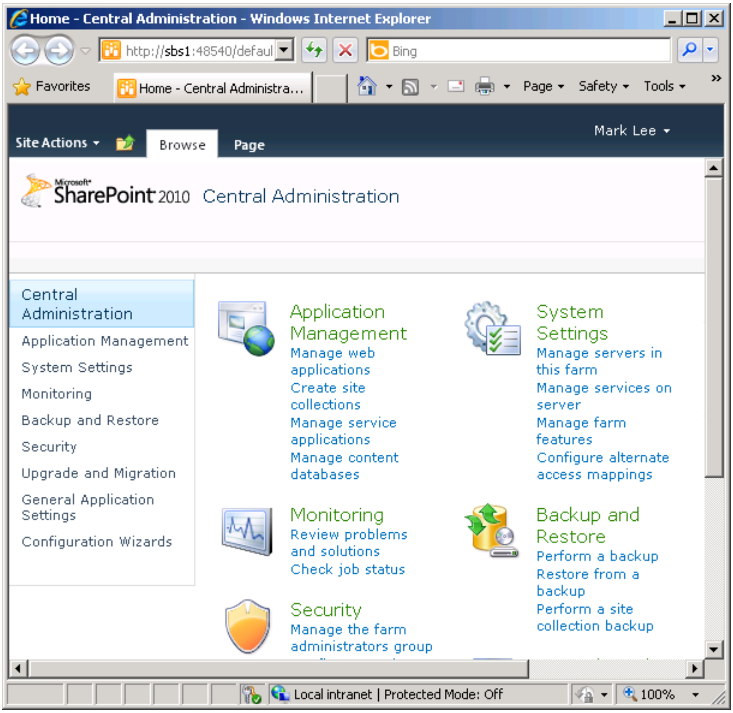
Windows Small Business Server provides your organization with this internal Web site. You can use your internal Web site to share documents, pictures, and other information with co-workers. You can also use features that enable e-mail and fax. For more...

Install the server's security certificate on your remote computer 1/10/2011 1:26 PM
by Administrator

You can configure remote computers to trust the Windows Small Business Server 2011 Standard server by installing the server's security certificate. This will enable your browser to connect to the Remote Web Access site without security warnings.

...

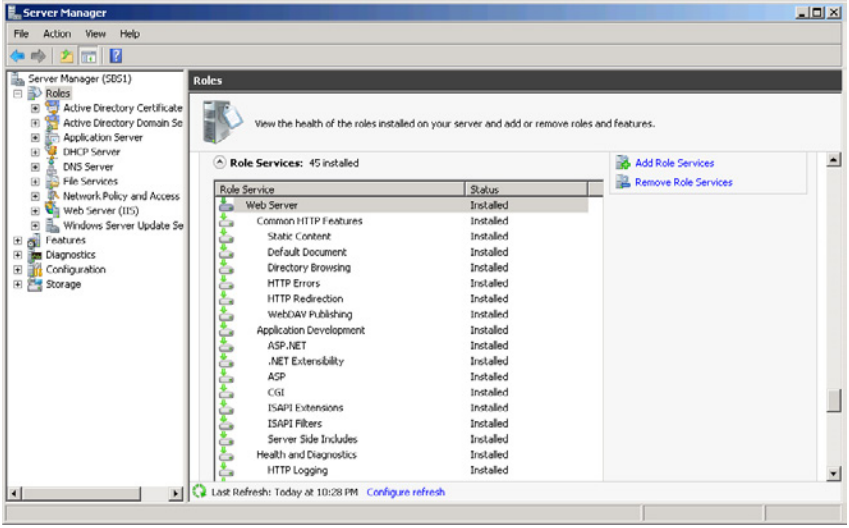
- **SharePoint Central Administration** SharePoint Central Administration creates a separate website that provides administrative control over the main SharePoint site.



MORE INFO **For more information on using and managing the SharePoint sites, see Chapter 17, "Working with SharePoint."**

Understanding the IIS Architecture

IIS takes the form of a role in the Windows Server 2008 R2 operating system. The Windows SBS 2011 setup program installs and configures eight different roles on your server during the installation process, among them the *Web Server (IIS)* role. The Web Server (IIS) role is a modular service that has 46 *role services*, as shown in Figure 16-1, which provide IIS with various security, management, logging, and application capabilities. By default, Windows SBS 2011 installs all the IIS role services except for those which compose the FTP Server, although it does not necessarily require all the role services it installs.



View the health of the roles installed on your server and add or remove roles and features.

Role Services: 45 installed

Role Service	Status
Web Server	Installed
Common HTTP Features	Installed
Static Content	Installed
Default Document	Installed
Directory Browsing	Installed
HTTP Errors	Installed
HTTP Redirection	Installed
WebDAV Publishing	Installed
Application Development	Installed
ASP.NET	Installed
.NET Extensibility	Installed
ASP	Installed
CGI	Installed
ISAPI Extensions	Installed
ISAPI Filters	Installed
Server Side Includes	Installed
Health and Diagnostics	Installed
HTTP Logging	Installed

Last Refresh: Today at 10:28 PM Configure refresh

FIGURE 16-1 The Web Server (IIS) role services.

In a Windows Server 2008 R2 installation, IIS has one default website with a placeholder splash screen, which uses the standard port for HTTP communications, port 80. This site and the splash screen are still accessible on a Windows SBS 2011 server if you use a Uniform Resource Locator (URL) containing only the server's name or Internet Protocol (IP) address, as shown in Figure 16-2. However, the default IIS installation in Windows SBS 2011 also includes several other sites, which are accessible using various other URLs.

In IIS, a *site* is an individual set of web pages that is separate from the other sites running on the computer. In Windows SBS 2011, the default IIS sites are all intended for use by a single organization, but it is also possible to use IIS to create completely separate sites for different companies, each with its own content and configuration settings. With IIS, you can create as many additional sites as your server hardware can support. You create and manage sites using the Internet Information Services (IIS) Manager application, as shown in Figure 16-3.

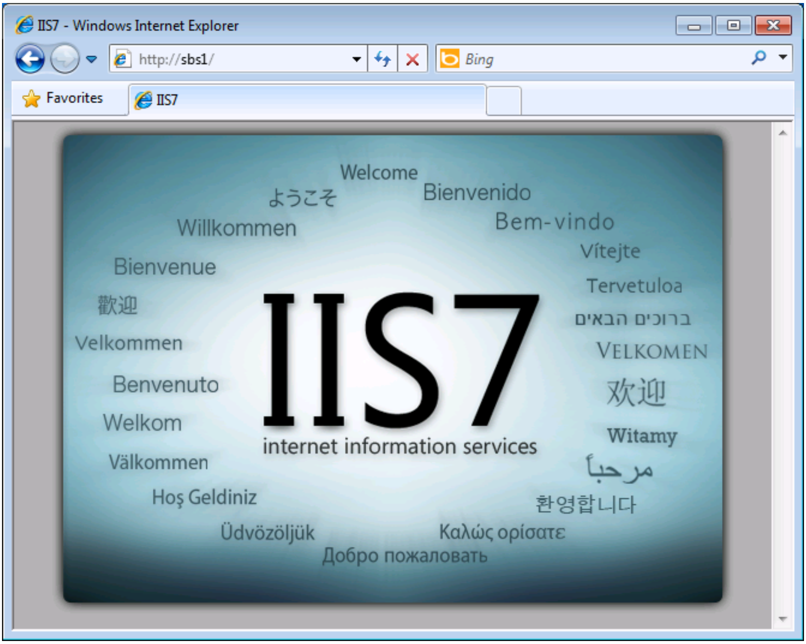
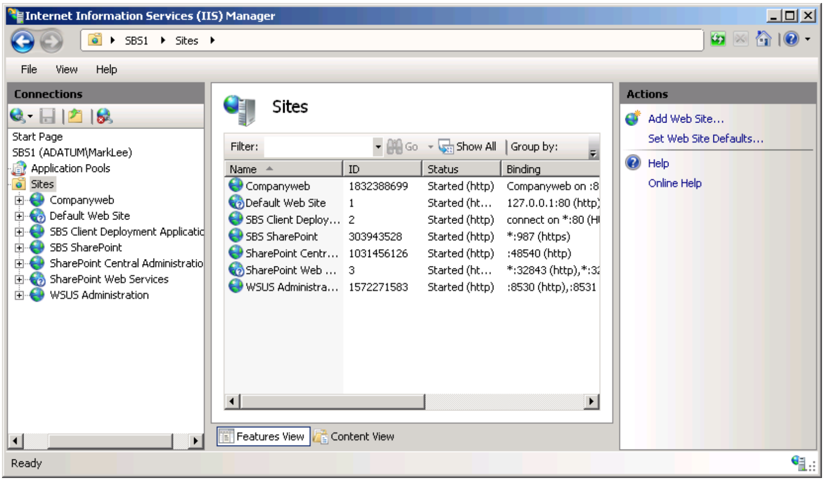


FIGURE 16-2 The default IIS website.



Name	ID	Status	Binding
Companyweb	1832388699	Started (http)	Companyweb on :8
Default Web Site	1	Started (ht...	127.0.0.1:80 (http)
SBS Client Deploy...	2	Started (http)	connect on *:80 (H
SBS SharePoint	303943528	Started (http)	*:987 (https)
SharePoint Centr...	1031456126	Started (http)	:48540 (http)
SharePoint Web ...	3	Started (ht...	*:32843 (http),*:3
WSUS Administra...	1572271583	Started (http)	:8530 (http),:8531

FIGURE 16-3 The default Windows SBS sites in the Internet Information Services (IIS) Manager.

Each site points to a location on a local drive that holds the files containing the site's content, such as HTML, image, and application files. Working with the content is a matter of creating and editing the files at this location.

IIS also supports the use of *virtual directories*, which are pointers to other locations on the same computer or on the local network. For example, if you have a site with its home directory on the local drive, but you want to publish some files located on another computer, you can either copy those files to the home directory (which can cause version synchronization problems) or just create a virtual directory on the site that points to the folder on the other computer. The files appear on the site, yet remain in their original location.

Running Multiple Sites

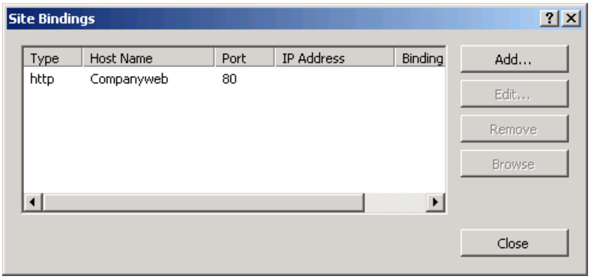
Hosting multiple websites on a single server presents a problem for IIS. When web browsers connect to a site, they do so by sending an HTTP request message to the web server's IP address using the well-known HTTP port number 80. When requests for different sites arrive at the server, how is IIS supposed to differentiate them and forward each request to the correct site?

The answer is by configuring each site with a different set of bindings. *Bindings* are rules that tell IIS how to associate incoming requests with specific sites. IIS supports three types of bindings, as follows:

- **IP address** It is possible to assign more than one IP address to a single computer. By doing this, you can configure IIS to use a different address for each site. However, you must also register a different name in a Domain Name System (DNS) domain for each address.
- **Port number** Web browsers send all their HTTP requests to port 80 on the destination server unless the user specifies a different port number in the URL. You can create bindings that assign a different port number to each site on an IIS server, enabling the server to distinguish among the incoming requests. However, to access a site that uses a nonstandard port number, users must specify that number in their URLs, following the server name and a colon, as in the example *www.adatum.com:1024*. In Windows SBS 2011, the WSUS site uses port number bindings because the URL that Windows Update clients use to access the web server, which contains the port number 8530, is hidden from users in a Group Policy object (GPO). In a situation like this, in which users do not have to remember the port number and type it in a URL, port number bindings are a viable option. Another reason to use port number bindings is to keep a site hidden from the average user. The SharePoint Central Administration site on your server uses a nonstandard port number, which is unknown to the network users, but which administrators can access through the Windows Small Business Server 2011 Standard Console.

- **Host header** Communications between browsers and web servers are based on IP addresses, not server names, but HTTP messages have a *Host* field that contains the server name that the user specified in the browser. A host header binding associates a particular *Host* field value with one of the sites on the IIS server, even if all the host names resolve into the same IP address. In Windows SBS 2011, the client deployment and SharePoint sites all use host header bindings.

To configure or modify the bindings for a site, you select a site in IIS Manager and open its Site Bindings dialog box, as shown in Figure 16-4.



Type	Host Name	Port	IP Address	Binding
http	Companyweb	80		

FIGURE 16-4 A Site Bindings dialog box in the IIS Manager.

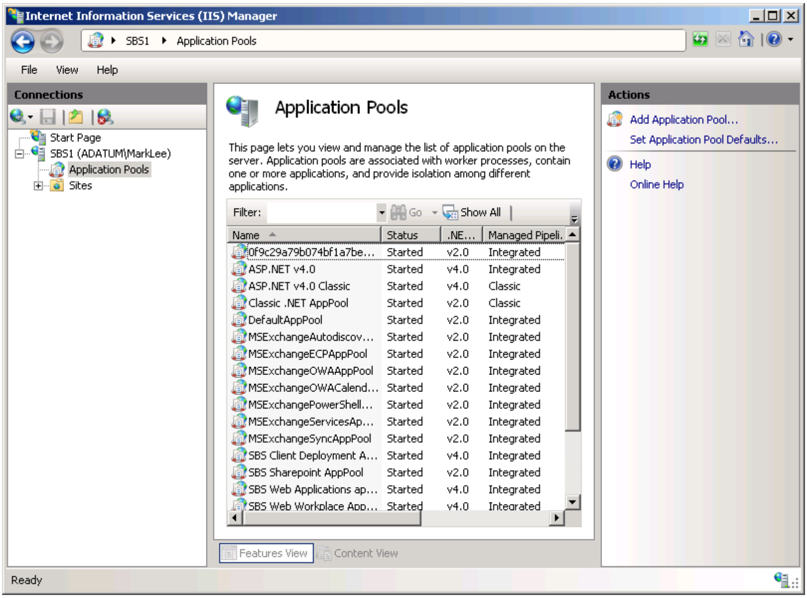
Running Web Applications

When software developers create standalone client/server applications, they have to design both the server and the client components from scratch, including the client user interface. Web applications for Windows SBS 2011 simplify the software design and deployment process by using the existing mechanisms of IIS on the server and Internet Explorer on the browser. Internet Explorer provides the basic functions that simplify the design of the user interface, and IIS includes role services that provide support for a number of application development environments, including Active Server Pages (ASP), ASP.NET, and Internet Server Application Programming Interface (ISAPI).

Originally, the Web consisted of static pages written in HTML, and the only function of the web server was to transmit those pages to browsers on request. Today, however, web applications enable sites to do much more than simply display static information. Application-enabled websites can generate pages on demand, using information provided by the user or extracted from a database.

The Companyweb site included with Windows SBS 2011 is a perfect example of this arrangement. Clients connect to the SharePoint site, and IIS runs the SharePoint web application that generates pages using content stored in a Microsoft SQL Server database. Windows SBS uses a single computer for the web server and the database server, but with Windows Server 2008 R2, it is also possible to deploy the components on separate computers.

IIS is capable of running multiple applications, each associated with a different site, and it can do so without one application jeopardizing the stability of the others or of the entire computer. IIS does this by using individual address spaces called *application pools*. Each application pool runs in its own protected space, so that if an application crashes, it cannot have any effect outside the pool. This is called *worker process application mode*. The Windows SBS 2011 setup program creates 20 separate application pools for the various sites in IIS, as shown in Figure 16-5.



Application Pools

This page lets you view and manage the list of application pools on the server. Application pools are associated with worker processes, contain one or more applications, and provide isolation among different applications.

Name	Status	.NE...	Managed Pipeli.
0f9c29a79b074bf1a7be...	Started	v2.0	Integrated
ASP.NET v4.0	Started	v4.0	Integrated
ASP.NET v4.0 Classic	Started	v4.0	Classic
Classic .NET AppPool	Started	v2.0	Classic
DefaultAppPool	Started	v2.0	Integrated
MSExchangeAutodiscov...	Started	v2.0	Integrated
MSExchangeECPAppPool	Started	v2.0	Integrated
MSExchangeOWAAppPool	Started	v2.0	Integrated
MSExchangeOWACalend...	Started	v2.0	Integrated
MSExchangePowerShell...	Started	v2.0	Integrated
MSExchangeServicesAp...	Started	v2.0	Integrated
MSExchangeSyncAppPool	Started	v2.0	Integrated
SBS Client Deployment A...	Started	v4.0	Integrated
SBS Sharepoint AppPool	Started	v2.0	Integrated
SBS Web Applications ap...	Started	v4.0	Integrated
SBS Web Workplace App...	Started	v4.0	Integrated

FIGURE 16-5 The default IIS application pools in Windows SBS 2011.

Accessing the Windows SBS Websites

The websites hosted by IIS on your Windows SBS 2011 server are accessible like any other website—by typing a URL in a browser window. However, Windows SBS provides a number of tools that make the sites more readily accessible to users and administrators.

Accessing the Client Deployment Site

The first site that each workstation accesses on the Windows SBS server is the client deployment site, which joins the computer to the domain and configures it to access the network's resources. To connect to this site, a user or administrator simply has to type the word **connect** in the browser's address box. This works for two reasons:

- The Windows SBS 2011 setup program creates an Alias (CNAME) resource record in the Active Directory Domain Services (AD DS) domain that equates the name *connect* with the name of the server. When the workstation performs a DNS name resolution on the name *connect*, it receives the IP address of the server in return.
- The client deployment website has a host header binding that associates the name *connect* with the site. As a result, IIS forwards HTTP requests containing *connect* in the *Host* field to the client deployment site.

Using Shortcuts and Links

In addition to joining the workstation to the network, the Connect Computer Wizard configures the workstation so that users have various ways to access the websites on the Windows SBS 2011 server, including the following:

- On the *Start* menu, the wizard creates a Windows SBS program group that contains an Internal Web Site shortcut pointing to the SharePoint site: *companyweb*.
- In the Internet Explorer Favorites list, the wizard creates links to the Internal Web Site and to the RWA site.

Using Remote Web Access

As mentioned earlier, RWA is a portal site that contains no content of its own, but provides users with access to the other Windows SBS 2011 websites, as well as other internal network resources. RWA is unique among the default Windows SBS websites in that it is available both to internal network users and to Internet users at remote locations. For internal users, RWA provides a convenient central access point for the Windows SBS network resources. For users at remote locations, however, RWA also provides the unique ability to log on to the AD DS domain from outside the physical network.

Once connected to the RWA site, a user with the correct permissions can perform several tasks:

- Connect to the OWA site
- Connect to the Internal *companyweb* website
- Establish a Remote Desktop Services connection to a workstation on the internal network

- Access shared folders on the network
- Change the user's password
- View the Windows Small Business Server 2008 Client Computer Help pages

Users with administrative credentials can perform these additional tasks:

- Establish a Remote Desktop Services connection to a the network server
- Access the Windows Small Business Server (SBS) Community and Official SBS Blog pages on the Internet

To provide this remote access, your Windows SBS 2011 server, your Internet access router, and your Internet domain must be configured properly. This configuration consists of the following elements:

- The Windows SBS 2011 setup program creates the RWA site in IIS and configures it with a host header binding that associates the site with the host name *remote*.
- The Internet Address Management Wizard creates a DNS resource record in your Internet domain, pointing the host name *remote* to your router's external (Internet) address.
- The Internet Address Management Wizard configures your router to admit Internet traffic through ports 25, 80, 443, 987, and 3389 and forward the traffic to your server.
- The Windows SBS 2011 setup program creates a certificate installation package that enables you to distribute your server's self-signed certificate to remote computers.

Connecting to the RWA Site

The RWA website is accessible to users, both on the internal Windows SBS network and on the Internet, through the URL *http://remote.domain_name.com*, where *domain_name.com* is the name of the Internet domain name you registered using the Internet Address Management Wizard. The server name in this URL resolves to the external address of your router, and the router forwards the traffic to your Windows SBS server. Internal users on the Windows SBS network can connect to the RWA site more easily by using the Favorite that the Connect Computer Wizard creates in Internet Explorer.

> ***TIP*** **If computers on the Internet are unable to connect to your server using RWA, the most likely causes of the problem are a missing or incorrect DNS resource record for the host name remote in your domain, or an improperly configured router that is not forwarding all the required port traffic to the server.**

When a user on the internal network connects to the RWA site, a sign-in page appears, as shown in Figure 16-6. The user must log on using his or her AD DS domain account to enter the site.

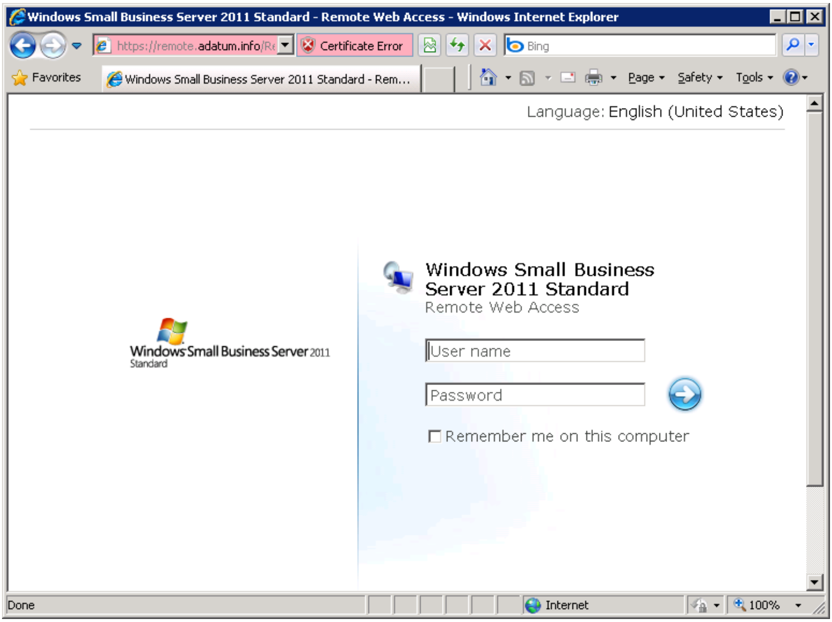
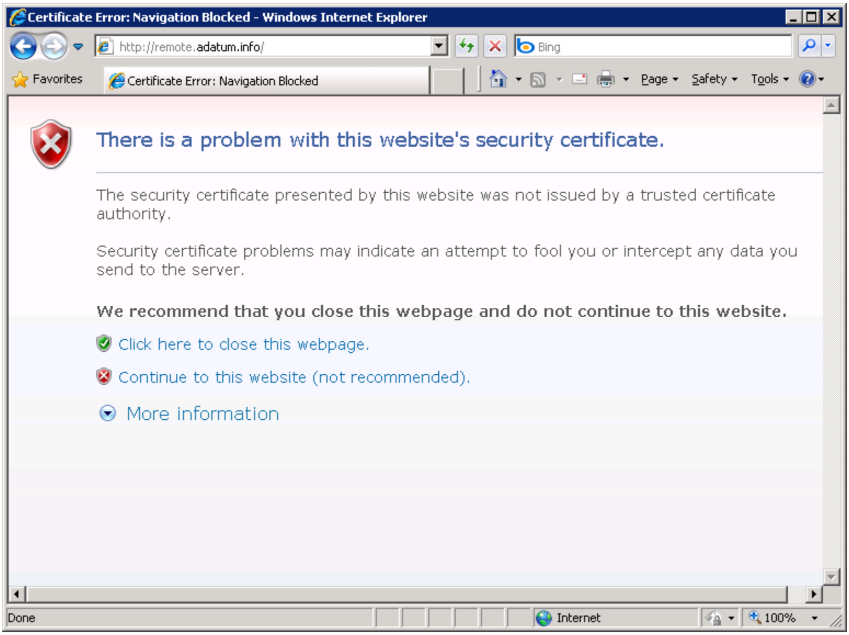

Windows Small Business Server 2011 Standard - Remote Web Access - Windows Internet Explorer
https://remote.adatum.info/Re
Certificate Error
Bing
Favorites
Windows Small Business Server 2011 Standard - Rem...
Page
Safety
Tools
Language: English (United States)
Windows Small Business Server 2011 Standard
Windows Small Business Server 2011 Standard
Remote Web Access
User name
Password
□ Remember me on this computer
Done
Internet
100%

FIGURE 16-6 The Remote Web Access sign-in page.

For Internet users, the process might be slightly more complicated in some cases. The RWA site uses Secure Sockets Layer (SSL) encryption, which uses digital certificates to confirm the identity of the server. If, during your initial Windows SBS 2011 server configuration, you used the Add A Trusted Certificate Wizard to purchase a certificate from a third-party provider and install it on your server, as described in Chapter 4, “Getting Started,” clients on the Internet trust the server’s certificate and allow the browser to access the RWA site.

If you did not purchase a certificate from a trusted third-party provider, your server is using a self-signed certificate. Computers on the local network trust the server’s self-signed certificate because they are members of the same AD DS domain. However, computers on the Internet are not members of the domain and have no reason to trust the server’s certificate. As a result, when Internet computers attempt to connect to the RWA site, a Certificate Error page appears, as shown in Figure 16-7.


Certificate Error: Navigation Blocked - Windows Internet Explorer
http://remote.adatum.info/
Bing
Favorites
Certificate Error: Navigation Blocked
Page
Safety
Tools
Done
Internet
100%

There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

More information

FIGURE 16-7 A Certificate Error page in Internet Explorer.

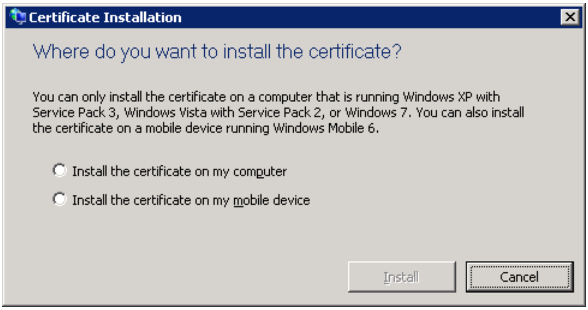
Installing a Server Certificate

The appearance of the Certificate Error page does not prevent the computer from accessing the site. Users can click the *Continue to this website* link to proceed to the RWA logon page, but unless they are aware of the reason for the error, they might be reluctant to do so. To prevent the Error page from appearing, you can either obtain a certificate from a commercial provider or install your server's self-signed certificate on each Internet computer that will access the RWA site.

Windows SBS 2011 provides a certificate installation package that simplifies the process of deploying the server certificate to remote clients. To deploy the server certificate, use the following procedure:

1. On your Windows SBS 2011 server, open Windows Explorer and browse to the *Public\Public Downloads* folder.
2. Copy the *Install certificate package* archive file to a removable medium, such as a flash drive or a writable CD or DVD.
3. On the computer where you want to deploy the certificate, insert the drive or disk.

4. Open Windows Explorer and copy the *Install certificate package* file to a local folder.
5. Browse to the *Install certificate package* file, right-click it and, from the context menu, select *Extract all*. The Extract Compressed (Zipped) Folders Wizard appears.
6. Click *Extract*. The wizard extracts the files from the archive and displays them in Windows Explorer.
7. Double-click the *InstallCertificate* program. An Open File – Security Warning dialog box appears.
8. Click *Run*. The Certificate Installation dialog box appears.



Certificate Installation

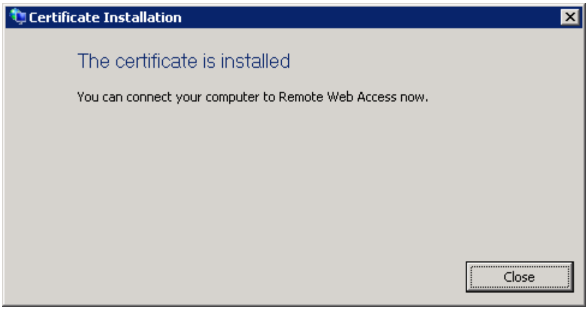
Where do you want to install the certificate?

You can only install the certificate on a computer that is running Windows XP with Service Pack 3, Windows Vista with Service Pack 2, or Windows 7. You can also install the certificate on a mobile device running Windows Mobile 6.

○ Install the certificate on my computer

○ Install the certificate on my mobile device

9. Select the *Install the certificate on my computer* option and click *Install*.
10. If a User Account Control dialog box appears, click *Continue*. A Certificate Installation message box appears, indicating that the certificate is installed.



Certificate Installation

The certificate is installed

You can connect your computer to Remote Web Access now.

11. Click *Close*.

Once the certificate is installed, the user can access the RWA site without displaying a Certificate Error page.

Accessing the WSUS Website

Unlike the other Windows SBS 2011 websites, users do not access the WSUS site using a web browser. Because the site is a local network replacement for the Microsoft Updates servers on the Internet, the Windows Update client on the network computers is responsible for accessing it. The Group Policy settings that configure the Windows Update clients contain a URL pointing to the Windows SBS 2011 server by name, with the port number 8530, to distinguish it from the server's other websites.

> ***MORE INFO*** **For information on accessing and managing the *companyweb* site on your Windows SBS 2011 server, see Chapter 17, "Working with SharePoint."**

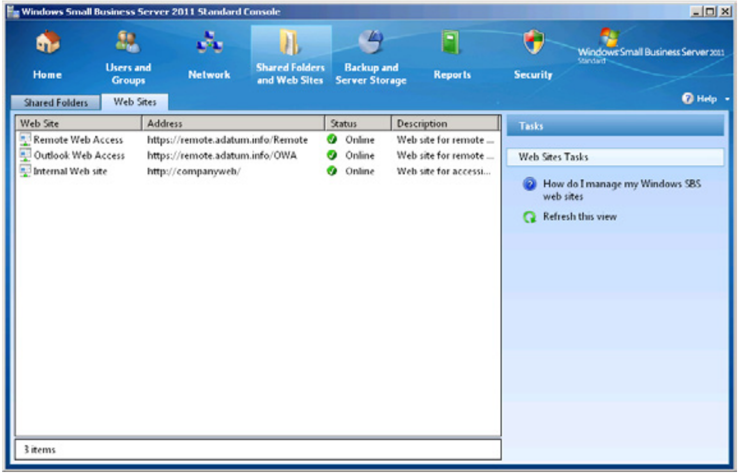
Managing the Windows SBS Websites

The Internet Information Services (IIS) Manager provides full control over all the Windows SBS 2011 websites and also enables you to create and configure new sites on your server. However, for everyday maintenance, the Windows SBS Console provides controls that enable you to manage the basic properties of the three main websites: OWA, RWA, and the Internal Web site.

Enabling and Disabling Websites

By default, Windows SBS 2011 enables all three of its main web internal websites, but you can disable them from the Windows SBS Console if you wish. To disable a website, use the following procedure:

1. Log on to your Windows SBS 2011 server using a domain account with administrative privileges. The Windows SBS Console appears.
2. Click *Shared folders and web sites* and then select the *Web sites* tab.



Windows Small Business Server 2011 Standard Console
Home
Users and Groups
Network
Shared Folders and Web Sites
Backup and Server Storage
Reports
Security
Windows Small Business Server 2011 Standard
Shared Folders
Web Sites
Help
Tasks
Web Sites Tasks
How do I manage my Windows SBS web sites
Refresh this view

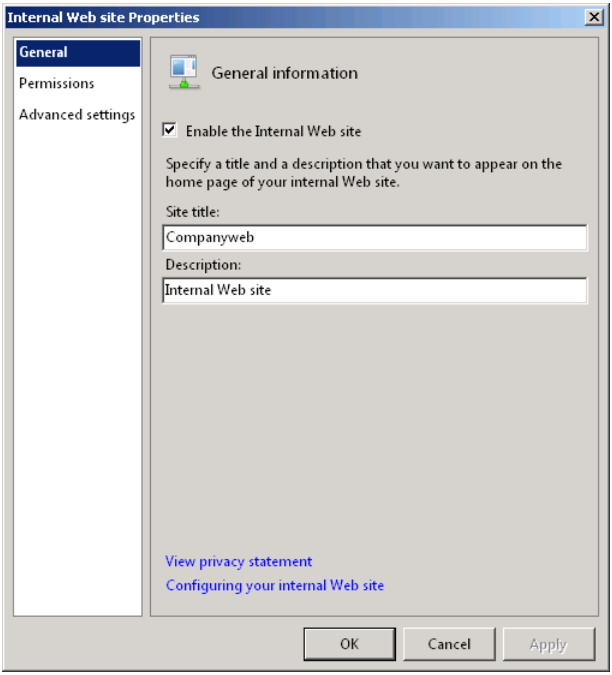
Web Site	Address	Status	Description
Remote Web Access	https://remote.adatum.info/Remote	✓ Online	Web site for remote ...
Outlook Web Access	https://remote.adatum.info/OWA	✓ Online	Web site for remote ...
Internal Web site	http://companyweb/	✓ Online	Web site for accessi...

3 items

3. Under Windows SBS *Web sites*, select the site you want to disable and, in the *Tasks* list, click *Disable this site*. The *Status* indicator for the site changes from *Online* to *Offline*.

Configuring General Settings

Each of the three Windows SBS websites has a Properties sheet, which you open by selecting a site on the Shared Folders And Web Sites/Web Sites page and clicking *View site properties* in the *Tasks* list. The *General* tab on each Properties sheet, as shown in Figure 16-8, has a check box that provides an alternative way to disable or enable the site. The Internal Web Site sheet also contains fields that enable you to modify the default *Site title* and *Description* values.


Internal Web site Properties

General information

☑ Enable the Internal Web site

Specify a title and a description that you want to appear on the home page of your internal Web site.

Site title: Companyweb

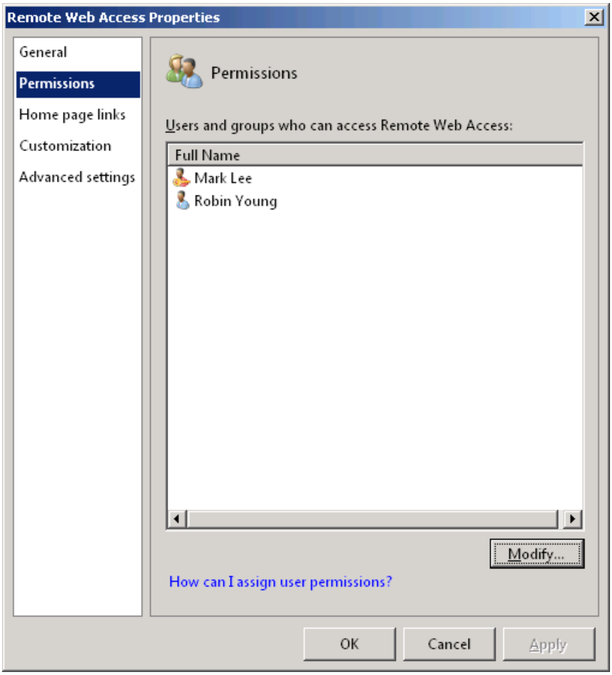
Description: Internal Web site

FIGURE 16-8 The *General* tab of the Internal Web Site Properties sheet.

Configuring Website Permissions

Although the Windows SBS Console refers to them as *permissions,* most IIS websites actually use group memberships to specify who can access them. For example, to access the RWA site, users must be members of the Windows SBS Remote Web Access Users group. To modify the membership of this group, do the following:

1. Log on to your Windows SBS 2011 server using a domain account with administrative privileges. The Windows SBS Console appears.
2. Click *Shared folders and web sites*, and then select the *Web sites* tab.
3. Under Windows SBS Web Sites, select the *Remote Web Access* site and, in the *Tasks* list, click *Manage permissions*. The Remote Web Access Properties sheet appears, displaying the *Permissions* tab.



Remote Web Access Properties

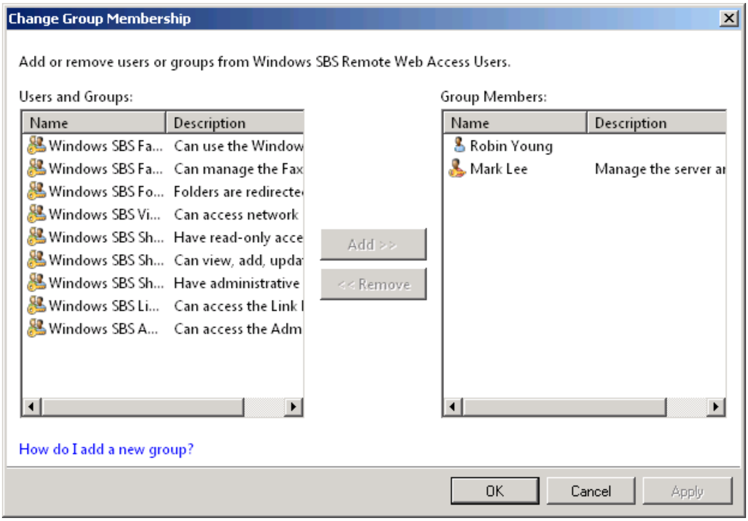
Permissions

Users and groups who can access Remote Web Access:

Full Name
Mark Lee
Robin Young

How can I assign user permissions?

4. Click *Modify*. The Change Group Membership dialog box appears.



Add or remove users or groups from Windows SBS Remote Web Access Users.

Users and Groups:

Name	Description
Windows SBS Fa...	Can use the Window
Windows SBS Fa...	Can manage the Fax
Windows SBS Fo...	Folders are redirecte
Windows SBS Vi...	Can access network
Windows SBS Sh...	Have read-only acce
Windows SBS Sh...	Can view, add, upda
Windows SBS Sh...	Have administrative
Windows SBS Li...	Can access the Link l
Windows SBS A...	Can access the Adm

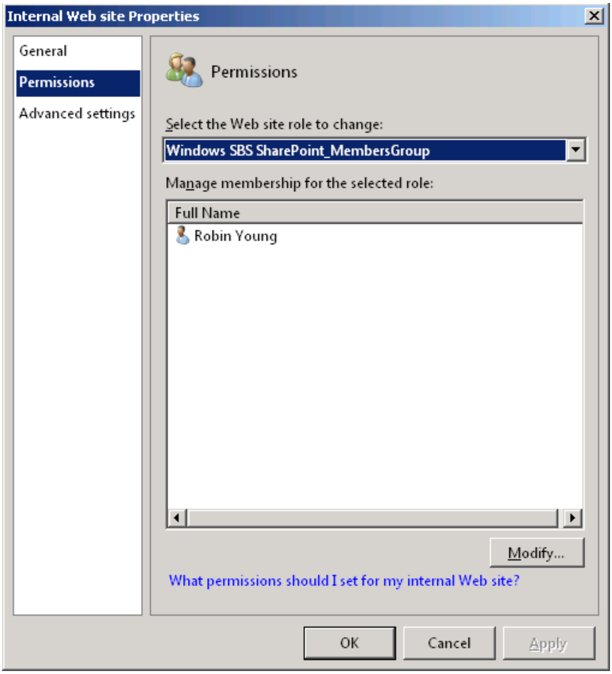
Group Members:

Name	Description
Robin Young	
Mark Lee	Manage the server ar

5. In the *Users and groups* list, select the users and groups that you want to add to the Windows SBS Remote Web Access Users group and click *Add*.
6. In the *Group members* list, select the users and groups that you want to remove from the Windows SBS Remote Web Access Users group and click *Remove*.
7. Click *OK* to close the Change Group Membership dialog box.
8. Click *OK* to close the Properties sheet.

The Internal website uses group memberships as well, as shown in Figure 16-9, but it has three levels of access, represented by the following three groups:

- **Windows SBS SharePoint_MembersGroup** Provides users with read and write access to the site
- **Windows SBS SharePoint_OwnersGroup** Provides users with administrative access to the site
- **Windows SBS SharePoint_VisitorsGroup** Provides users with read-only access to the site


Internal Web site Properties
General
Permissions
Advanced settings
Permissions

Select the Web site role to change: Windows SBS SharePoint_MembersGroup

Manage membership for the selected role:

Full Name
Robin Young

Modify...
What permissions should I set for my internal Web site?
OK
Cancel
Apply

FIGURE 16-9 The *Permissions* tab of the Internal Web Site Properties sheet.

The OWA site uses the same basic interface to manage permissions, but in this case, the Windows SBS Console is modifying a property of the user's Exchange Server mailbox rather than a group membership. You can also grant a user access to the OWA site by selecting the *Outlook Web Access* tab on the *Web sites* tab of the user's Properties sheet.

Configuring RWA

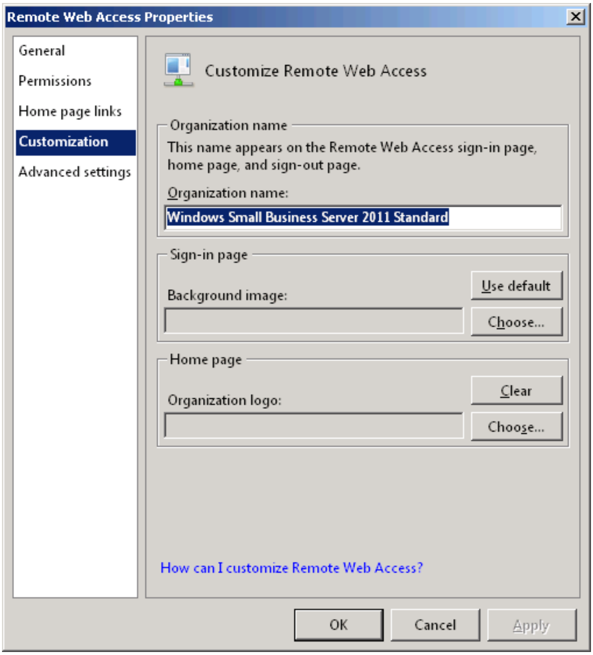
The Windows SBS Console enables you to specify what items appear in the RWA interface and how the site appears to users.

Customizing the RWA Site

To customize the appearance of the RWA site, use the following procedure:

1. Log on to your Windows SBS 2011 server using a domain account with administrative privileges. The Windows SBS Console appears.
2. Click *Shared folders and web sites* and then select the *Web sites* tab.
3. Under Windows SBS *Web sites*, select the *Remote Web Access* site and, in the *Tasks* list, click *View site properties*. The Remote Web Access Properties sheet appears.

4. Click the *Customization* tab.



Organization name

This name appears on the Remote Web Access sign-in page, home page, and sign-out page.

Organization name: Windows Small Business Server 2011 Standard

Sign-in page

Background image:

Home page

Organization logo:

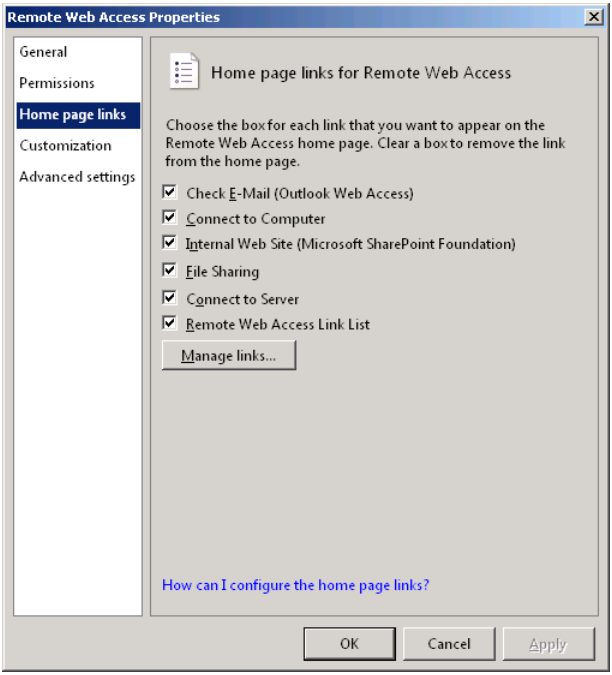
5. To change the title that appears on the site's pages, modify the value in the *Organization name* text box.
6. To change the background of the sign-in page, click the *Choose* button next to the *Background image* text box. An *Open* combo box appears.
7. Browse to an image file and click *Open*. The file you selected appears in the *Background image* text box.
8. To change the logo on the RWA Home page, click the *Choose* button next to the *Organization logo* text box. An *Open* combo box appears.
9. Browse to an image file and click *Open*. The file you selected appears in the *Organization logo* text box.
10. Click *OK* to close the Remote Web Access Properties sheet.

Configuring RWA Site Content

To specify the items that should appear on the RWA site, follow these steps:

1. Log on to your Windows SBS 2011 server using a domain account with administrative privileges. The Windows SBS Console appears.
2. Click *Shared folders and web sites* and then select the *Web sites* tab.

3. Under Windows SBS Web Sites, select the *Remote Web Access* site and, in the *Tasks* list, click *View site properties*. The Remote Web Access Properties sheet appears.
4. Click the *Home page links* tab.

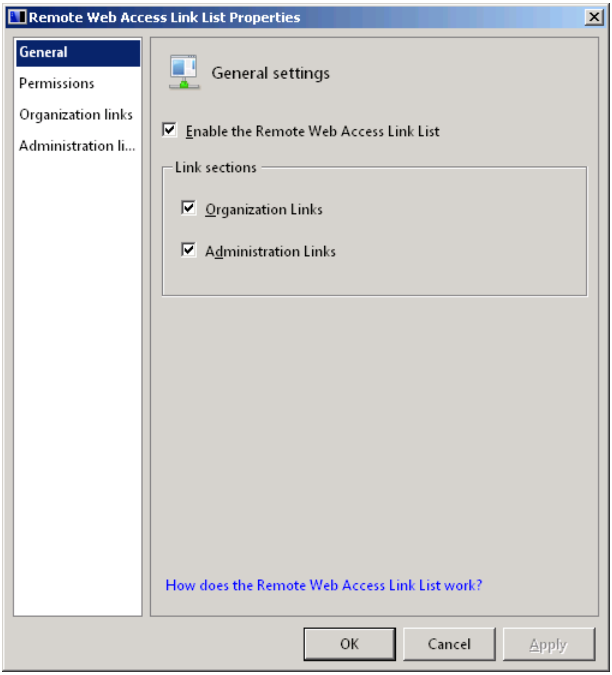


Home page links for Remote Web Access

Choose the box for each link that you want to appear on the Remote Web Access home page. Clear a box to remove the link from the home page.

☑ Check E-Mail (Outlook Web Access)
☑ Connect to Computer
☑ Internal Web Site (Microsoft SharePoint Foundation)
☑ File Sharing
☑ Connect to Server
☑ Remote Web Access Link List

5. To remove elements from the RWA Home page, clear some or all of the check boxes on the *Home page links* tab.
6. Click *Manage links*. The Remote Web Access Link List Properties sheet appears.



Remote Web Access Link List Properties

General settings

☑ Enable the Remote Web Access Link List

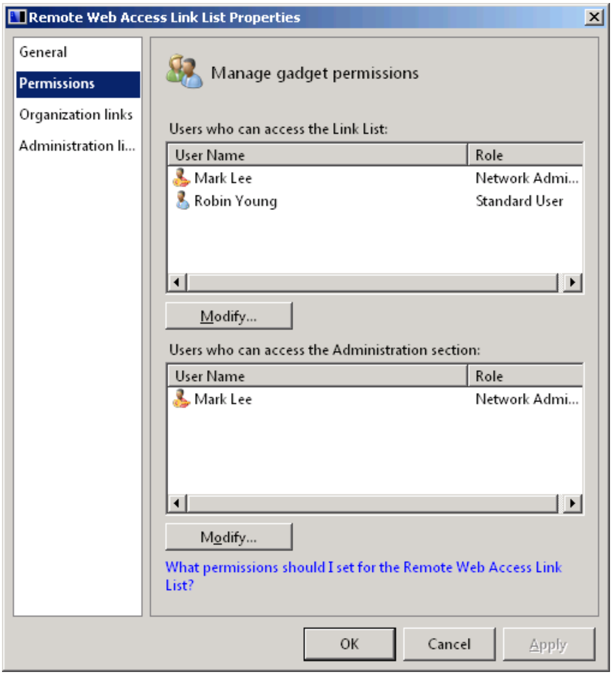
Link sections

☑ Organization Links

☑ Administration Links

How does the Remote Web Access Link List work?

7. On the *General* tab, clear any of the following check boxes, as desired:
    - *Enable the Remote Web Access link list*
    - *Organization links*
    - *Administration links*
8. Click the *Permissions* tab.



Remote Web Access Link List Properties

Manage gadget permissions

Users who can access the Link List:

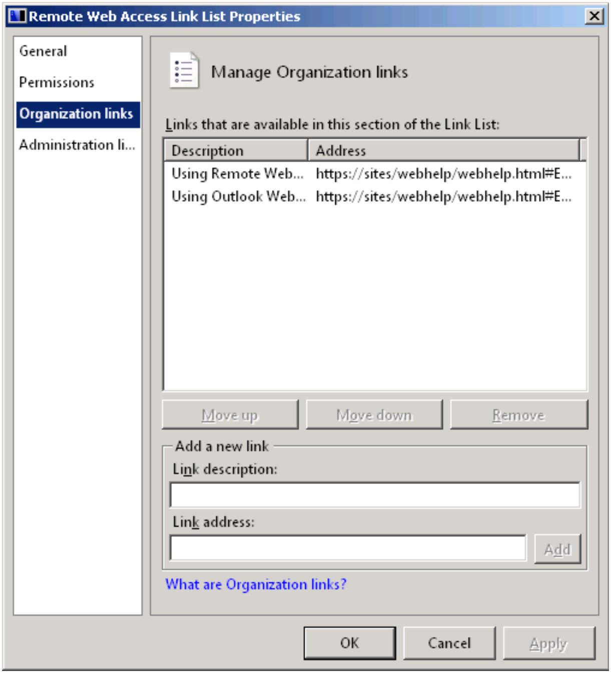
User Name	Role
Mark Lee	Network Admi...
Robin Young	Standard User

Users who can access the Administration section:

User Name	Role
Mark Lee	Network Admi...

What permissions should I set for the Remote Web Access Link List?

9. In the *Users who can access the link list* section, click *Modify* to open a Change Group Membership dialog box, in which you can specify which users and groups are able to access the *Remote Web Access link list*.
10. In the *Users who can access the Administration* section area, click *Modify* to open a Change Group Membership dialog box, in which you can specify which users and groups are able to access the *Administration links* in the *Remote Web Access link list*.
11. Click the *Organization links* tab.


Remote Web Access Link List Properties
General
Permissions
Organization links
Administration li...
Manage Organization links
Links that are available in this section of the Link List:

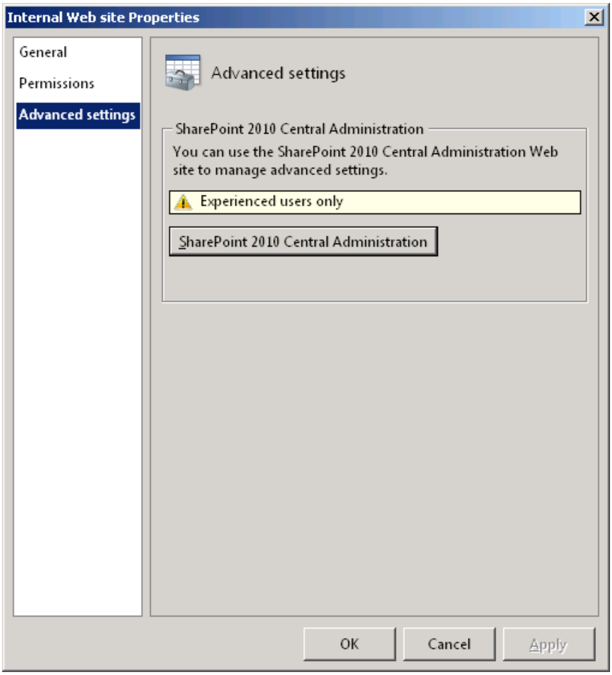
Description	Address
Using Remote Web...	https://sites/webhelp/webhelp.html#E...
Using Outlook Web...	https://sites/webhelp/webhelp.html#E...

Move up
Move down
Remove
Add a new link
Link description:
Link address:
Add
What are Organization links?
OK
Cancel
Apply

12. To add a link to the *Organization links* list, type a descriptive title in the *Link description* text box and a URL in the *Link address* text box. Then click *Add*. The new link appears in the list.
13. Click the *Administration links* tab and repeat step 12 to add a hyperlink to the *Administration links* list, if desired.
14. Click *OK* to close the Remote Web Access Link List Properties sheet.
15. Click *OK* to close the Remote Web Access Properties sheet.

Configuring Advanced Settings

The Properties sheet for each of the Windows SBS websites has an *Advanced settings* tab, which contains only a button providing access to a tool that provides more comprehensive access to the site's configuration, as shown in Figure 16-10. The Properties sheets for the *Remote Web Access* and *Outlook Web Access* sites provide access to IIS Manager, while the Internal Web Site Properties sheet provides access to the SharePoint 2010 Central Administration site.



Internal Web site Properties

Advanced settings

SharePoint 2010 Central Administration

You can use the SharePoint 2010 Central Administration Web site to manage advanced settings.

⚠ Experienced users only

FIGURE 16-10 The *Advanced settings* tab of the Internal Web Site Properties sheet.

CHAPTER 17

Working with SharePoint

In Chapter 16, "Working with Websites," you learned how Windows Small Business Server (SBS) 2011 uses Internet Information Services (IIS) 7.0 to implement multiple websites for use by both internal and remote network users. Most of these websites require only minimal administrative attention because the Windows SBS 2011 setup program creates and configures them during the operating system installation. However, many administrators want to customize the internal Windows SharePoint Services website or create their own additional sites by using IIS or Microsoft Office Live Small Business. To help you do so, this chapter examines some of the more advanced website creation and management features found in Windows SBS 2011.

Working with SharePoint Foundation 2010

The primary intranet website on your Windows SBS network is a SharePoint Foundation 2010 site, which is created by default during the installation of Windows SBS 2011. SharePoint Foundation 2010 is a web application that provides browser-based clients with an interface that enables them to share, collaborate on, and discuss documents using a variety of tools. At the server, the SharePoint application stores user-contributed documents and information in a Microsoft SQL Server database.

SharePoint can function as a distributed application, with the website running on one server and the database on another. However, in Windows SBS 2011, everything runs on your primary server. IIS hosts the SharePoint website, and the Windows Internal Database feature hosts the database.

NOTE **The SQL Server database that Windows SBS 2011 creates is located on the primary server and has no connection to the SQL Server 2008 R2 product included with the Windows SBS 2011 Premium Add-on product. Although it is possible for Windows SBS 2011 Premium networks to use the secondary server to host a SharePoint database, you cannot use the Windows Internal Database to host a third-party application.**

Although the SharePoint site is usable as is, you can improve its appearance and functionality by configuring and customizing it in many ways.

Accessing the Internal Website

By default, Windows SBS 2011 configures the internal website to use the standard port number 80 with a host header binding containing the name *Companyweb*. Your internal Domain Name System (DNS) domain has an Alias (CNAME) resource record equating the name *Companyweb* with the name of your Windows SBS primary server.

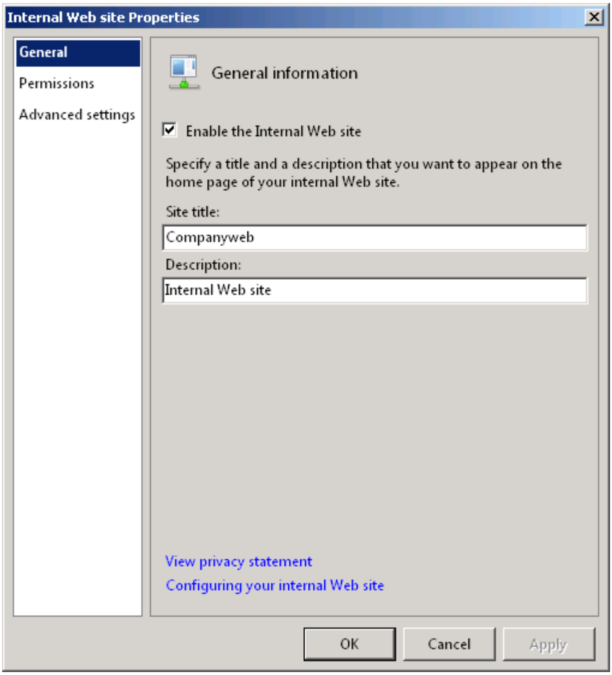
MORE INFO **For more information on website bindings, see the section entitled "Running Multiple Sites" in Chapter 16.**

Internal network users can therefore access the site from any browser by using the Uniform Resource Locator (URL) *http://companyweb*. Users can also access the site using the Internal Web Site shortcut that the Connect Computer Wizard creates on client workstations or the favorite of the same name in Internet Explorer. Finally, both internal and remote users can access the site through the Remote Web Access (RWA) interface or by using the URL *https://remote.domain_name.com:987*, where *domain_name.com* is your Internet domain name.

Managing the Internal Website Properties

The Windows SBS Console provides the same basic control over the internal website that it does over the other default websites that IIS hosts. To configure the internal website's properties, use the following procedure:

1. Log on to your Windows SBS 2011 server using a domain account with administrative privileges. The Windows SBS Console appears.
2. Click *Shared folders and web sites*, and then select the *Web sites* tab.
3. Under *Windows SBS web sites*, select *Internal web site*, and, in the *Tasks* list, click *View site properties*. The Internal Web Site Properties sheet appears.



☑ Enable the Internal Web site

Specify a title and a description that you want to appear on the home page of your internal Web site.

Site title:
Companyweb

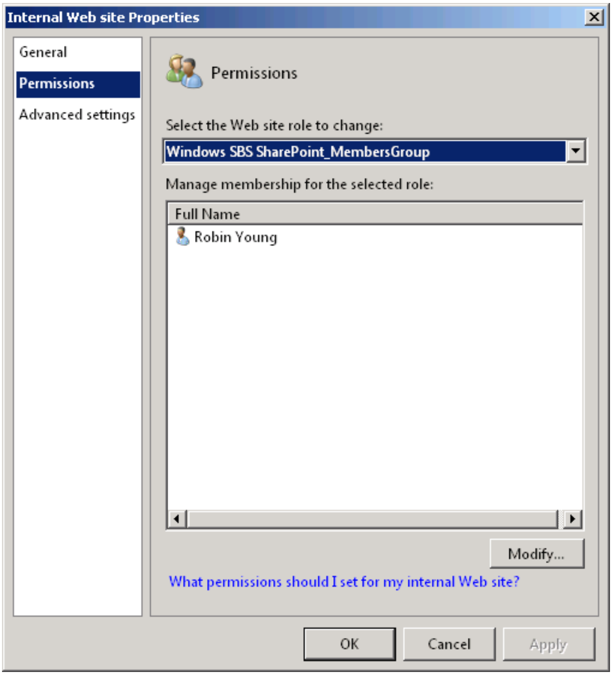
Description:
Internal Web site

View privacy statement
Configuring your internal Web site

4. On the *General* tab, configure the following properties, if desired:
   - **Enable the internal web site** *Clear this check box to disable the website entirely.*
   - **Site title** *Modify this value to change the title displayed on the upper left of each page on the site.*
   - **Description** *Modify this value to change the descriptive text displayed at the top of the site's Home page.*

   NOTE Changing the *Site title* field from its default *Companyweb* value does not change the host header binding or the DNS record associated with the site. Users can still type the URL *http://companyweb* to access the internal website.

5. Click the *Permissions* tab.



Internal Web site Properties

Permissions

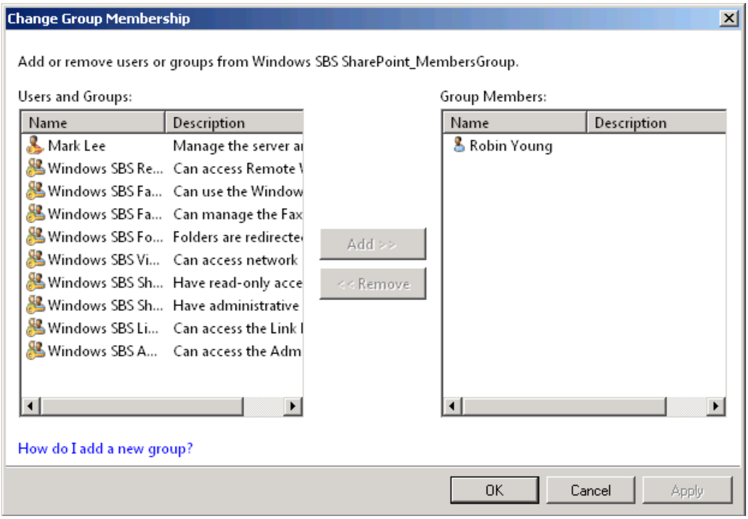
Select the Web site role to change: Windows SBS SharePoint_MembersGroup

Manage membership for the selected role:

Full Name
Robin Young

What permissions should I set for my internal Web site?

6. In the *Select the web site role to change* drop-down list, select the group whose membership you want to change and click *Modify*. The Change Group Membership dialog box appears.



Change Group Membership

Add or remove users or groups from Windows SBS SharePoint_MembersGroup.

Users and Groups:

Name	Description
Mark Lee	Manage the server ai
Windows SBS Re...	Can access Remote \
Windows SBS Fa...	Can use the Window
Windows SBS Fa...	Can manage the Fax
Windows SBS Fo...	Folders are redirecte
Windows SBS Vi...	Can access network
Windows SBS Sh...	Have read-only acce
Windows SBS Sh...	Have administrative
Windows SBS Li...	Can access the Link I
Windows SBS A...	Can access the Adm

Group Members:

Name	Description
Robin Young	

How do I add a new group?

7. In the *Users and groups* list, select the users and groups that you want to add to the selected group and click *Add*.
8. In the *Group members* list, select the users and groups that you want to remove from the selected group and click *Remove*.
9. Click *OK* to close the Change Group Membership dialog box.
10. Repeat steps 6 through 9 to modify the memberships of the other groups, if desired.
11. Click *OK* to close the Properties sheet.

Understanding the Default SharePoint Permissions

Unlike the other Windows SBS 2011 sites, the internal website uses three separate groups to provide three levels of access to the site, as follows:

- **Windows SBS SharePoint_OwnersGroup** Provides users with full administrative access to the site. All new user accounts you create with the Network Administrator role are members of this group.
- **Windows SBS SharePoint_MembersGroup** Enables users to read and write content on the site. Users can add documents to the site and edit existing ones, but they cannot create document libraries or make other modifications to the structure of the site. All new user accounts you create with the Standard User role are members of this group.
- **Windows SBS SharePoint_VisitorsGroup** Enables users to read content on the site.

These three groups are Active Directory Domain Services (AD DS) security groups, which the Windows SBS 2011 setup program creates during the operating system installation. However, SharePoint Foundation 2010 also has its own system of groups, and each of the AD DS groups is a member of one of the SharePoint groups. SharePoint has its own system of permissions as well. SharePoint groups can have any of the following SharePoint permissions:

- **Full Control** Provides unlimited administrative access to the site
- **Design** Provides the ability to view, add, update, delete, approve, and customize site content
- **Contribute** Provides the ability to view, add, update, and delete content
- **Read** Provides the ability to view content only

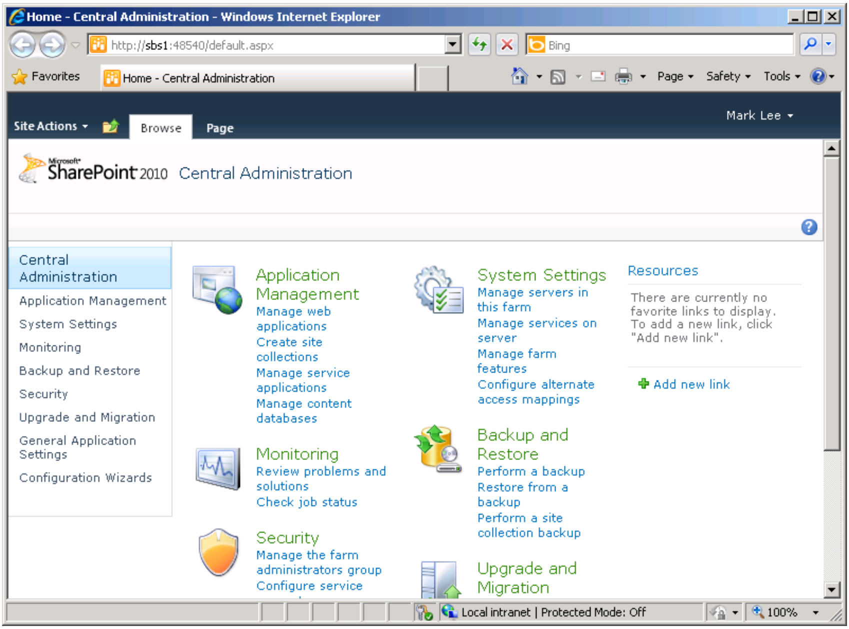
By creating the AD DS groups and adding them to the SharePoint groups, Windows SBS 2011 simplifies the process of working with the site's permissions. Using the Windows SBS Console, administrators can control access to the site simply by altering the AD DS group memberships. The actual relationships between the AD DS security groups, the SharePoint groups, and the SharePoint permissions are shown in Table 17-1.

TABLE 17-1 Relationships Between AD DS and SharePoint Groups

AD DS GROUP NAME	SHAREPOINT GROUP NAME	SHAREPOINT PERMISSION
Windows SBS SharePoint_OwnersGroup	Companyweb Owners	Full Control
Windows SBS SharePoint_MembersGroup	Companyweb Members	Design
Windows SBS SharePoint_VisitorsGroup	Companyweb Visitors	Read

Using the SharePoint Central Administration Site

The *Advanced settings* tab of the Internal Web Site Properties sheet contains a button that opens the SharePoint 2010 Central Administration website, shown in Figure 17-1. This is a completely separate, administrative site that uses a random port number binding to distinguish it from the main site.



There are currently no favorite links to display. To add a new link, click "Add new link".

FIGURE 17-1 The SharePoint 2010 Central Administration website.

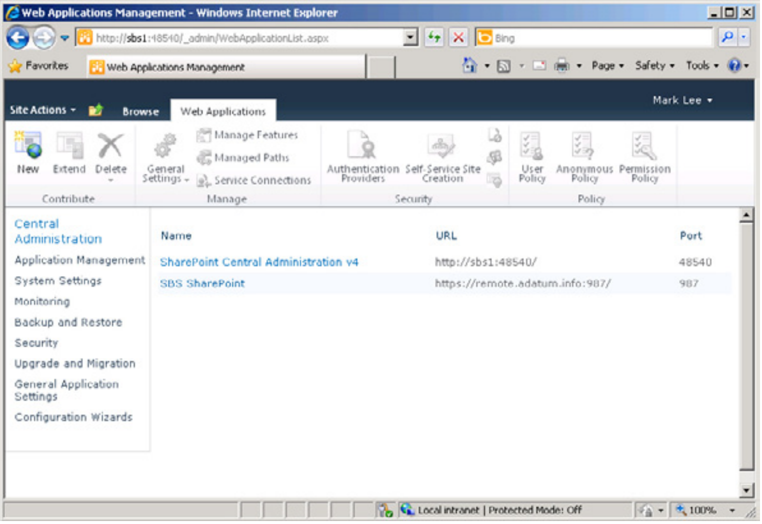
When you select one of the eight headings on the Central Administration Home page, a page appears containing links to the various controls you can use to configure SharePoint's capabilities.

As with all the other applications included with Windows SBS 2011, SharePoint Foundation 2010 is implemented using a single server. However, the SharePoint Foundation product is highly extendable, and a good deal of the configuration interface in the Central Administration site is devoted to creating, configuring, and managing a SharePoint server farm.

> ***NOTE*** **A *server farm* is a group of computers, all running the same application or applications, to provide the network with load balancing or fault tolerance capabilities.**

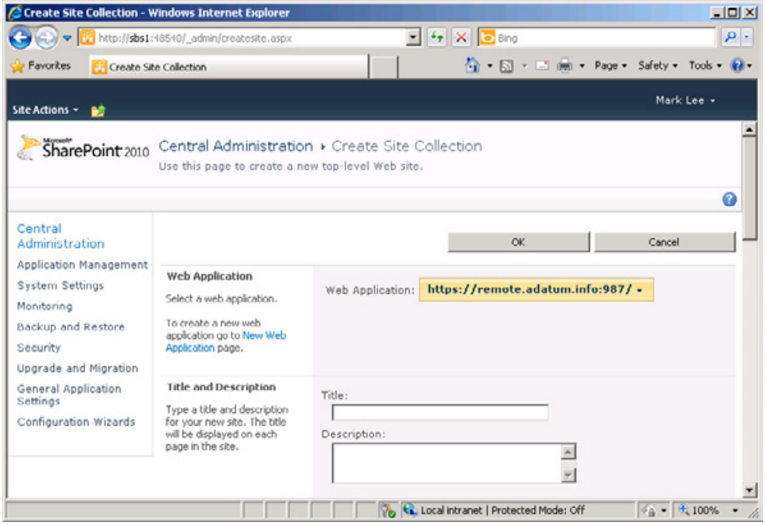
The pages available on the Central Administration site are as follows:

- **Application management** Provides access to controls that enable administrators to manage four SharePoint components.
- **Web applications** By default, the SharePoint Foundation installation in Windows SBS 2011 includes two applications: one for the Companyweb page and one or the Central Administration page. Using the controls shown here, you can create your own additional web applications.



Name	URL	Port
SharePoint Central Administration v4	http://sbs1:48540/	48540
SBS SharePoint	https://remote.adatum.info:987/	987

- **Site collections** A site collection is a combination of a web page and a web application that enables you to create a top-level SharePoint page. SharePoint Foundation 2010 includes templates that specify what features are available on the new sites you create, such as blogs and meeting workspaces.



Central Administration ▸ Create Site Collection

Use this page to create a new top-level Web site.

Web Application

Select a web application.

To create a new web application go to New Web Application page.

Web Application: https://remote.adatum.info:987/

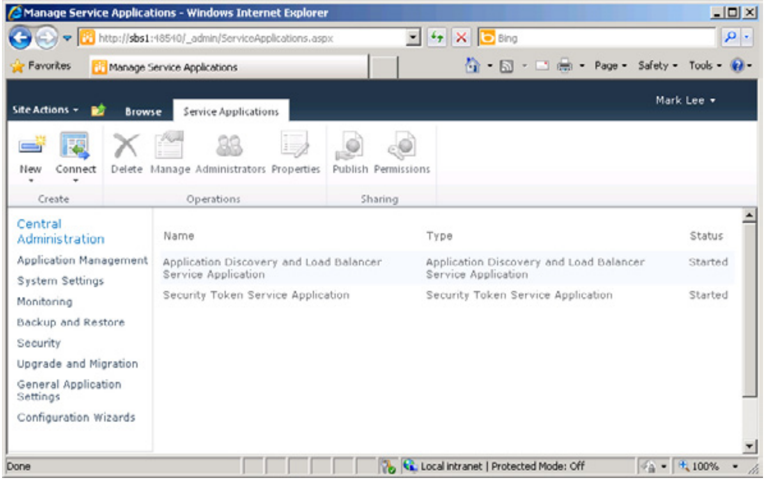
Title and Description

Type a title and description for your new site. The title will be displayed on each page in the site.

Title:

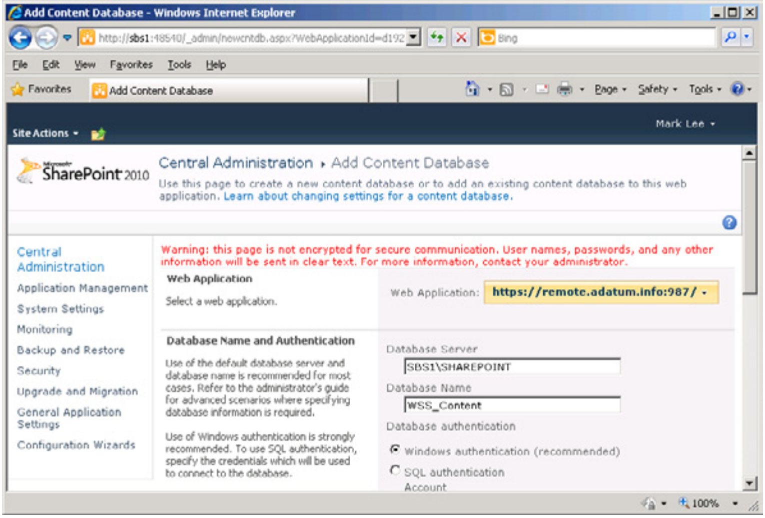
Description:

- **Service applications** SharePoint Foundation 2010 uses a new service application architecture to replace the shared service providers used in previous versions. Service applications enable sites running in different web applications to share resources. This makes it possible for the SBS administrator to expand the SharePoint Foundation functionality from a single server to a server farm.



Name	Type	Status
Application Discovery and Load Balancer Service Application	Application Discovery and Load Balancer Service Application	Started
Security Token Service Application	Security Token Service Application	Started

- **Databases** Provides controls that enable administrators to create new database instances and associate them with specific web applications.



Add Content Database - Windows Internet Explorer

http://sbs1:48540/_admin/newcntdb.aspx?WebApplicationId=d192

Central Administration ▸ Add Content Database

Use this page to create a new content database or to add an existing content database to this web application. Learn about changing settings for a content database.

Warning: this page is not encrypted for secure communication. User names, passwords, and any other information will be sent in clear text. For more information, contact your administrator.

Web Application

Select a web application.

Web Application: https://remote.adatum.info:987/

Database Name and Authentication

Use of the default database server and database name is recommended for most cases. Refer to the administrator's guide for advanced scenarios where specifying database information is required.

Use of Windows authentication is strongly recommended. To use SQL authentication, specify the credentials which will be used to connect to the database.

Database Server: SBS1\SHAREPOINT

Database Name: WSS_Content

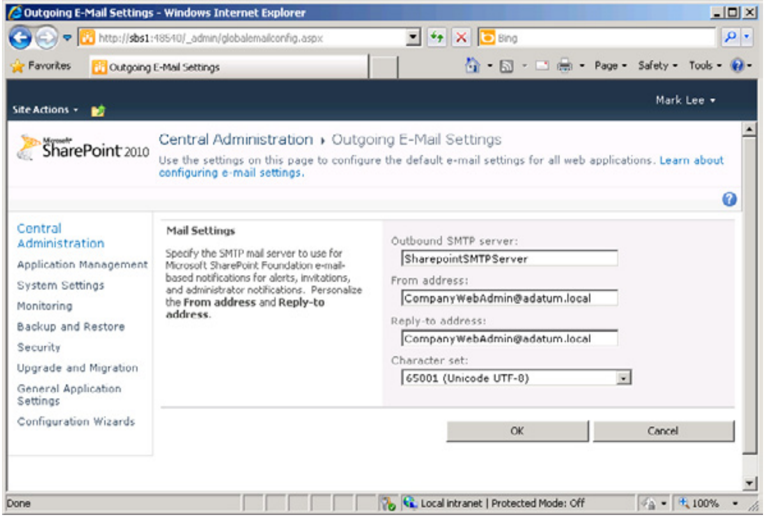
Database authentication

● Windows authentication (recommended)

○ SQL authentication

Account

- **System Settings** Enables administrators to manage the SharePoint servers on the network; the incoming and outgoing email settings for the SharePoint email services; and settings for server farm management, such as alternate access mappings that enable administrators to specify the URLs that provide access to the SharePoint site.



Outgoing E-Mail Settings - Windows Internet Explorer

http://sbs1:48540/_admin/globalemailconfig.aspx

Central Administration ▸ Outgoing E-Mail Settings

Use the settings on this page to configure the default e-mail settings for all web applications. Learn about configuring e-mail settings.

Mail Settings

Specify the SMTP mail server to use for Microsoft SharePoint Foundation e-mail-based notifications for alerts, invitations, and administrator notifications. Personalize the **From address** and **Reply-to address**.

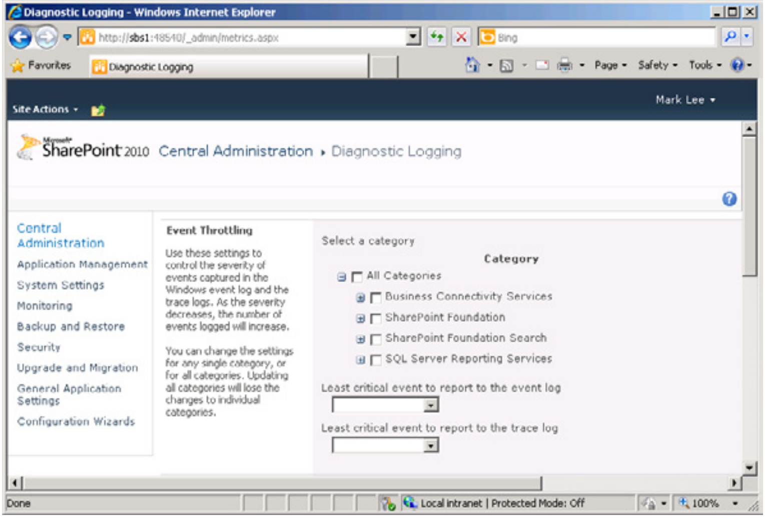
Outbound SMTP server: SharepointSMTPServer

From address: CompanyWebAdmin@adatum.local

Reply-to address: CompanyWebAdmin@adatum.local

Character set: 65001 (Unicode UTF-8)

- **Monitoring** Provides access to tools that enable administrators to monitor SharePoint functions and configure the SharePoint logging and reporting capabilities.


Diagnostic Logging - Windows Internet Explorer
http://sbs1:48540/_admin/metrics.aspx
Bing
Favorites
Diagnostic Logging
Page
Safety
Tools
Site Actions
Mark Lee
Done
Local intranet | Protected Mode: Off
100%

SharePoint 2010 Central Administration ▸ Diagnostic Logging

Central Administration
Application Management
System Settings
Monitoring
Backup and Restore
Security
Upgrade and Migration
General Application Settings
Configuration Wizards

Event Throttling

Use these settings to control the severity of events captured in the Windows event log and the trace logs. As the severity decreases, the number of events logged will increase.

You can change the settings for any single category, or for all categories. Updating all categories will lose the changes to individual categories.

Select a category

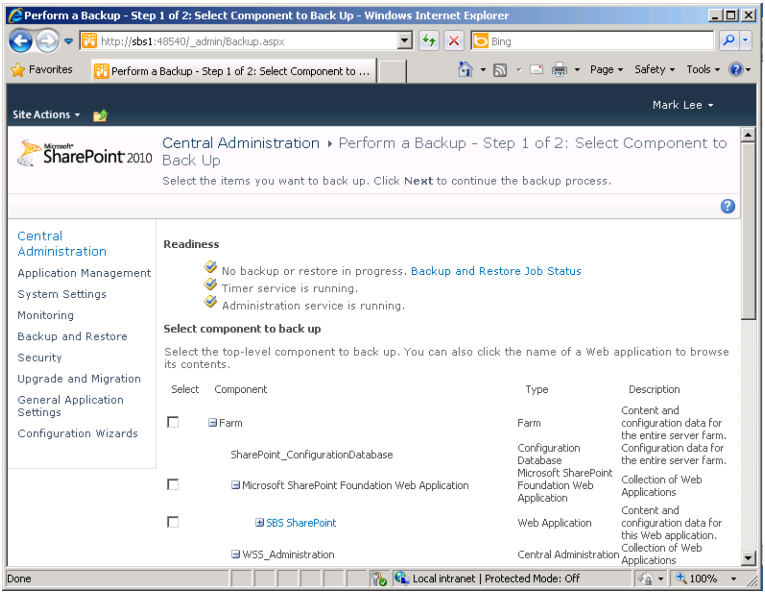
Category

- ⊟ □ All Categories
  - ⊞ □ Business Connectivity Services
  - ⊞ □ SharePoint Foundation
  - ⊞ □ SharePoint Foundation Search
  - ⊞ □ SQL Server Reporting Services

Least critical event to report to the event log

Least critical event to report to the trace log

- **Backup and restore** Because SharePoint stores its data in a SQL Server database, traditional backup software products cannot copy the database while it is in an open state. SharePoint therefore has its own backup capability that enables administrators to copy the SharePoint data from servers and farms to another location.


Perform a Backup - Step 1 of 2: Select Component to Back Up - Windows Internet Explorer
http://sbs1:48540/_admin/Backup.aspx
Bing
Favorites
Perform a Backup - Step 1 of 2: Select Component to ...
Page
Safety
Tools
Site Actions
Mark Lee
Done
Local intranet | Protected Mode: Off
100%

SharePoint 2010 Central Administration ▸ Perform a Backup - Step 1 of 2: Select Component to Back Up

Select the items you want to back up. Click **Next** to continue the backup process.

Central Administration
Application Management
System Settings
Monitoring
Backup and Restore
Security
Upgrade and Migration
General Application Settings
Configuration Wizards

Readiness

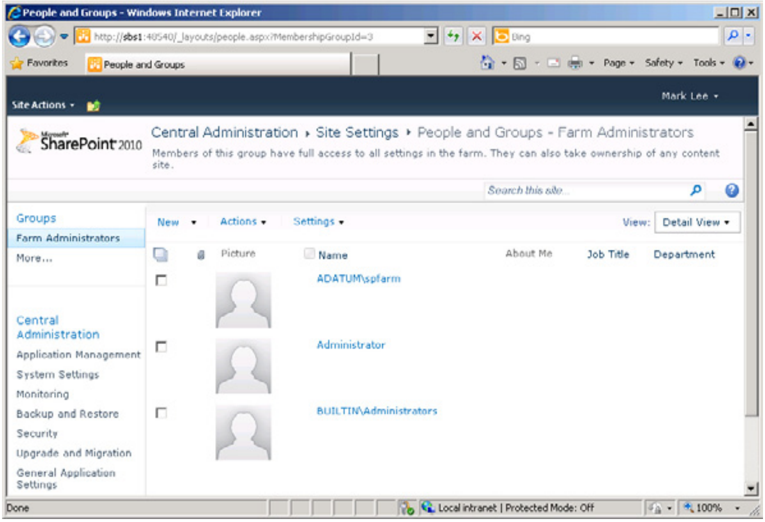
✓ No backup or restore in progress. Backup and Restore Job Status
✓ Timer service is running.
✓ Administration service is running.

Select component to back up

Select the top-level component to back up. You can also click the name of a Web application to browse its contents.

Select	Component	Type	Description
□	⊟ Farm	Farm	Content and configuration data for the entire server farm.
	SharePoint_ConfigurationDatabase	Configuration Database	Configuration data for the entire server farm.
□	⊟ Microsoft SharePoint Foundation Web Application	Microsoft SharePoint Foundation Web Application	Collection of Web Applications
□	⊞ SBS SharePoint	Web Application	Content and configuration data for this Web application.
	⊟ WSS_Administration	Central Administration	Collection of Web Applications

- **Security** These pages enable administrators to configure antivirus settings; configure access control for SharePoint sites, in the form of user accounts and groups; block specific file types; and manage passwords.



People and Groups - Windows Internet Explorer

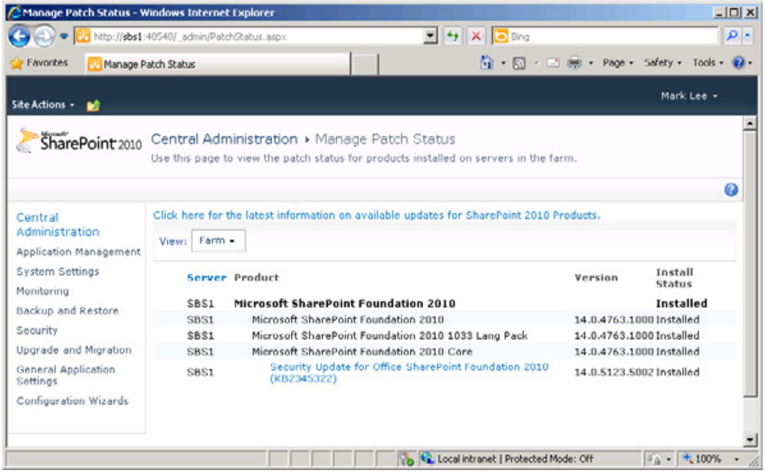
http://sbs1:40540/_layouts/people.aspx?MembershipGroupId=3

Central Administration › Site Settings › People and Groups - Farm Administrators

Members of this group have full access to all settings in the farm. They can also take ownership of any content site.

	Picture	Name	About Me	Job Title	Department
□		ADATUM\spfarm			
□		Administrator			
□		BUILTIN\Administrators			

- **Upgrade and migration** Enables administrators to view and manage the update status for all the servers in a farm.



Manage Patch Status - Windows Internet Explorer

http://sbs1:40540/_admin/PatchStatus.aspx

Central Administration › Manage Patch Status

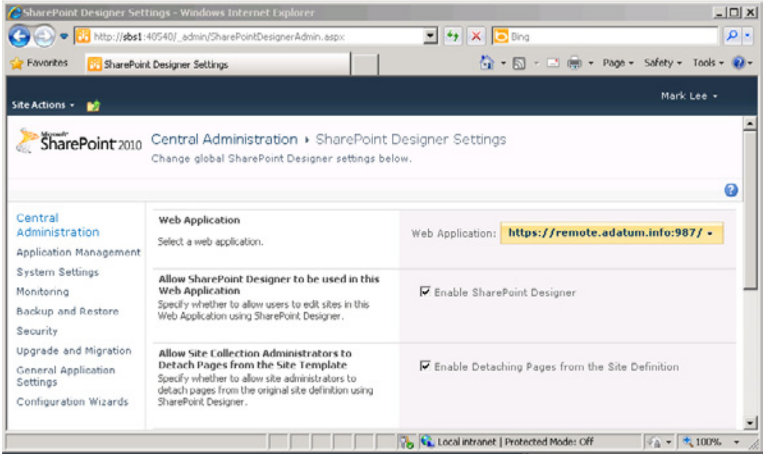
Use this page to view the patch status for products installed on servers in the farm.

Click here for the latest information on available updates for SharePoint 2010 Products.

View: Farm

Server	Product	Version	Install Status
SBS1	**Microsoft SharePoint Foundation 2010**		**Installed**
SBS1	Microsoft SharePoint Foundation 2010	14.0.4763.1000	Installed
SBS1	Microsoft SharePoint Foundation 2010 1033 Lang Pack	14.0.4763.1000	Installed
SBS1	Microsoft SharePoint Foundation 2010 Core	14.0.4763.1000	Installed
SBS1	Security Update for Office SharePoint Foundation 2010 (KB2345322)	14.0.5123.5002	Installed

- **General application settings** Provides access to SharePoint Designer controls as well as external service connections and reporting services.



Central Administration ▸ SharePoint Designer Settings

Change global SharePoint Designer settings below.

Web Application
Select a web application.

Web Application: **https://remote.adatum.info:987/**

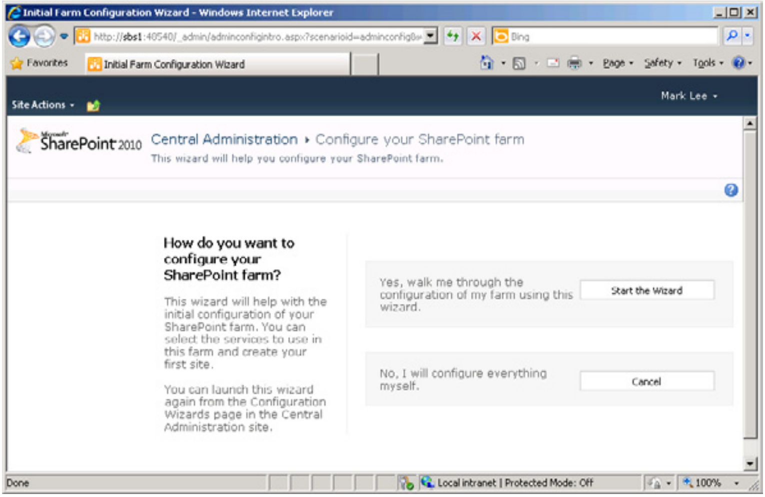
Allow SharePoint Designer to be used in this Web Application
Specify whether to allow users to edit sites in this Web Application using SharePoint Designer.

☑ Enable SharePoint Designer

Allow Site Collection Administrators to Detach Pages from the Site Template
Specify whether to allow site administrators to detach pages from the original site definition using SharePoint Designer.

☑ Enable Detaching Pages from the Site Definition

- **Configuration Wizards** Provides access to the SharePoint Farm Configuration Wizard.


Initial Farm Configuration Wizard - Windows Internet Explorer
http://sbs1:40540/_admin/adminconfigintro.aspx?scenarioid=adminconfig&
Bing
Favorites
Initial Farm Configuration Wizard
Page
Safety
Tools
Site Actions
Mark Lee
SharePoint 2010
Start the Wizard
Cancel
Done
Local intranet | Protected Mode: Off
100%

Central Administration ▸ Configure your SharePoint farm

This wizard will help you configure your SharePoint farm.

How do you want to configure your SharePoint farm?

This wizard will help with the initial configuration of your SharePoint farm. You can select the services to use in this farm and create your first site.

You can launch this wizard again from the Configuration Wizards page in the Central Administration site.

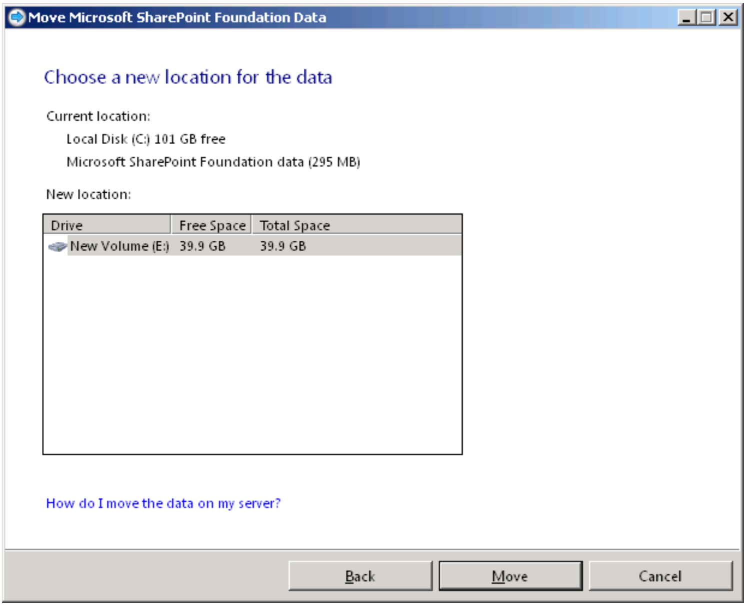
Yes, walk me through the configuration of my farm using this wizard.

No, I will configure everything myself.

Moving the SharePoint Data Store

As with all its other services, Windows SBS 2011 configures SharePoint Foundation 2010 to store its data on the system drive during the operating system installation. If you create additional storage volumes after the installation, you might want to move the SharePoint data to another drive using the following procedure:

1. Log on to your Windows SBS 2011 server using a domain account with administrative privileges. The Windows SBS Console appears.
2. Click *Backup and server storage* and then select the *Server storage* tab.
3. In the *Tasks* list, select *Move SharePoint Foundation data*. The Move SharePoint Foundation Data Wizard appears.
4. Click *Next* to bypass the Getting Started page. The wizard checks your server's backup status and searches for available volumes. If your server is not configured to perform regular backups, a Server Backup Is Not Configured dialog box appears.
5. Click *OK* to close the Server Backup Is Not Configured dialog box. The Choose A New Location For The Data page appears.



Move Microsoft SharePoint Foundation Data

Choose a new location for the data

Current location:

Local Disk (C:) 101 GB free

Microsoft SharePoint Foundation data (295 MB)

New location:

Drive	Free Space	Total Space
New Volume (E:)	39.9 GB	39.9 GB

How do I move the data on my server?

6. Select the volume where you want to move the SharePoint data and click *Move*. The wizard moves the data to the volume you selected and a The Microsoft SharePoint Foundation Data Was Moved Successfully page appears.
7. Click *Finish*. The wizard closes.

Migrating a SharePoint Website

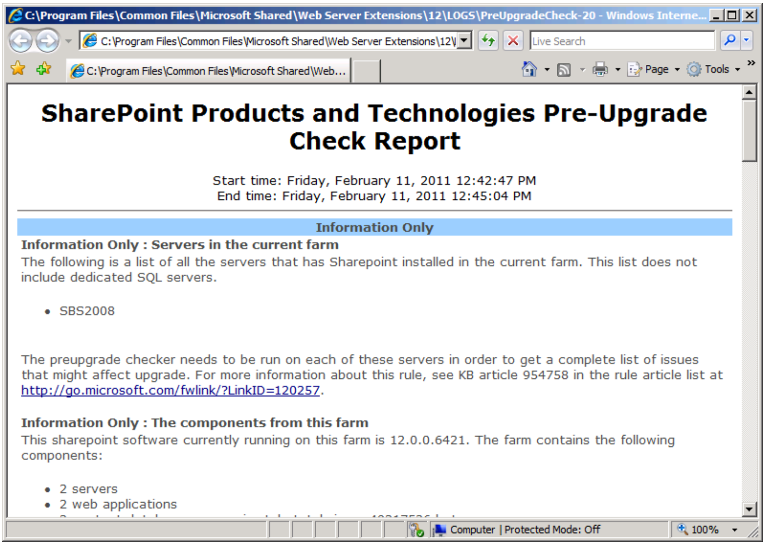
If you are migrating to Windows SBS 2011 from a previous version of Windows SBS and you have been using Windows SharePoint Services on your old server, you probably want to migrate your existing SharePoint database to your new server. Unfortunately, the process of migrating the SharePoint database is manual. When you run the Migrate To Windows Small Business Server 2011 Wizard on your Windows SBS 2011 server, *Migrate SharePoint web site* appears as one of the optional tasks. Selecting this task displays a link to the Microsoft TechNet library that provides detailed instructions for the migration process.

> ***MORE INFO*** **For more information on the process of migrating from Windows SBS 2008 to Windows SBS 2011, see Chapter 5, "Migrating to Windows SBS 2011."**

The process of migrating the SharePoint site from an existing Windows SBS 2008 server to your new Windows SBS 2011 server consists of the following tasks:

> ***CAUTION*** **Before you begin the SharePoint migration process, be sure that you have applied all the latest service packs and updates on both servers.**

- **Run the pre-upgrade checker** Built in to the Stsadm.exe command-line program, the pre-upgrade checker examines the SharePoint source data for any problems that can inhibit the upgrade process and generates a report.


C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\12\LOGS\PreUpgradeCheck-20 - Windows Interne...
C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\12\
Live Search
C:\Program Files\Common Files\Microsoft Shared\Web...
Page
Tools
Computer | Protected Mode: Off
100%

SharePoint Products and Technologies Pre-Upgrade Check Report

Start time: Friday, February 11, 2011 12:42:47 PM
End time: Friday, February 11, 2011 12:45:04 PM

Information Only

Information Only : Servers in the current farm
The following is a list of all the servers that has Sharepoint installed in the current farm. This list does not include dedicated SQL servers.

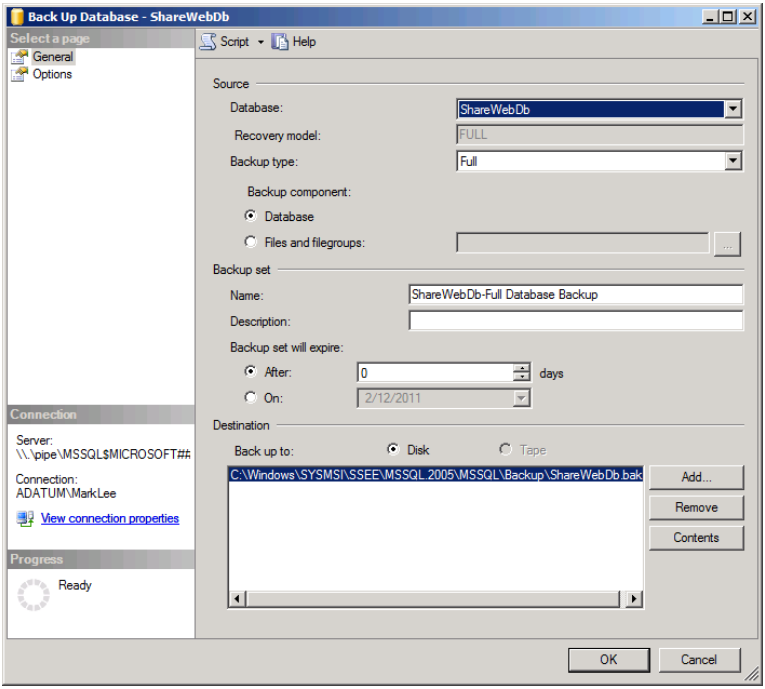
- SBS2008

The preupgrade checker needs to be run on each of these servers in order to get a complete list of issues that might affect upgrade. For more information about this rule, see KB article 954758 in the rule article list at http://go.microsoft.com/fwlink/?LinkID=120257.

Information Only : The components from this farm
This sharepoint software currently running on this farm is 12.0.0.6421. The farm contains the following components:

- 2 servers
- 2 web applications

- **Back up the content database on the existing source server** Using the SQL Server Management Studio Express Console on the source server, you can back up the SharePoint data from the database to a file on the local disk.



Back Up Database - ShareWebDb

Source

Database: ShareWebDb

Recovery model: FULL

Backup type: Full

Backup component:

● Database

○ Files and filegroups:

Backup set

Name: ShareWebDb-Full Database Backup

Description:

Backup set will expire:

● After: 0 days

○ On: 2/12/2011

Destination

Back up to: ● Disk ○ Tape

C:\Windows\SYSMSI\SSEE\MSSQL.2005\MSSQL\Backup\ShareWebDb.bak

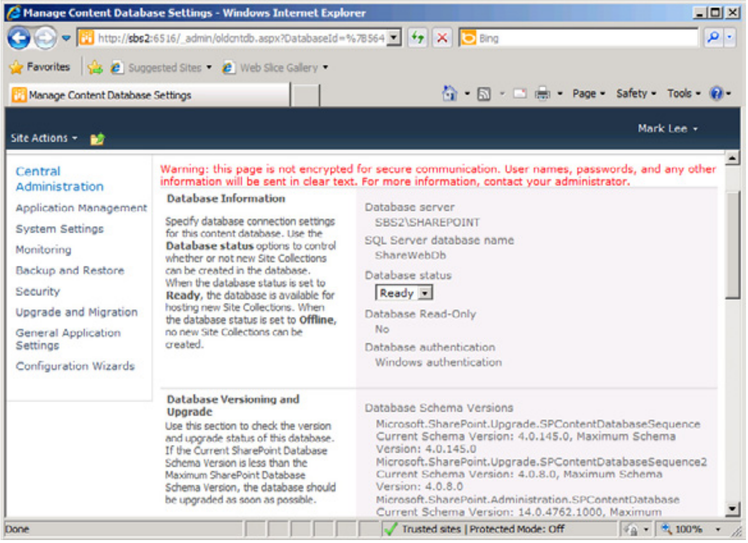
Connection

Server:
\\.\pipe\MSSQL$MICROSOFT##

Connection:
ADATUM\MarkLee

Ready

- **Remove the SharePoint database from the destination server** Before you can restore the database from your source server on the destination computer, you must remove the new (empty) database, using the SharePoint 2010 Central Administration website.



Manage Content Database Settings - Windows Internet Explorer

http://sbs2:6516/_admin/oldcntdb.aspx?DatabaseId=%7B564

Warning: this page is not encrypted for secure communication. User names, passwords, and any other information will be sent in clear text. For more information, contact your administrator.

Database Information

Specify database connection settings for this content database. Use the **Database status** options to control whether or not new Site Collections can be created in the database. When the database status is set to **Ready**, the database is available for hosting new Site Collections. When the database status is set to **Offline**, no new Site Collections can be created.

Database server
SBS2\SHAREPOINT

SQL Server database name
ShareWebDb

Database status
Ready

Database Read-Only
No

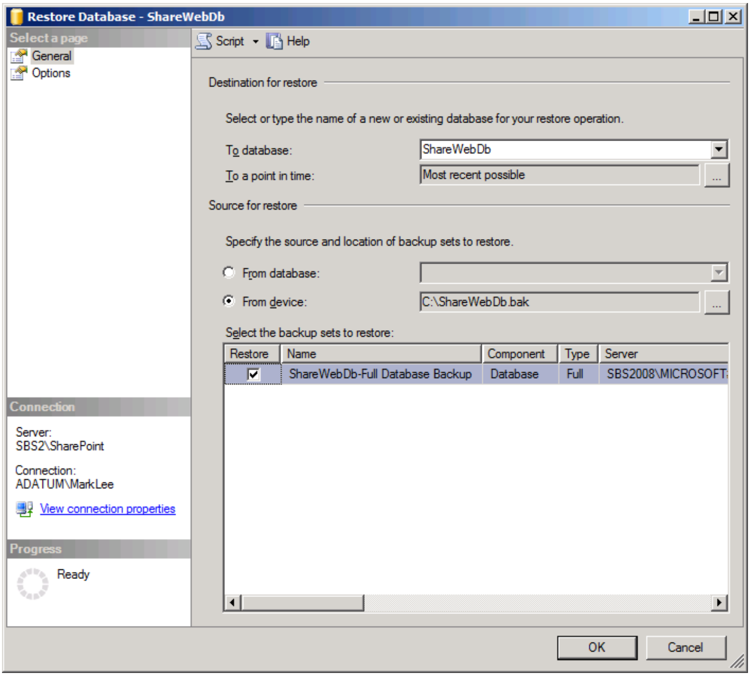
Database authentication
Windows authentication

Database Versioning and Upgrade

Use this section to check the version and upgrade status of this database. If the Current SharePoint Database Schema Version is less than the Maximum SharePoint Database Schema Version, the database should be upgraded as soon as possible.

Database Schema Versions
Microsoft.SharePoint.Upgrade.SPContentDatabaseSequence Current Schema Version: 4.0.145.0, Maximum Schema Version: 4.0.145.0
Microsoft.SharePoint.Upgrade.SPContentDatabaseSequence2 Current Schema Version: 4.0.8.0, Maximum Schema Version: 4.0.8.0
Microsoft.SharePoint.Administration.SPContentDatabase Current Schema Version: 14.0.4762.1000, Maximum

- **Restore the backed up database to the destination database** After deleting the existing SharePoint database on the destination server, you can restore the source database from the backup copy you made earlier.



Restore Database - ShareWebDb

Destination for restore

Select or type the name of a new or existing database for your restore operation.

To database: ShareWebDb

To a point in time: Most recent possible

Source for restore

Specify the source and location of backup sets to restore.

○ From database:

● From device: C:\ShareWebDb.bak

Select the backup sets to restore:

Restore	Name	Component	Type	Server
☑	ShareWebDb-Full Database Backup	Database	Full	SBS2008\MICROSOFT

Connection

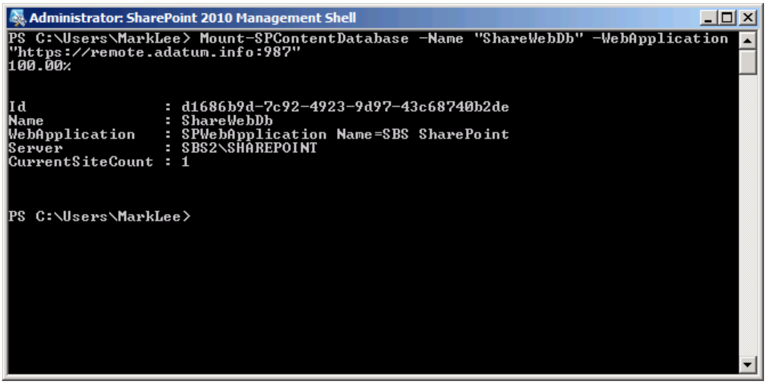
Server:
SBS2\SharePoint

Connection:
ADATUM\MarkLee

Progress

Ready

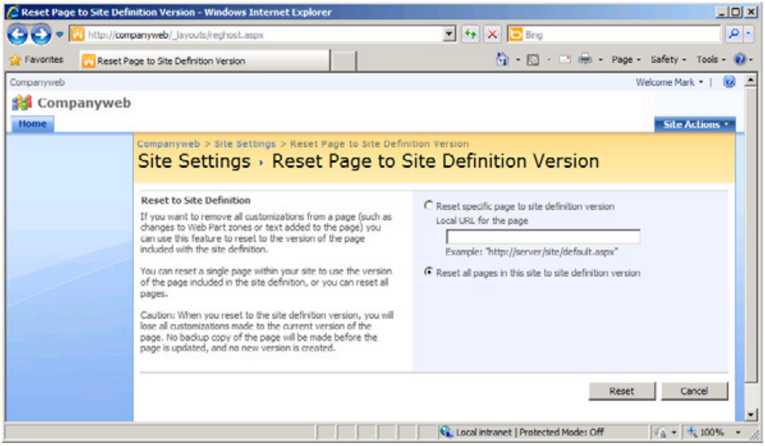
- **Mount the database** Use the SharePoint 2010 Management Shell to mount the newly restored database on the destination server.



Administrator: SharePoint 2010 Management Shell

```
PS C:\Users\MarkLee> Mount-SPContentDatabase -Name "ShareWebDb" -WebApplication
"https://remote.adatum.info:987"
100.00%


Id                : d1686b9d-7c92-4923-9d97-43c68740b2de
Name              : ShareWebDb
WebApplication    : SPWebApplication Name=SBS SharePoint
Server            : SBS2\SHAREPOINT
CurrentSiteCount : 1



PS C:\Users\MarkLee>
```

- **Enable SharePoint 2010 features** On the Site Settings page of the new Companyweb site, select the *Reset to site definition* and *visual upgrade* links to enable SharePoint Foundation 2010 features on your restored Windows SharePoint Services site.



Reset Page to Site Definition Version - Windows Internet Explorer

http://companyweb/_layouts/reghost.aspx

Companyweb > Site Settings > Reset Page to Site Definition Version

Site Settings › Reset Page to Site Definition Version

Reset to Site Definition

If you want to remove all customizations from a page (such as changes to Web Part zones or text added to the page) you can use this feature to reset to the version of the page included with the site definition.

You can reset a single page within your site to use the version of the page included in the site definiton, or you can reset all pages.

Caution: When you reset to the site definition version, you will lose all customizations made to the current version of the page. No backup copy of the page will be made before the page is updated, and no new version is created.

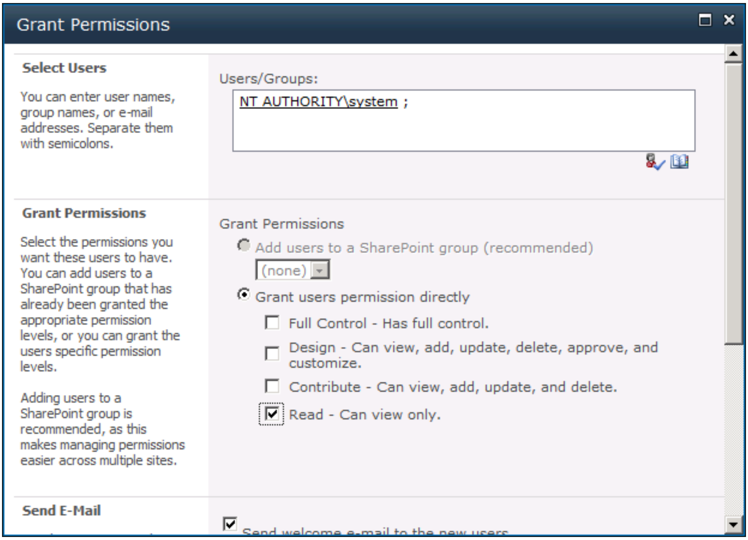
○ Reset specific page to site definition version

Local URL for the page

Example: "http://server/site/default.aspx"

● Reset all pages in this site to site definition version

- **Re-create the Read permissions on the destination server** Use the *Site permissions* control on the Site Settings page to grant the NT Authority\System user the Read permission.



Grant Permissions

Select Users

You can enter user names, group names, or e-mail addresses. Separate them with semicolons.

Users/Groups:

NT AUTHORITY\system ;

Grant Permissions

Select the permissions you want these users to have. You can add users to a SharePoint group that has already been granted the appropriate permission levels, or you can grant the users specific permission levels.

Adding users to a SharePoint group is recommended, as this makes managing permissions easier across multiple sites.

Grant Permissions

○ Add users to a SharePoint group (recommended)

(none)

● Grant users permission directly

□ Full Control - Has full control.

□ Design - Can view, add, update, delete, approve, and customize.

□ Contribute - Can view, add, update, and delete.

☑ Read - Can view only.

Send E-Mail

☑ Send welcome e-mail to the new users

The process of migrating the SharePoint data from a Windows SBS 2003 server to Windows SBS 2011 is slightly different, but consists of the same basic steps.

CHAPTER 18

Adding a Second Server

When you purchase the Windows Small Business Server (SBS) 2011 Premium Add-on product, you receive the software and the licenses needed to install a second server on your network running Windows Server 2008 R2. You also receive a copy of Microsoft SQL Server 2008 R2 Standard for Small Business to run on your additional server. Microsoft designed the Premium Add-on package to accommodate customers who want to deploy a second server for any reason, including running a SQL-based line-of-business (LOB) application.

The Windows SBS 2011 primary server is already performing many different roles, so adding another major application would, in most cases, be unwise. A secondary server provides a better platform for SQL-based applications and can perform other roles as well. You can use the second server as an additional file or print server, a Remote Desktop Services server, or even as a backup domain controller. This chapter examines the process of deploying an additional server on your network and describes some of the ways you can use it.

Expanding Your Network

Windows SBS 2011 is designed primarily for networks consisting of one or two servers and up to 75 workstations. However, a Windows SBS network is more expandable than many people think. First, although you can add a second server by purchasing the Windows SBS 2011 Premium Add-on, you don't have to implement your second server in this way. If you purchase Windows SBS 2011 Standard when you initially set up your network, you can always add a second server later by purchasing a copy of Windows Server 2008 R2.

The operating system for the second server in the Windows SBS 2011 Premium Add-on is Windows Server 2008 R2 Standard, with no additional components. No Windows SBS 2011 additions or restrictions are incorporated into the operating system. The Premium Add-on product also includes both 32-bit and 64-bit editions of SQL Server 2008 R2 for Small Business, which is not incorporated into the second server operating system, either. You receive it as a separate DVD, which you can run on either the 32-bit or 64-bit platform.

In other words, the only difference between buying the Windows SBS 2011 Premium Add-on product and buying standalone copies of Windows Server 2008 R2 and SQL Server 2008 R2 is the price. At this writing, the price for the Windows SBS 2011 Premium Add-on product is US $1604. To purchase the components individually would cost:

- Windows Server 2008 R2: US $1029
- SQL Server 2008 R2 Standard: US $898
- Windows SBS 2011 CAL Suite for Premium Add-on Users or Devices 5-pack: US $457

The total price would therefore be $2,384. You would save $780 by purchasing the Windows SBS 2011 Premium Add-on product, assuming that you needed all the components that product contains. If, for example, you only need a second server, but do not intend to run SQL applications, it would be more economical to buy a standalone copy of Windows Server 2008 R2.

Understanding Windows SBS 2011 Limitations

Running Windows SBS 2011 on your network is not the same as running Windows Server 2008 plus Microsoft Exchange Server 2007 and (optionally) SQL Server 2008 Standard, even if you disregard the differences in software costs. Windows SBS 2011 imposes certain limitations on the network with regard to the additional servers and workstations you can add to the network, although they are not as stringent as some people think. These limitations include the following:

- Your Windows SBS 2011 network can consist of only one Active Directory Domain Services (AD DS) domain, with the Windows SBS primary server functioning as the first domain controller in this root domain.
- You cannot install more than one Windows SBS 2011 primary server in a single AD DS domain, even if you purchase an additional license.
- You cannot create subdomains, such as newyork.adatum.local, beneath the AD DS domain you create on your Windows SBS 2011 server.
- You cannot establish trusts between your Windows SBS 2011 domain and any other AD DS domain, whether running on Windows SBS 2011, Windows Server 2008 R2, or any other operating system.

- You can install the second server included with Windows SBS 2011 Premium Add-on only on your Windows SBS 2011 network. You cannot install it on another network or use it as the domain controller for another AD DS domain.
- You can install the copy of SQL Server 2008 R2 for Small Business included with Windows SBS 2011 Premium Add-on on the Windows SBS 2011 primary or secondary server. You cannot install it on a non-SBS server or network.

> ***CAUTION*** **Although you can install SQL Server 2008 R2 on your primary server, you must not use it to host the SBSMONITORING or Windows Server Update Services databases that Windows SBS 2011 creates. You can move the SharePoint Foundation 2010 content database to SQL Server 2008 R2, running on either your primary or secondary server, but you cannot move the SharePoint configuration or search databases.**

- You cannot install the copy of Exchange Server 2010 Standard included with Windows SBS 2011 on any server other than the Windows SBS 2011 primary server.
- You cannot use more than 75 Client Access Licenses (CALs) on your Windows SBS 2011 network.

With these limitations in mind, this means that you can do either of the following:

- You can add as many additional servers as you want to your Windows SBS 2011 network, so long as you purchase appropriate licenses for any servers other than the secondary server included with the Premium Add-on package.
- You can add as many domain controllers as you want to your Windows SBS 2011 domain, using the Windows SBS secondary server or any additional Windows Server 2008 R2 computers.

Understanding Licensing for Additional Servers

When you purchase the Windows SBS 2011 Premium Add-on product, you receive an additional license for a secondary server, running the Windows Server 2008 R2 operating system included with the product. You also receive a license to install SQL Server 2008 R2 Small Business on that secondary server. The terms for the secondary server licenses are the same as those for the primary server.

However, you are not required to install SQL Server 2008 R2 on the secondary server, nor are you required to install the secondary server at all. If you prefer to hold off on deploying the secondary server until later, you can do so, but, as mentioned earlier, you cannot use the license to deploy the secondary server on another network.

If you want to install additional servers on your Windows SBS 2011 network other than the ones supplied with Standard Edition and the Premium Add-on, you are free to do so. However, you must purchase an appropriate license for each copy of Windows Server 2008 R2 you plan to deploy, using any of the standard

Microsoft licensing options. For example, you can purchase a new computer with an original equipment manufacturer (OEM) license included, or purchase a retail copy of Windows Server 2008 R2 and install it on an existing computer. You can also purchase a license through Microsoft Open Value Licensing (MOVL) or Microsoft Open License Program (MOLP). The type of license you choose does not have to match that of your Windows SBS 2011 license.

It is important to understand, however, that many vendors bundle the Windows Server 2008 R2 server license with a number of CALs, which adds to the cost. You do not need to purchase additional CALs when you add a server to your Windows SBS 2011 network. The Windows SBS 2011 Standard or Premium CALs you have purchased for your Windows SBS 2011 users or devices enable them to access any additional Windows Server 2008 R2 computers, so long as you join those servers to your Windows SBS domain.

> ***NOTE*** **If you plan to use the Remote Desktop Services or Rights Management Services capabilities built into Windows Server 2008 R2, you must purchase the appropriate RDS or RMS CALs for the users that will be accessing those services.**

Deploying a Second Server

As discussed earlier in this chapter, the Windows SBS 2011 Premium Add-on enables you to install a second server on your network for any purpose you wish. What you plan to do with the server determines what hardware the computer requires and how the installation should proceed. These are some of the roles for which you might use a second server:

- **File and print server** If your users have heavy file storage and printing requirements, if might be beneficial to move your file and print services to a second server.
- **Second domain controller** A second domain controller can provide redundancy on a local network, but it can also enable a branch office to access AD DS resources without having to connect to a remote domain controller over a wide area network (WAN) link.
- **Secondary web server** The primary Windows SBS 2011 server uses Internet Information Services (IIS) to host SharePoint Foundation 2010 and perform a variety of administrative tasks. You can use IIS on a secondary server to deploy additional websites and web-based intranet applications that might overwhelm the primary server.

- **Remote Desktop Services application server** The primary server on a Windows SBS 2011 network cannot function as a Remote Desktop Services server, but you can use a secondary server for this purpose, eliminating the need to install applications on individual workstations.
- **SQL Server–based application server** Using SQL Server 2008 R2, the secondary server can provide services to your network using a wide variety of applications, either existing or custom-developed.

Planning a Second Server Deployment

The role or roles you want your second server to perform determine what type of computer you should buy and what hardware and software you should install. As discussed in Chapter 3, "Installing Windows Small Business Server (SBS) 2011," planning is a crucial part of the network deployment process, and your plan for your secondary server should be no less detailed than that for your primary one.

Determining System Hardware Requirements

The first step of the deployment process is selecting the server hardware. The first decision to make is that of the processor platform. Unlike the Windows SBS 2011 primary server, which requires a computer with a 64-bit processor, your secondary server can conceivably be a 32-bit or 64-bit computer. Although Windows Server 2008 R2 runs on 64-bit computers only, the version of SQL Server 2008 R2 supplied with the Premium Add-on product includes both 32-bit and 64-bit versions of the software. You can conceivably install SQL Server 2008 R2 on an existing 32-bit server with an older version of Windows Server running on it and add that server to the Windows SBS network.

If you are purchasing a new computer for your second server, then it will almost certainly be capable of running the 64-bit versions of both Windows Server 2008 R2 and SQL Server 2008 R2. Before you make this decision, however, be sure that all the applications you plan to use on the secondary server run on the platform you select.

> ***TIP*** **If you are migrating from an earlier version of Windows SBS to Windows SBS 2011 with the Premium Add-on, you might want to consider buying a new computer for your primary server and, after the migration process is complete, reinstalling your old server to make it the secondary server on your Windows SBS 2011 network.**

Adding Role-Specific Hardware

The base system requirements for the secondary server are listed in Chapter 3, but you must also determine whether you need additional hardware, which depends on the details of the server's role. For example, if you plan to deploy a file server, you must decide how much storage you need for your users, in addition to that required for the operating system, and what type of storage you want to use. You should also plan for future growth and purchase a computer to which you can add more storage and more memory later.

A modest file server for a very small network might just have one or two Serial ATA (SATA) hard disks. For a slightly larger network that has all its users constantly accessing server files, you might want to move up to Small Computer System Interface (SCSI) disks, and, if your applications require fault tolerance, you might want use a redundant array of independent disks (RAID). The amount of storage you have in the server will also influence the amount of memory it needs.

> ***MORE INFO*** **For more information on choosing a server configuration, see the section entitled "Selecting Server Hardware," in Chapter 3.**

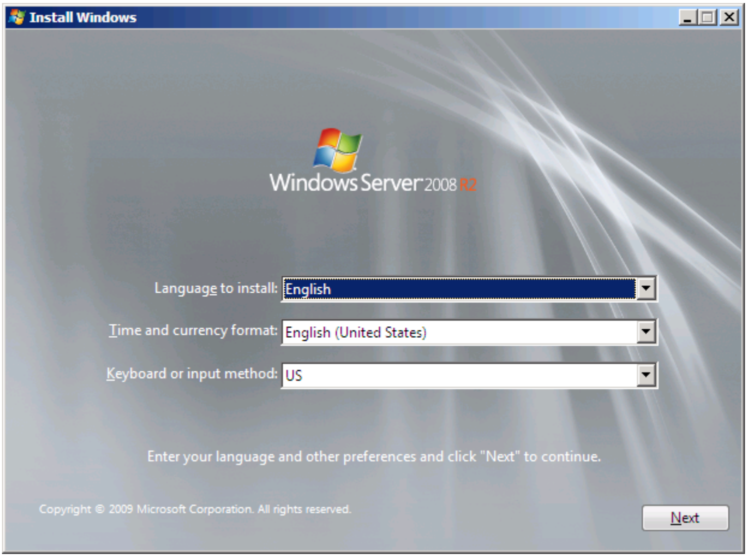
For an application server, the planning process should begin by selecting the applications you intend to run. For example, if you are going to deploy a Remote Desktop Services application server, you should list all the applications you want to provide to network users, along with the maximum number of users that will access each application at the same time. These factors affect the server's storage configuration, and more importantly, its memory capacity.

For business-specific web and SQL Server–based applications, you must select the exact applications you plan to run before you begin shopping for hardware. If you intend to purchase an existing application, the manufacturer usually has specific hardware requirements that you must observe. If you intend to work with software developers to create your own custom application, the selection of the server hardware should be a collaborative effort between your organization and the developers.

Installing a Second Server

To install a secondary server running Windows Server 2008 R2 on your network, use the following procedure:

1. Turn on the computer and insert the appropriate additional server disk from the Windows SBS 2011 Premium Add-on package into the DVD-ROM drive.
2. Press a key to boot from the DVD if the system prompts you to do so. The computer reads from the DVD and displays the first page of the Install Windows Wizard.



Language to install: English

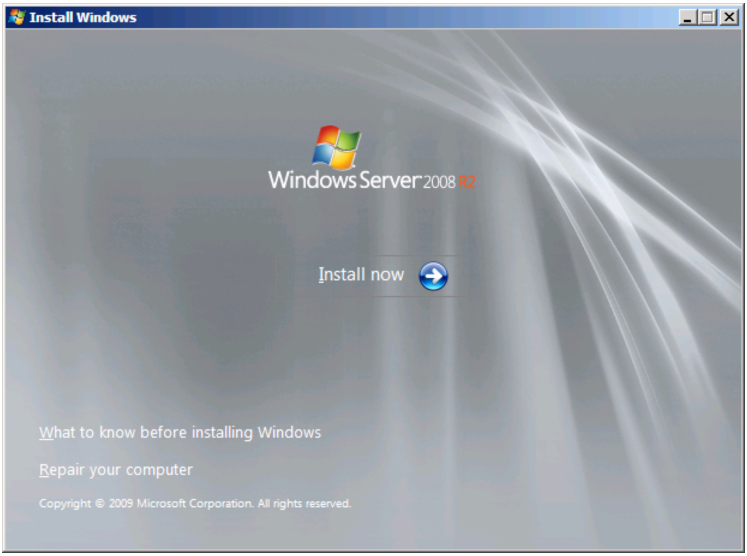
Time and currency format: English (United States)

Keyboard or input method: US

Enter your language and other preferences and click "Next" to continue.

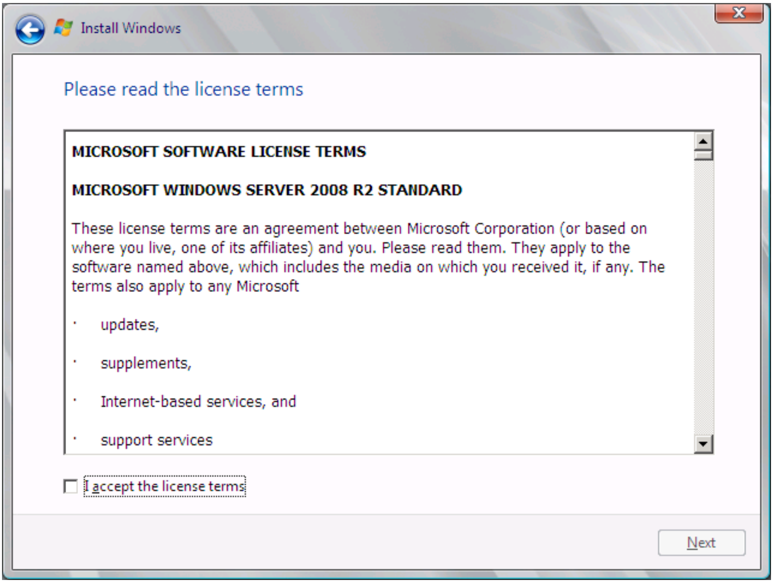
Copyright © 2009 Microsoft Corporation. All rights reserved.

3. If you plan to use language, time and currency format, or keyboard settings other than the defaults, select your preferences from the three drop-down lists on this page. Then click *Next*. The Install Now page appears.



Copyright © 2009 Microsoft Corporation. All rights reserved.

4. Click *Install now*. The Please Read The License Terms page appears.



Please read the license terms

MICROSOFT SOFTWARE LICENSE TERMS

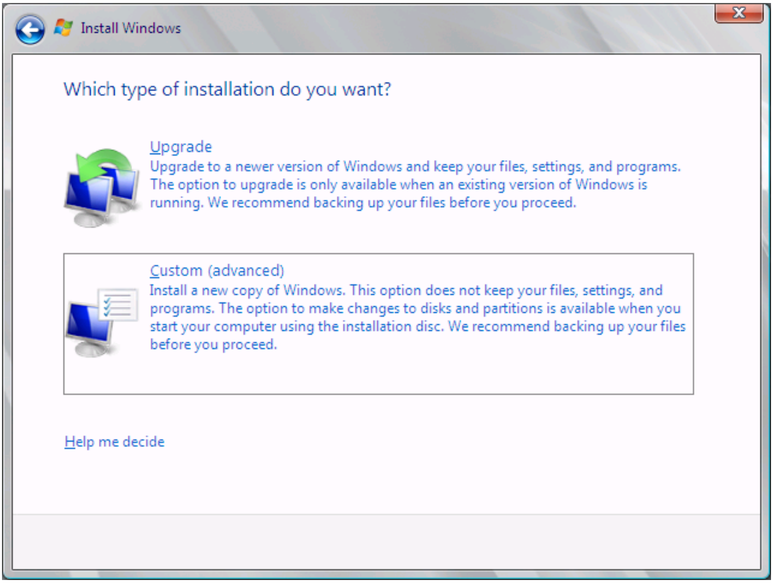
MICROSOFT WINDOWS SERVER 2008 R2 STANDARD

These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to the software named above, which includes the media on which you received it, if any. The terms also apply to any Microsoft

- updates,
- supplements,
- Internet-based services, and
- support services

□ I accept the license terms

5. Select the *I accept the license terms* check box and click *Next*. The Which Type Of Installation Do You Want? page appears.

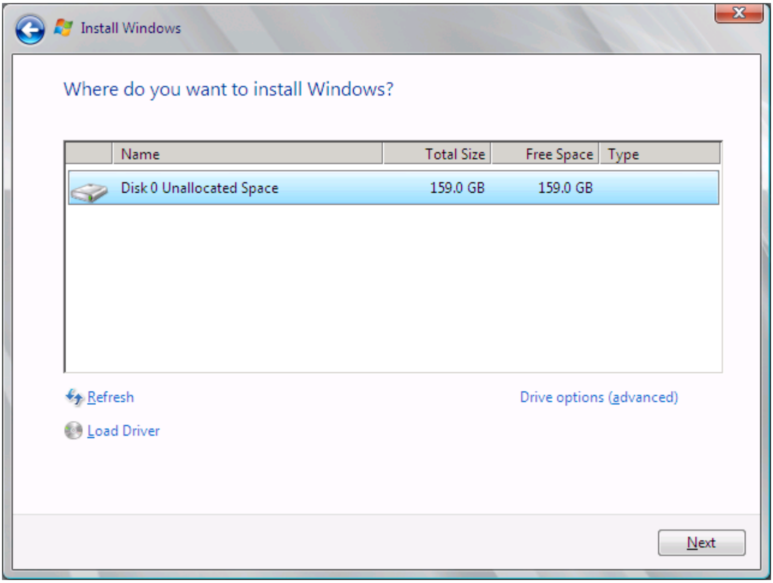


Which type of installation do you want?

Upgrade
Upgrade to a newer version of Windows and keep your files, settings, and programs. The option to upgrade is only available when an existing version of Windows is running. We recommend backing up your files before you proceed.

Custom (advanced)
Install a new copy of Windows. This option does not keep your files, settings, and programs. The option to make changes to disks and partitions is available when you start your computer using the installation disc. We recommend backing up your files before you proceed.

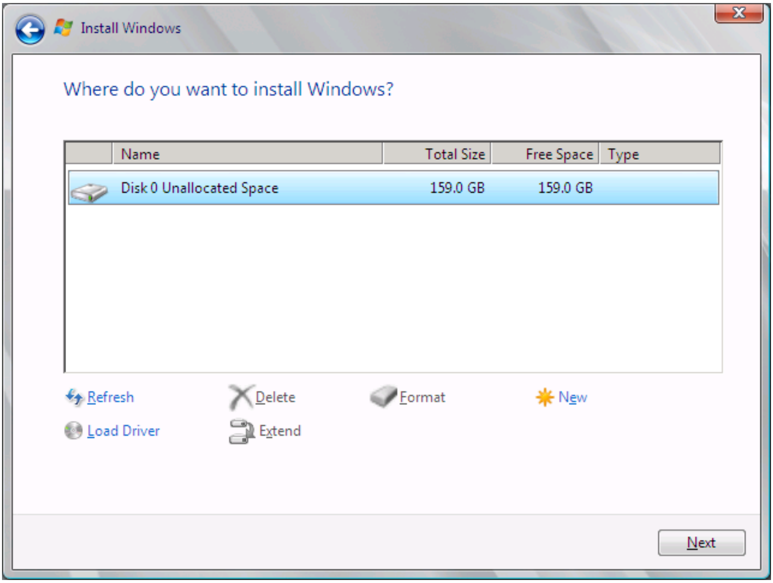
6. Click *Custom (advanced)*. The Where Do You Want To Install Windows? page appears.



Where do you want to install Windows?

	Name	Total Size	Free Space	Type
	Disk 0 Unallocated Space	159.0 GB	159.0 GB	

7. To create a partition on a disk, click *Drive options (advanced)* to display additional controls.

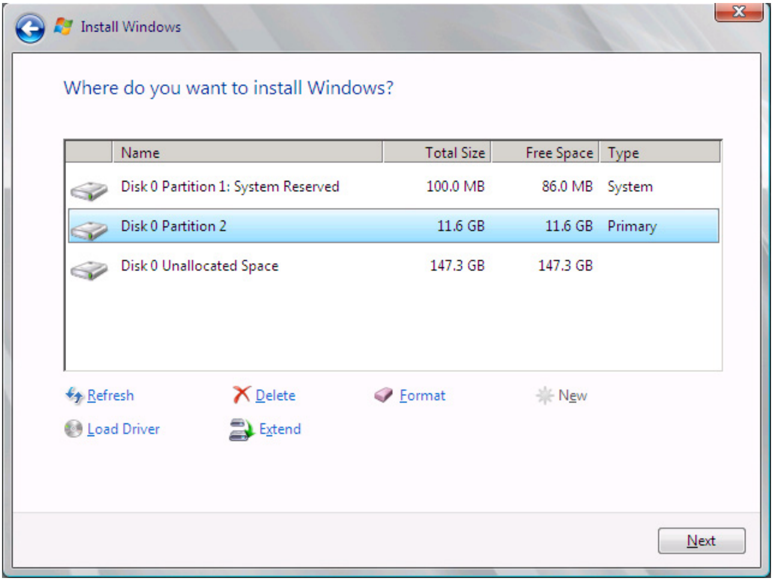


Where do you want to install Windows?

	Name	Total Size	Free Space	Type
	Disk 0 Unallocated Space	159.0 GB	159.0 GB	

8. Select the disk on which you want to create the partition and click *New*. In the *Size* box that appears, specify a size greater than 12,740 megabytes (MB) for the partition and click *Apply*. An Install Windows message box appears, informing you that Windows might create additional partitions on the disk.

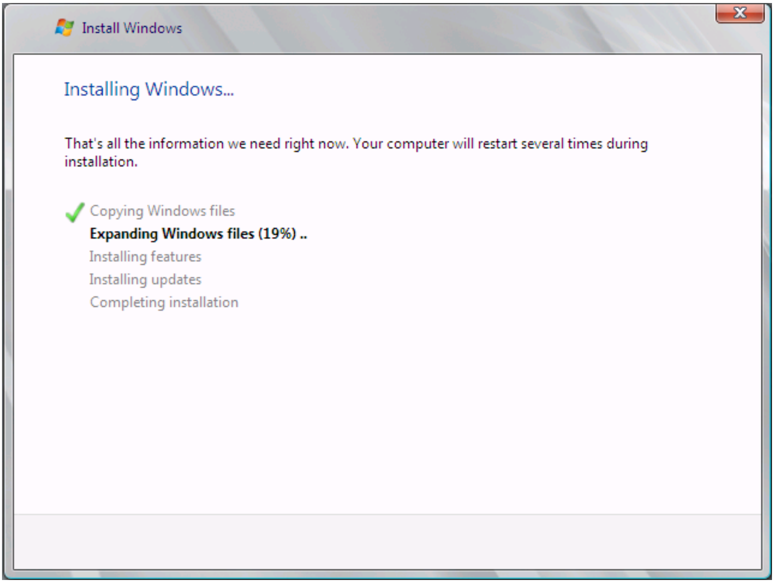
9. Click *OK*. The new partition appears in the list.



Where do you want to install Windows?

Name	Total Size	Free Space	Type
Disk 0 Partition 1: System Reserved	100.0 MB	86.0 MB	System
Disk 0 Partition 2	11.6 GB	11.6 GB	Primary
Disk 0 Unallocated Space	147.3 GB	147.3 GB	

10. Select the partition on which you want to install Windows Server 2008 R2 and click Next. The Installing Windows page appears, and the setup program proceeds through the various stages of the operating system installation.

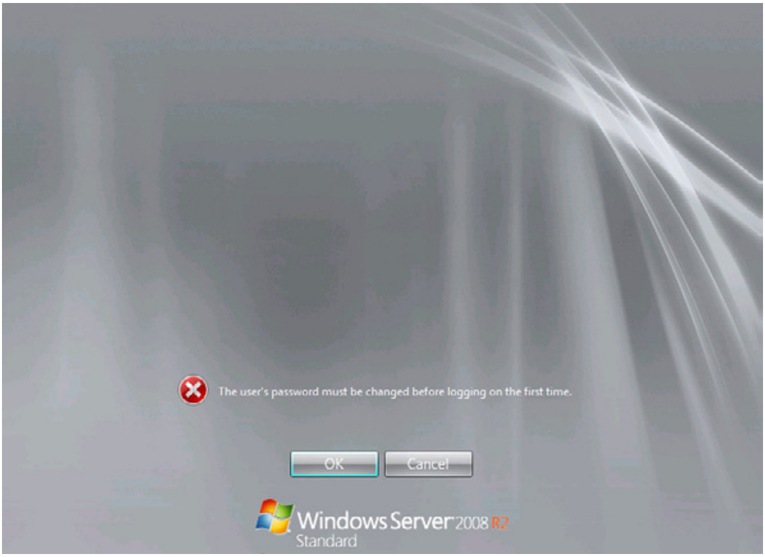


Installing Windows...

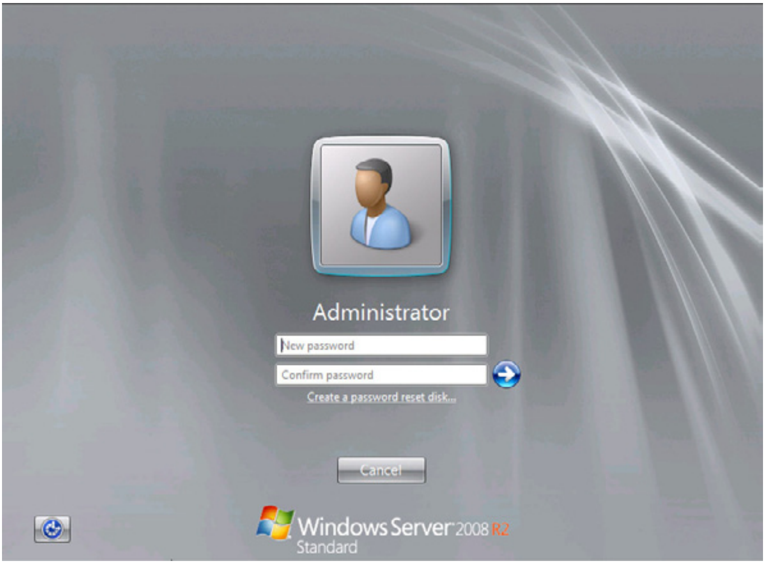
That's all the information we need right now. Your computer will restart several times during installation.

✓ Copying Windows files
Expanding Windows files (19%) ..
Installing features
Installing updates
Completing installation

When this phase of the installation process is completed, the computer restarts, and a message appears, stating that you must change the password.


The user's password must be changed before logging on the first time.

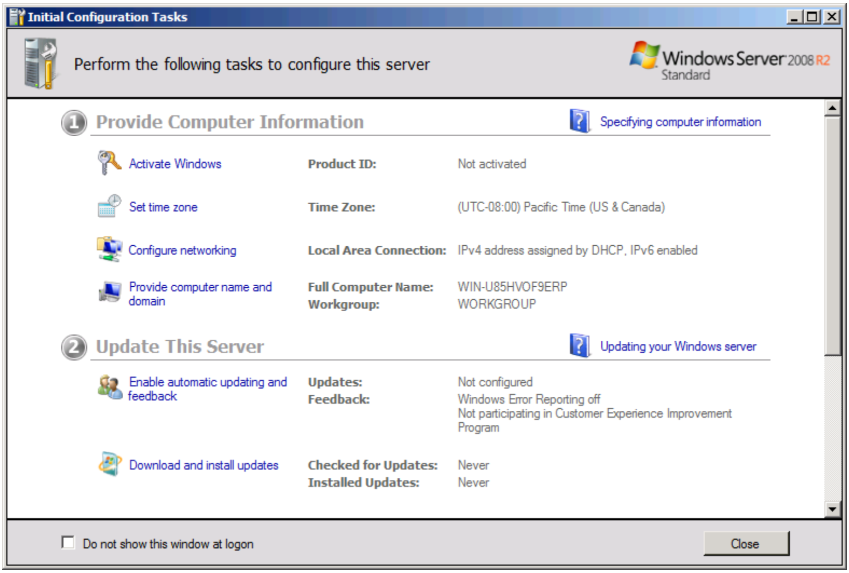
11. Click *OK*. A Windows logon page appears.



12. Type a password for the local Administrator account in the *New password* and *Confirm password* text boxes, and click the right arrow button. A message appears, stating that the password has been changed.
13. Click *OK*. The Windows desktop appears.

Performing Post-Installation Tasks

Once the Windows Server 2008 R2 installation process is finished, you see the Initial Configuration Tasks window, as shown in Figure 18-1. Unlike the primary server installation, which automatically configures many of the computer's settings, the secondary server installation is a bare-bones affair. You must configure the server yourself and add the roles and features it needs to provide the services you want.



Initial Configuration Tasks

Perform the following tasks to configure this server

Windows Server 2008 R2
Standard

1 Provide Computer Information — Specifying computer information

Activate Windows — **Product ID:** Not activated

Set time zone — **Time Zone:** (UTC-08:00) Pacific Time (US & Canada)

Configure networking — **Local Area Connection:** IPv4 address assigned by DHCP, IPv6 enabled

Provide computer name and domain — **Full Computer Name:** WIN-U85HVOF9ERP
Workgroup: WORKGROUP

2 Update This Server — Updating your Windows server

Enable automatic updating and feedback — **Updates:** Not configured
Feedback: Windows Error Reporting off
Not participating in Customer Experience Improvement Program

Download and install updates — **Checked for Updates:** Never
Installed Updates: Never

☐ Do not show this window at logon

Close

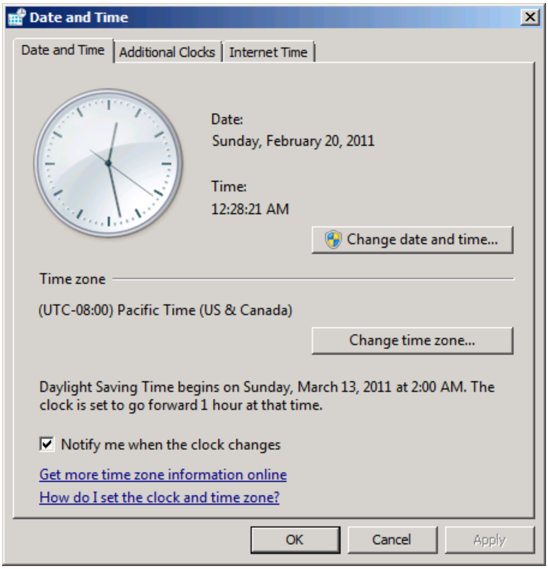
FIGURE 18-1 The Initial Configuration Tasks window.

The following sections describe the procedures you must perform on a newly installed secondary server.

Adjusting Time Zone Settings

By default, new Windows Server 2008 R2 computers are configured to use the Pacific time zone. To change the computer to another time zone, use the following procedure:

1. Log on to Windows Server 2008 R2 using the local Administrator account. The Initial Configuration Tasks window appears.
2. In the *Provide computer information* section, click *Set time zone*. The Date And Time dialog box appears.



Date:
Sunday, February 20, 2011

Time:
12:28:21 AM

Time zone

(UTC-08:00) Pacific Time (US & Canada)

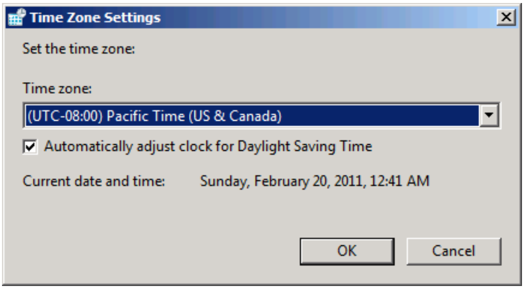
Daylight Saving Time begins on Sunday, March 13, 2011 at 2:00 AM. The clock is set to go forward 1 hour at that time.

☑ Notify me when the clock changes

Get more time zone information online

How do I set the clock and time zone?

3. Click *Change time zone*. The Time Zone Settings dialog box appears.



Set the time zone:

Time zone:
(UTC-08:00) Pacific Time (US & Canada)

☑ Automatically adjust clock for Daylight Saving Time

Current date and time: Sunday, February 20, 2011, 12:41 AM

4. In the *Time zone* drop-down list, select the correct time zone for your location and click *OK*.

   TIP **If you are installing a server that you will move to another location later, such as a branch office, select the time zone for the server's final location.**

5. Click *OK* to close the Date And Time dialog box.

Configuring Network Settings

By default, a newly installed computer running Windows Server 2008 R2 attempts to obtain an Internet Protocol (IP) address and other Transmission Control Protocol/Internet Protocol (TCP/IP) settings from a Dynamic Host Configuration Protocol

(DHCP) server on the local network. If your primary server is functioning as a DHCP server, as described in Chapter 3, "Installing Windows Small Business Server (SBS) 2011," the secondary server automatically configures its network interface using TCP/IP settings it obtains from the primary server.

> ***MORE INFO*** **For more information on IP addressing and DHCP, see Chapter 2, "A Networking Primer."**

Depending on the tasks you expect your secondary server to perform, this default arrangement might not be satisfactory. When a computer obtains its IP address using DHCP, it is possible that the address might change someday. For standard Windows server functions, such as file and printer sharing, this is usually not a problem because the DHCP server changes the domain's Domain Name System (DNS) records when it changes the IP address. This enables the other computers on the network to locate the secondary server, no matter how often its address changes.

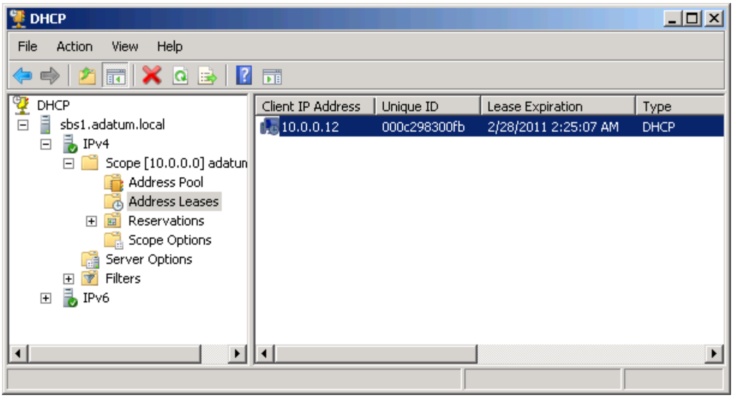
However, certain roles and applications require a server to have a static IP address. For example, if you intend to configure the secondary server to function as a domain controller or as a second DHCP server, you must reconfigure the network settings with a static IP address.

When you ran the Connect To The Internet Wizard on your primary server, the wizard configured the DHCP Server service by creating an address scope and excluding certain IP addresses from that scope, including the addresses of your router and of the primary server itself. This prevents DHCP from assigning those addresses to other computers. If you plan to assign a static IP address to your secondary server, you should use one of these excluded addresses or create a new exclusion, if necessary.

There are two ways to configure your server to use a static IP address: You can create a DHCP reservation that permanently associates the server's hardware address with a specific IP address assignment, or you can manually configure the TCP/IP client on the server.

CREATING A DHCP RESERVATION

The procedure for creating a DHCP reservation for your server is the same as the one described in the section entitled "Creating a DHCP Reservation for a Printer" in Chapter 10, "Sharing Printers." When you look at the *Address leases* node in the DHCP Console, you see your secondary server's lease, as shown in Figure 18-2. As with a printer, the server has an arbitrary name specified by the device. The *Unique ID* value displayed in the lease entry is the hardware address you use when creating the reservation.



Client IP Address	Unique ID	Lease Expiration	Type
10.0.0.12	000c298300fb	2/28/2011 2:25:07 AM	DHCP

FIGURE 18-2 The IP address lease of a newly installed secondary server, as displayed in the *Address leases* node of the DHCP Console.

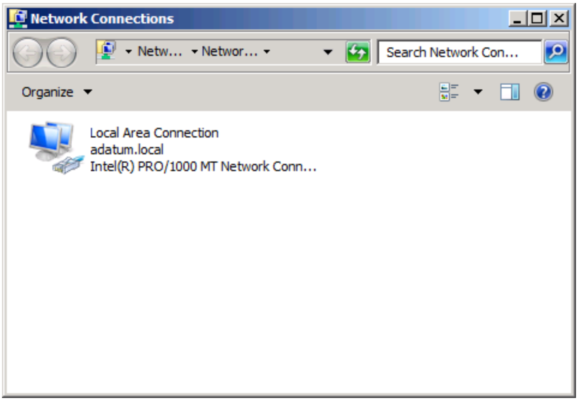
> ***TIP*** **To confirm that you are using the correct Unique ID value when creating your DHCP reservation, check the computer name selected by your secondary server during the operating system installation, which appears in the Initial Configuration Tasks window, in the *Provide computer informatio*n section.**

Once you have created the DHCP reservation, restart the secondary server to force its DHCP client to reconfigure the computer's TCP/IP settings using the address you reserved.

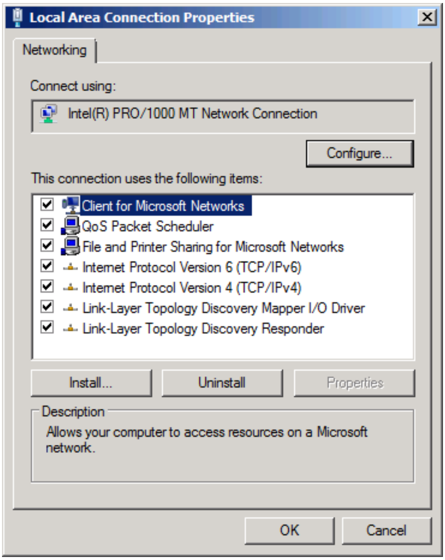
CONFIGURING THE TCP/IP CLIENT

If you choose to configure your server's TCP/IP client manually, you must still use an IP address that is excluded from your DHCP scope. Once you have determined an appropriate address, use the following procedure to complete the configuration:

1. Log on to your secondary server using the local Administrator account.
   The Initial Configuration Tasks window appears.
2. In the *Provide computer information* section, click *Configure networking*.
   The Network Connections window appears.



3. Right-click the *Local area connection* icon and, from the context menu, select *Properties*. The Local Area Connection Properties sheet appears.



Connect using:

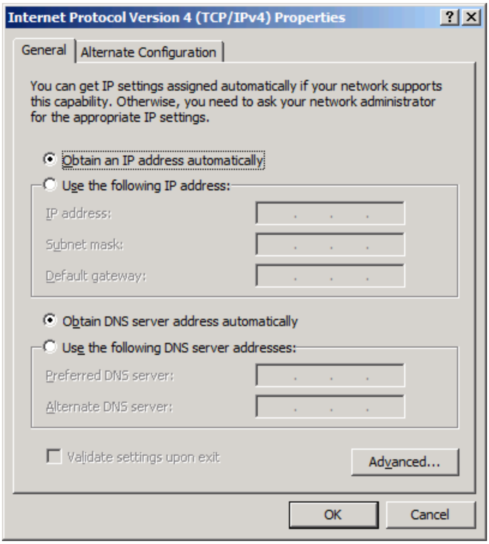
Intel(R) PRO/1000 MT Network Connection

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Allows your computer to access resources on a Microsoft network.

4. Select the *Internet Protocol Version 4 (TCP/IPv4)* component and click *Properties*. The Internet Protocol Version 4 (TCP/IPv4) Properties sheet appears.



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

5. Select the *Use the following IP address* option.
6. In the *IP address* text box, type the excluded address you want to use for your server, and in the *Subnet mask* text box, type the appropriate mask for your network.
7. In the *Default gateway* text box, type the IP address of your Internet access router.
8. In the *Preferred DNS server* text box, type the IP address of your primary Windows SBS 2011 server and click *OK*.
9. Click *OK* to close the Local Area Connection Properties sheet.
10. Close the Network Connections window.

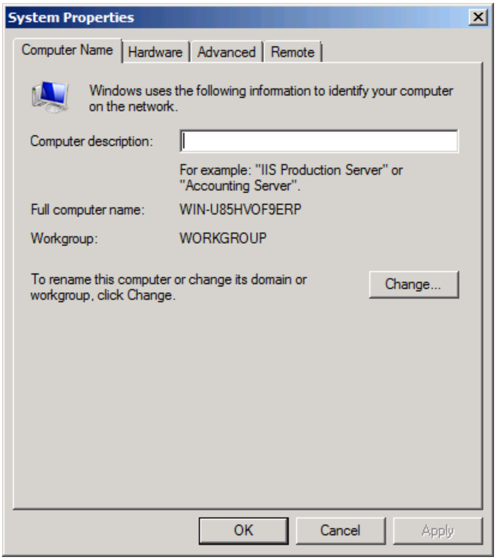
Changing the Computer Name and Joining the Domain

During the operating system installation on your secondary server, the Windows Server 2008 R2 setup program selects an arbitrary computer name, one that no other computer on the local network possesses. During the initial planning phase of your network deployment, you should have devised a computer-naming scheme that enables you to select an appropriate name for your server easily. You also have to join the server to your AD DS domain manually.

MORE INFO **For more information on computer naming, see the section entitled "Selecting Names," in Chapter 3.**

To change your server's computer name and join it to your domain, use the following procedure:

1. Log on to Windows Server 2008 R2 using the local Administrator account. The Initial Configuration Tasks window appears.
2. In the *Provide computer information* section, click *Provide computer name and domain*. The System Properties sheet appears.



System Properties

Windows uses the following information to identify your computer on the network.

Computer description:

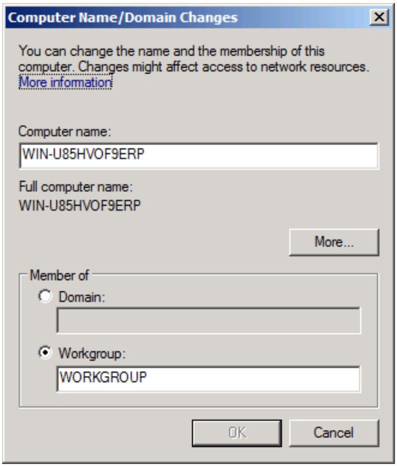
For example: "IIS Production Server" or "Accounting Server".

Full computer name: WIN-U85HVOF9ERP

Workgroup: WORKGROUP

To rename this computer or change its domain or workgroup, click Change.

3. Click *Change*. The Computer Name/Domain Changes dialog box appears.



Computer Name/Domain Changes

You can change the name and the membership of this computer. Changes might affect access to network resources. More information

Computer name: WIN-U85HVOF9ERP

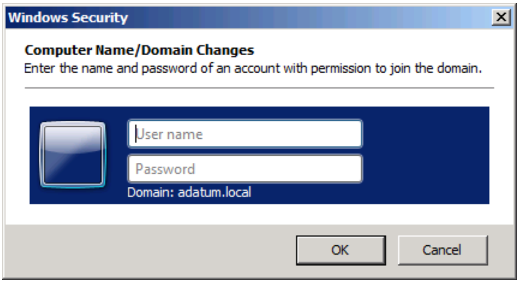
Full computer name: WIN-U85HVOF9ERP

Member of

○ Domain:

● Workgroup: WORKGROUP

4. In the *Computer name* text box, type the name you selected for your server.
5. In the *Member of* box, select the *Domain* option and type the full name of your AD DS domain.
6. Click *OK*. A Windows Security dialog box appears.



Windows Security

Computer Name/Domain Changes

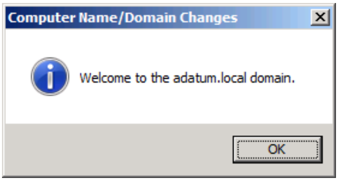
Enter the name and password of an account with permission to join the domain.

User name

Password

Domain: adatum.local

7. In the *User name* text box, type the name of the network Administrator account you created when installing your primary server.
8. In the *Password* text box, type the password associated with the account and click *OK*. A Computer Name/Domain Changes message box appears, welcoming you to the domain.



Computer Name/Domain Changes

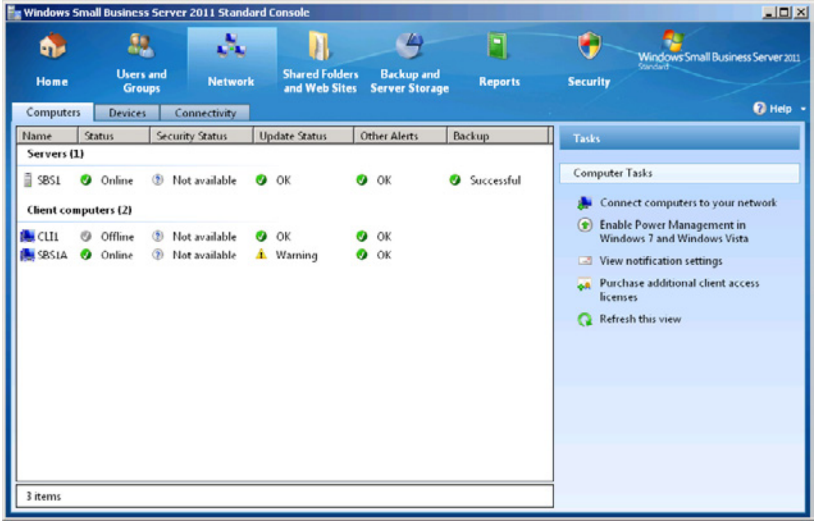
Welcome to the adatum.local domain.

9. Click *OK*. Another message box appears, informing you that you must restart the computer.
10. Click *OK*. Then click *Close* to close the System Properties sheet. A Windows message box appears, prompting you to restart the computer.
11. Click *Restart now*. The computer restarts.

Once the computer has restarted, you can log on using a domain account instead of the local administrator account.

Moving the Computer Object

Once you have joined the secondary server to your AD DS domain, the server appears in the Windows SBS Console, on the *Network/Computers* tab, as shown in Figure 18-3. However, notice that the server appears in the *Client computers* section, not the *Servers* section. This is because during the process of joining the server to the domain, the domain controller has no way of distinguishing a server from a workstation.


Windows Small Business Server 2011 Standard Console
Home
Users and Groups
Network
Shared Folders and Web Sites
Backup and Server Storage
Reports
Security
Windows Small Business Server 2011 Standard
Help
Computers
Devices
Connectivity

Name	Status	Security Status	Update Status	Other Alerts	Backup
Servers (1)					
SBS1	Online	Not available	OK	OK	Successful
Client computers (2)					
CLI1	Offline	Not available	OK	OK	
SBS1A	Online	Not available	Warning	OK	

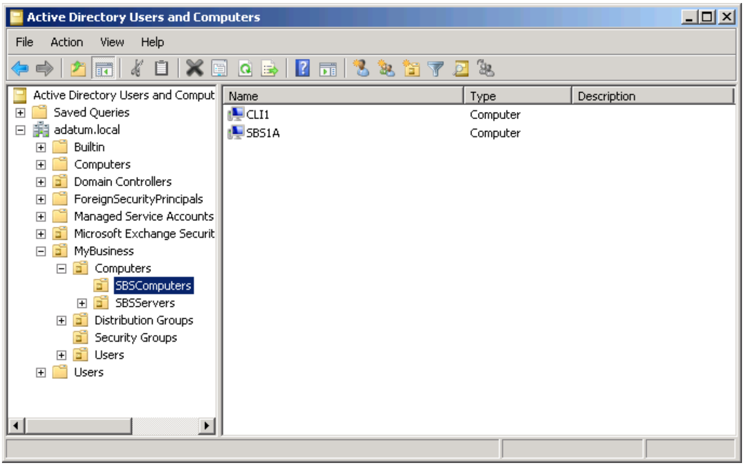
3 items

Tasks
Computer Tasks
Connect computers to your network
Enable Power Management in Windows 7 and Windows Vista
View notification settings
Purchase additional client access licenses
Refresh this view

FIGURE 18-3 A newly joined secondary server, as shown in the Windows SBS Console.

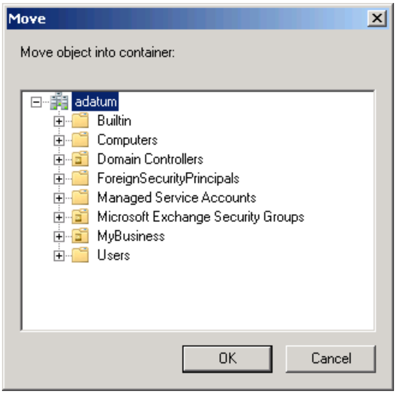
To move the secondary server to the *Servers* section and configure it to receive the Group Policy settings intended for servers, perform the following:

1. Log on to your Windows SBS 2011 primary server using the local Administrator account. The Windows SBS Console appears.
2. Click *Start*. Then click *Administrative tools*, *Active Directory users and computers*. The Active Directory Users And Computers Console appears.
3. Expand the node named for your domain and browse to the *My business/ Computers/SBSComputers* organizational unit (OU).



Name	Type	Description
CLI1	Computer	
SBS1A	Computer	

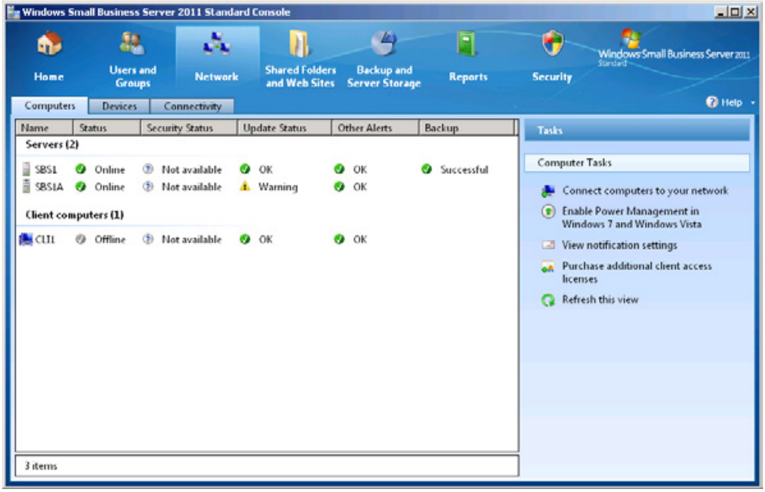
4. Right-click the computer object representing your secondary server and, in the context menu, select *Move*. The Move dialog box appears.



Move object into container:

- adatum
  - Builtin
  - Computers
  - Domain Controllers
  - ForeignSecurityPrincipals
  - Managed Service Accounts
  - Microsoft Exchange Security Groups
  - MyBusiness
  - Users

5. In your domain, browse to and select the *My business/Computers/SBSServers* OU and click *OK*. The console moves the computer object to the *SBSServers* container.
6. Close the Active Directory Users And Computers Console.
7. In the Windows SBS Console, click *Network* and select the *Computers* tab.
8. In the *Tasks* list, click *Refresh this view*. Your secondary server moves from the *Client computers* section to the *Servers* section.


Windows Small Business Server 2011 Standard Console
Home
Users and Groups
Network
Shared Folders and Web Sites
Backup and Server Storage
Reports
Security
Windows Small Business Server 2011 Standard
Computers
Devices
Connectivity
Help
Tasks
Computer Tasks
3 items

Name	Status	Security Status	Update Status	Other Alerts	Backup
Servers (2)					
SBS1	Online	Not available	OK	OK	Successful
SBS1A	Online	Not available	Warning	OK	
Client computers (1)					
CLI1	Offline	Not available	OK	OK	

- Connect computers to your network
- Enable Power Management in Windows 7 and Windows Vista
- View notification settings
- Purchase additional client access licenses
- Refresh this view

9. Restart the secondary server to refresh its Group Policy settings.

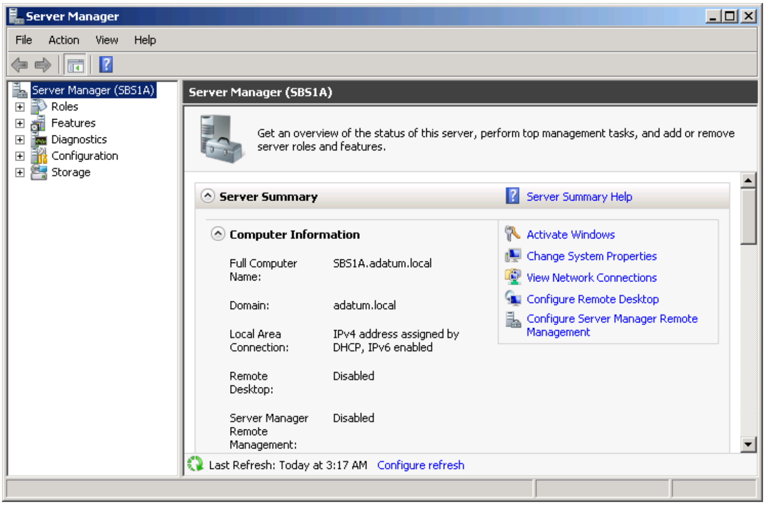
Deploying a Second Domain Controller

As mentioned earlier, the Windows SBS 2011 license terms do not allow you to use your secondary server to create another AD DS domain, whether in the same forest or in a different one. You can, however, configure it to function as a second domain controller in your existing Windows SBS 2011 domain. A second domain controller provides redundancy for times when your primary server is offline, and if your organization has a branch office at a remote location, a second domain controller provides users at that location with local access to AD DS services.

> ***TIP*** **If you are installing a domain controller that you will be moving to another location later, you should use an IP address on the local network for this procedure. Just before you shut down the computer prior to moving it, change the network settings to an IP address on the network that will be the server's final destination.**

Promoting a server to a domain controller is a two-stage process. First, you must install the AD DS role and then you must run the Active Directory Domain Services Installation Wizard. To configure your secondary server to function as a domain controller, use the following procedure:

1. Log on to your Windows SBS 2011 secondary server using a domain account with network Administrator privileges.
2. Click *Start*. Then click *Administrative Tools, Server Manager*. The Server Manager Console appears.



Server Manager (SBS1A)

Get an overview of the status of this server, perform top management tasks, and add or remove server roles and features.

Server Summary

Computer Information

Full Computer Name: SBS1A.adatum.local

Domain: adatum.local

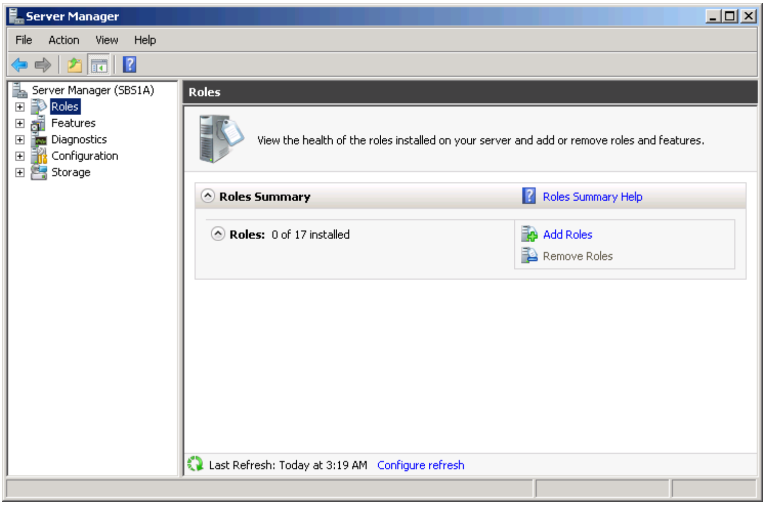
Local Area Connection: IPv4 address assigned by DHCP, IPv6 enabled

Remote Desktop: Disabled

Server Manager Remote Management: Disabled

Last Refresh: Today at 3:17 AM

3. In the Scope (left) pane, select the *Roles* node.



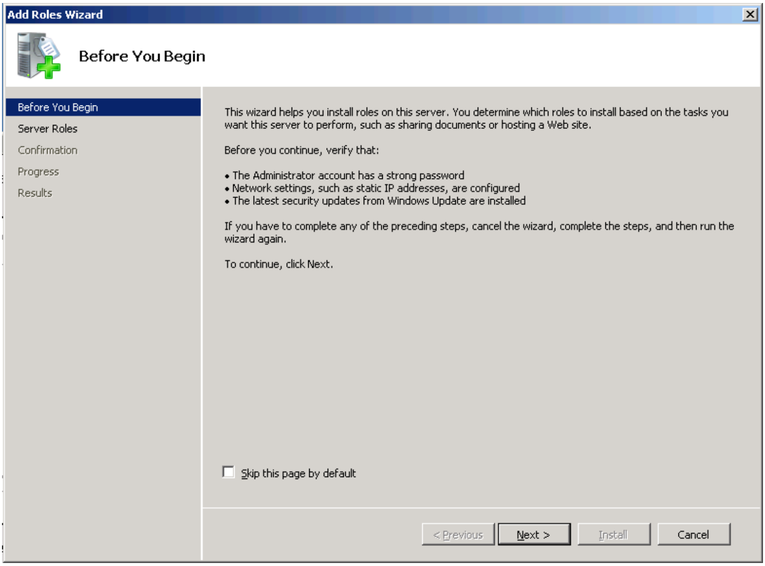
View the health of the roles installed on your server and add or remove roles and features.

Roles Summary

Roles: 0 of 17 installed

Last Refresh: Today at 3:19 AM

4. Click *Add roles*. The Add Roles Wizard appears.



This wizard helps you install roles on this server. You determine which roles to install based on the tasks you want this server to perform, such as sharing documents or hosting a Web site.

Before you continue, verify that:

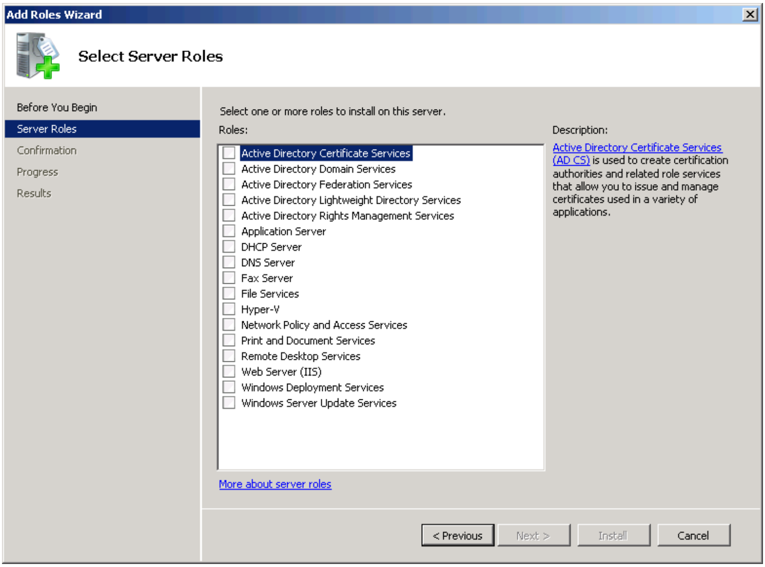
- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The latest security updates from Windows Update are installed

If you have to complete any of the preceding steps, cancel the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

□ Skip this page by default

5. Click *Next* to bypass the Before You Begin page. The Select Server Roles page appears.



Select Server Roles

Select one or more roles to install on this server.

Roles:

- □ Active Directory Certificate Services
- □ Active Directory Domain Services
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Application Server
- □ DHCP Server
- □ DNS Server
- □ Fax Server
- □ File Services
- □ Hyper-V
- □ Network Policy and Access Services
- □ Print and Document Services
- □ Remote Desktop Services
- □ Web Server (IIS)
- □ Windows Deployment Services
- □ Windows Server Update Services

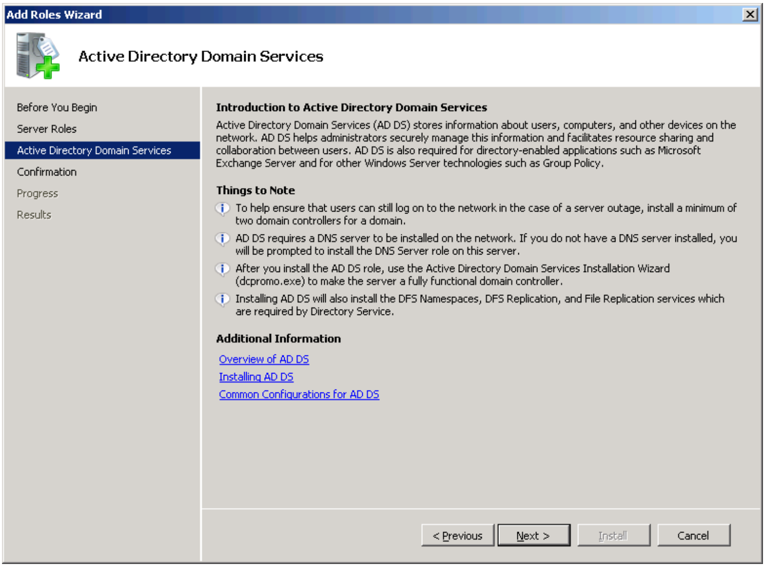
Description:

Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.

More about server roles

6. Select the *Active Directory Domain Services* check box. The Add Features Required For Active Directory Domain Services? dialog box appears.

7. Click *Add required features*, and then click *Next*. The Active Directory Domain Services page appears.



Active Directory Domain Services

Introduction to Active Directory Domain Services

Active Directory Domain Services (AD DS) stores information about users, computers, and other devices on the network. AD DS helps administrators securely manage this information and facilitates resource sharing and collaboration between users. AD DS is also required for directory-enabled applications such as Microsoft Exchange Server and for other Windows Server technologies such as Group Policy.

Things to Note

- ⓘ To help ensure that users can still log on to the network in the case of a server outage, install a minimum of two domain controllers for a domain.
- ⓘ AD DS requires a DNS server to be installed on the network. If you do not have a DNS server installed, you will be prompted to install the DNS Server role on this server.
- ⓘ After you install the AD DS role, use the Active Directory Domain Services Installation Wizard (dcpromo.exe) to make the server a fully functional domain controller.
- ⓘ Installing AD DS will also install the DFS Namespaces, DFS Replication, and File Replication services which are required by Directory Service.

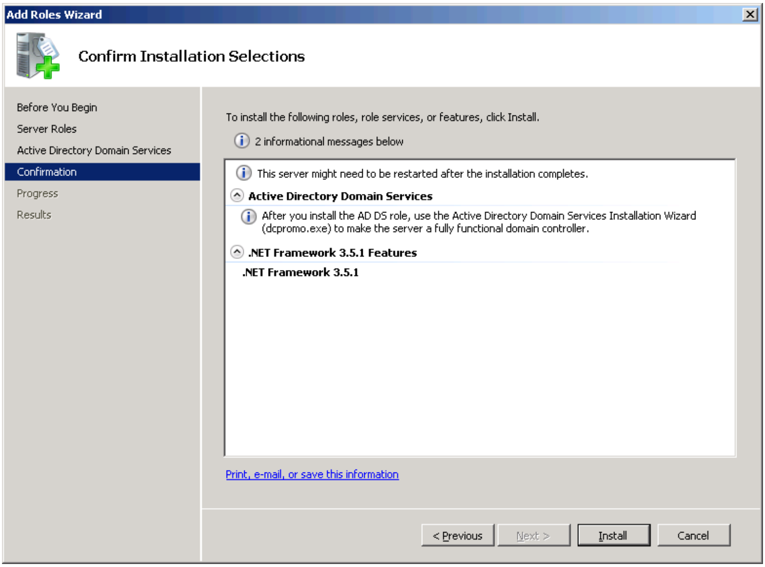
Additional Information

Overview of AD DS

Installing AD DS

Common Configurations for AD DS

8. Click *Next* to continue. The Confirm Installation Selections page appears.



Add Roles Wizard

Confirm Installation Selections

Before You Begin
Server Roles
Active Directory Domain Services
Confirmation
Progress
Results

To install the following roles, role services, or features, click Install.

ⓘ 2 informational messages below

ⓘ This server might need to be restarted after the installation completes.

Active Directory Domain Services

ⓘ After you install the AD DS role, use the Active Directory Domain Services Installation Wizard (dcpromo.exe) to make the server a fully functional domain controller.

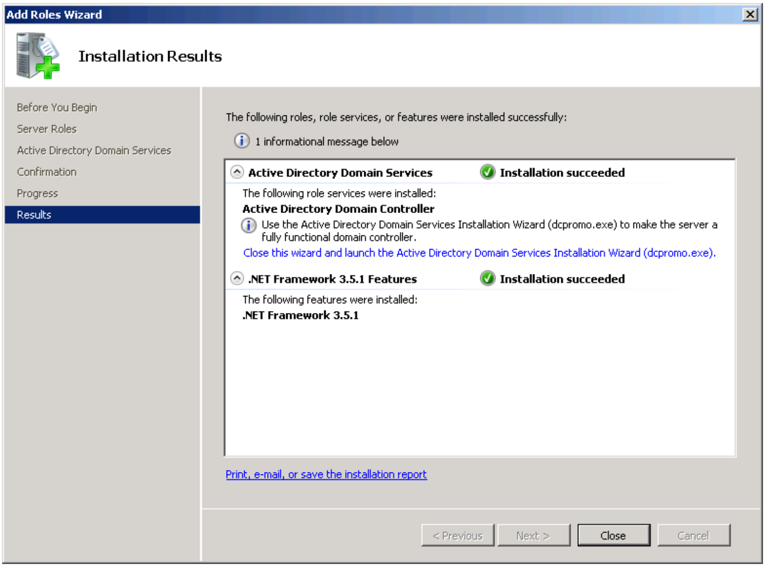
.NET Framework 3.5.1 Features

.NET Framework 3.5.1

Print, e-mail, or save this information

< Previous | Next > | Install | Cancel

9. Click *Install*. The wizard installs the role and the Installation Results page appears.



Add Roles Wizard

Installation Results

Before You Begin
Server Roles
Active Directory Domain Services
Confirmation
Progress
Results

The following roles, role services, or features were installed successfully:

ⓘ 1 informational message below

Active Directory Domain Services ✓ **Installation succeeded**

The following role services were installed:
Active Directory Domain Controller

ⓘ Use the Active Directory Domain Services Installation Wizard (dcpromo.exe) to make the server a fully functional domain controller.

Close this wizard and launch the Active Directory Domain Services Installation Wizard (dcpromo.exe).

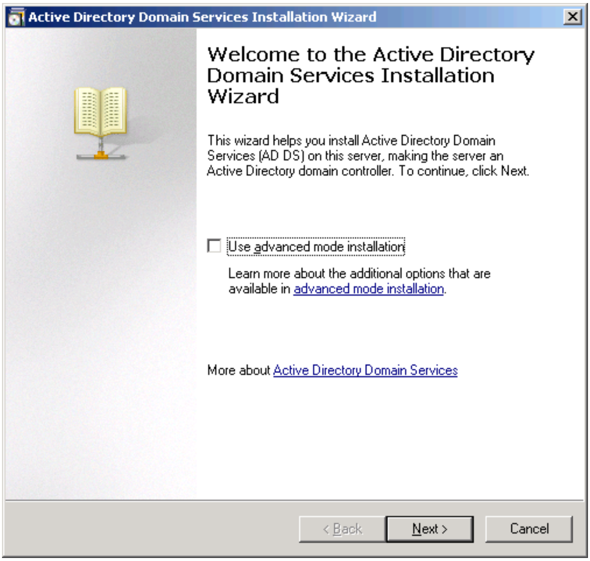
.NET Framework 3.5.1 Features ✓ **Installation succeeded**

The following features were installed:
.NET Framework 3.5.1

Print, e-mail, or save the installation report

< Previous | Next > | Close | Cancel

10. Click the *Close this wizard and launch the Active Directory Domain Services Installation Wizard (Dcpromo.exe)* link. The Active Directory Domain Services Installation Wizard appears.



Active Directory Domain Services Installation Wizard

Welcome to the Active Directory Domain Services Installation Wizard

This wizard helps you install Active Directory Domain Services (AD DS) on this server, making the server an Active Directory domain controller. To continue, click Next.

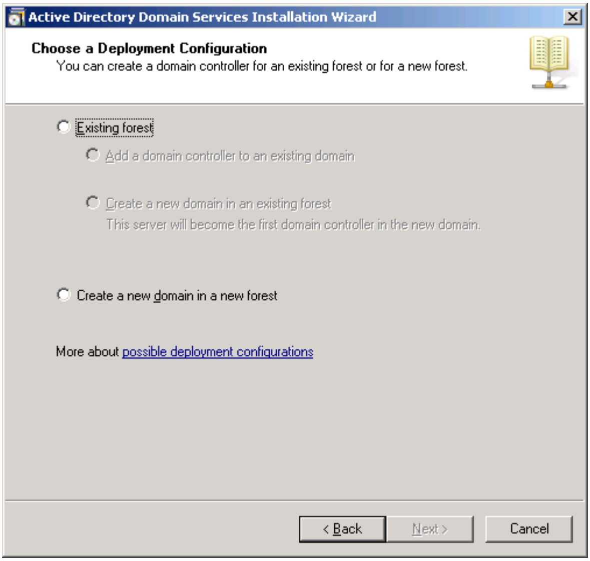
□ Use advanced mode installation

Learn more about the additional options that are available in advanced mode installation.

More about Active Directory Domain Services

11. Click *Next* to bypass the Welcome page. The Operating System Compatibility page appears.

12. Click *Next*. The Choose A Deployment Configuration page appears.



Active Directory Domain Services Installation Wizard

Choose a Deployment Configuration

You can create a domain controller for an existing forest or for a new forest.

○ Existing forest

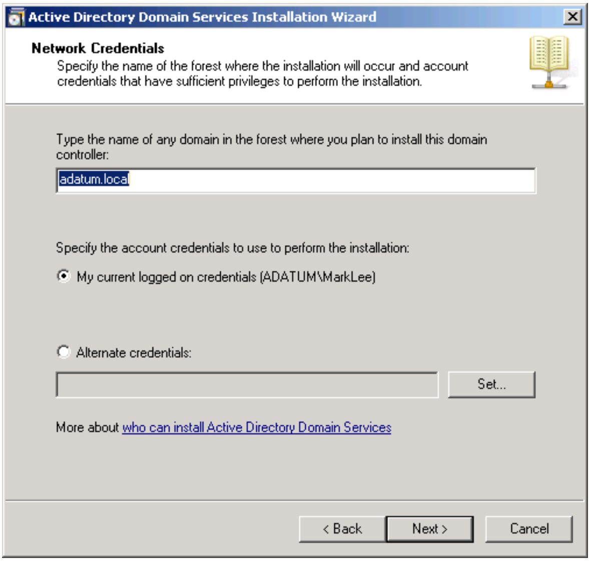
○ Add a domain controller to an existing domain

○ Create a new domain in an existing forest
This server will become the first domain controller in the new domain.

○ Create a new domain in a new forest

More about possible deployment configurations

13. Select the *Existing forest* option, and then leave the *Add a domain controller to an existing domain* option selected and click *Next*. The Network Credentials page appears.



Active Directory Domain Services Installation Wizard

Network Credentials

Specify the name of the forest where the installation will occur and account credentials that have sufficient privileges to perform the installation.

Type the name of any domain in the forest where you plan to install this domain controller:

adatum.local

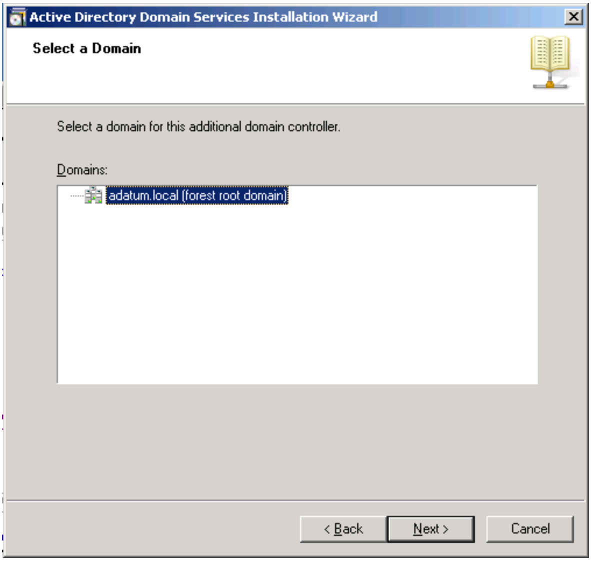
Specify the account credentials to use to perform the installation:

● My current logged on credentials (ADATUM\MarkLee)

○ Alternate credentials:

More about who can install Active Directory Domain Services

14. Make sure that the full name of your AD DS domain appears in the *Type the name of any domain in the forest where you plan to install this domain controller* text box and click *Next*. The Select A Domain page appears.



Active Directory Domain Services Installation Wizard

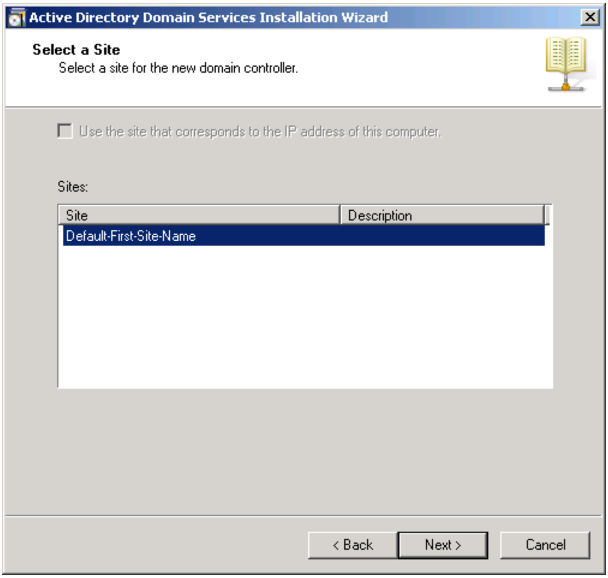
Select a Domain

Select a domain for this additional domain controller.

Domains:

adatum.local (forest root domain)

15. Click *Next* to accept the default forest root domain. The Select A Site page appears.



Active Directory Domain Services Installation Wizard

Select a Site

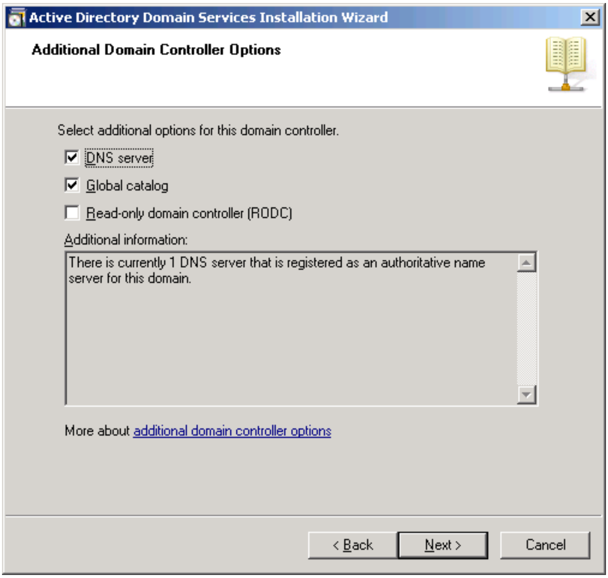
Select a site for the new domain controller.

□ Use the site that corresponds to the IP address of this computer.

Sites:

Site	Description
Default-First-Site-Name	

16. Click *Next* to accept the *Default-first-site-name* site. The Additional Domain Controller Options page appears.



Active Directory Domain Services Installation Wizard

Additional Domain Controller Options

Select additional options for this domain controller.

☑ DNS server

☑ Global catalog

□ Read-only domain controller (RODC)

Additional information:

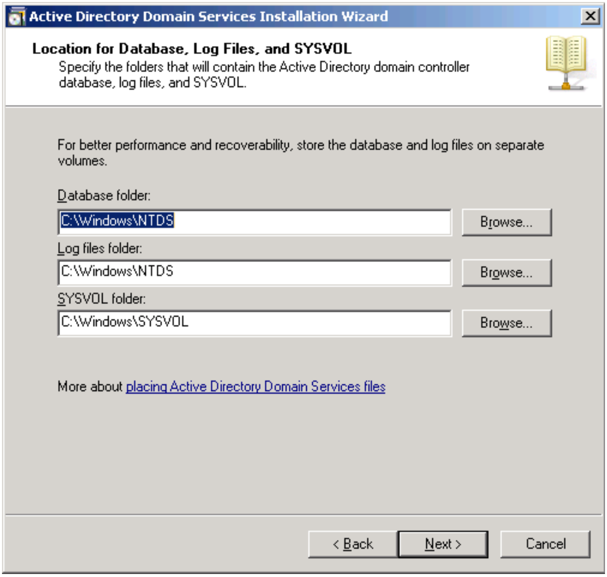
There is currently 1 DNS server that is registered as an authoritative name server for this domain.

More about additional domain controller options

17. Click *Next* to accept the default settings. A Static Ip Address Assignment message box appears, warning you that the computer has a dynamically assigned IP address.

NOTE If you have already configured your server to use a static IP address, as described in the section entitled "Configuring Network Settings," earlier in this chapter, this message refers to the computer's IPv6 address, which you can safely leave as a dynamically assigned address.

18. Click *Yes, the computer will use a dynamically assigned IP address (not recommended)*. An Active Directory Domain Services Installation Wizard message box appears, advising you to create a delegation to the DNS server in the parent zone.
19. Click *Yes*. The Location For Database, Log Files, And SYSVOL page appears.



Location for Database, Log Files, and SYSVOL

Specify the folders that will contain the Active Directory domain controller database, log files, and SYSVOL.

For better performance and recoverability, store the database and log files on separate volumes.

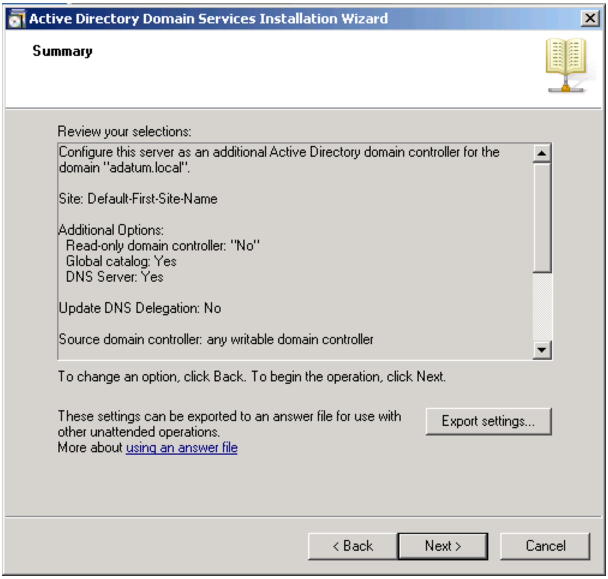
Database folder: C:\Windows\NTDS

Log files folder: C:\Windows\NTDS

SYSVOL folder: C:\Windows\SYSVOL

More about placing Active Directory Domain Services files

20. Click *Next* to accept the default values. The Directory Services Restore Mode Administrator Password page appears.
21. In the *Password* and *Confirm password* text boxes, type the password you want to use when starting the computer in Directory Services Restore Mode and click *Next*. The Summary page appears.



Summary

Review your selections:

Configure this server as an additional Active Directory domain controller for the domain "adatum.local".

Site: Default-First-Site-Name

Additional Options:
  Read-only domain controller: "No"
  Global catalog: Yes
  DNS Server: Yes

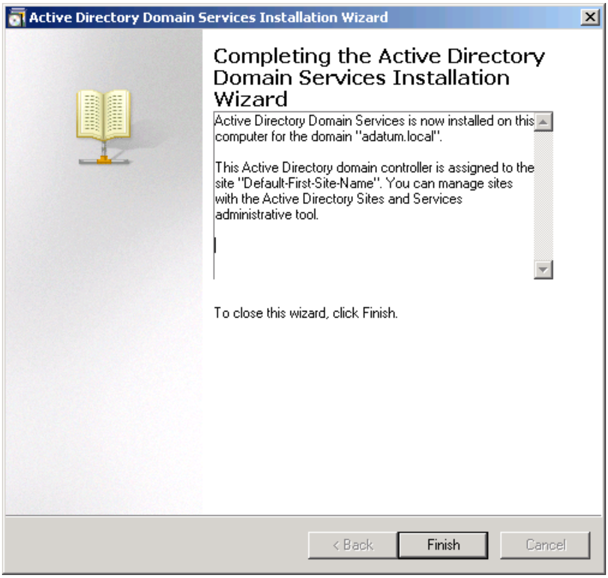
Update DNS Delegation: No

Source domain controller: any writable domain controller

To change an option, click Back. To begin the operation, click Next.

These settings can be exported to an answer file for use with other unattended operations.
More about using an answer file

22. Click *Next*. The wizard configures the server to function as a domain controller, and the Completing The Active Directory Domain Services Installation Wizard page appears.



Completing the Active Directory Domain Services Installation Wizard

Active Directory Domain Services is now installed on this computer for the domain "adatum.local".

This Active Directory domain controller is assigned to the site "Default-First-Site-Name". You can manage sites with the Active Directory Sites and Services administrative tool.

To close this wizard, click Finish.

23. Click *Finish*. An Active Directory Domain Services Installation Wizard message box appears, prompting you to restart the computer.

24. Click *Restart now*. The computer restarts.

Deploying SQL Server 2008 R2 for Small Business

The Windows SBS 2011 Premium Add-on includes SQL Server 2008 R2 for Small Business, a database management application that enables you to run a variety of LOB applications on your secondary server. The Windows SBS 2011 package includes SQL Server on a separate disk, which you must install manually. SQL Server is not a self-contained application; instead, it is an environment that enables applications to store information in and retrieve information from SQL databases. How you install and configure SQL Server on your secondary server depends completely on the applications you plan to run.

Selecting Applications

There are two basic ways to obtain an application that uses SQL Server databases: You can purchase a product that already exists, or you can work with a developer to create a custom application for your business. SQL-based applications are available for many vertical markets, including packages designed to manage professional offices, such as medical practices and legal firms, as well as utilities that can be valuable to any business, such as time-clock and payroll software.

Purchasing an application of this type is not the same as going to the computer store and selecting a commercial software product off the shelf. In most cases, you are dealing with a vendor that has designed and developed applications for specific markets or that is prepared to custom-design an application to your needs. In either situation, your relationship with the vendor is probably more personal, and you should plan to pay more for that privilege. Retail software prices are based on the product's attraction to a large market. A large company that creates a word processor program that appeals to millions of users can afford to sell it for far less than a company that creates a semicustomized application for a niche market with only hundreds or thousands of potential customers.

Selecting a SQL application for your business, or having one developed, is a major part of your network planning process. The requirements of the application dictate what hardware you need in your secondary server and how you install SQL Server 2008 R2 on the computer. The application selection process should include the following elements:

- Meetings with your staff, including department managers or supervisors, as well as key employees that actually will be using the product. Use these meetings to compile a list of features that your application must have and a wish list of features you would like to have.

- Discussions with multiple vendors of software solutions appropriate for your organization. In addition to gathering product collateral and other information about the software, try to ascertain what kind of support the vendor supplies and how they respond to requests for new features and custom software modifications.
- Detailed system requirements for the software products you are considering. Determine whether you can run each product on your version of SQL Server 2008 R2 and whether your budget can support the purchase of the required hardware.
- Live demonstrations of the applications, if possible, attended by the managers and users with whom you developed your list of requirements.
- Communications with other users of each software package you are considering to determine whether they are satisfied with the product and with the vendor's service.

Determining SQL Server Requirements

Hardware requirements for SQL-based applications often go far beyond just a specific processor and a certain amount of memory. Many applications base their hardware requirements on the number of users that access the application or on the size of the database. For example, as you add more users, you might need a faster processor, additional memory, and more disk space.

Some applications also have specific requirements for the computer's storage subsystem. For example, an application might require a certain RAID configuration or specify that you place the database files on drives that are separate from the database log files and the system files.

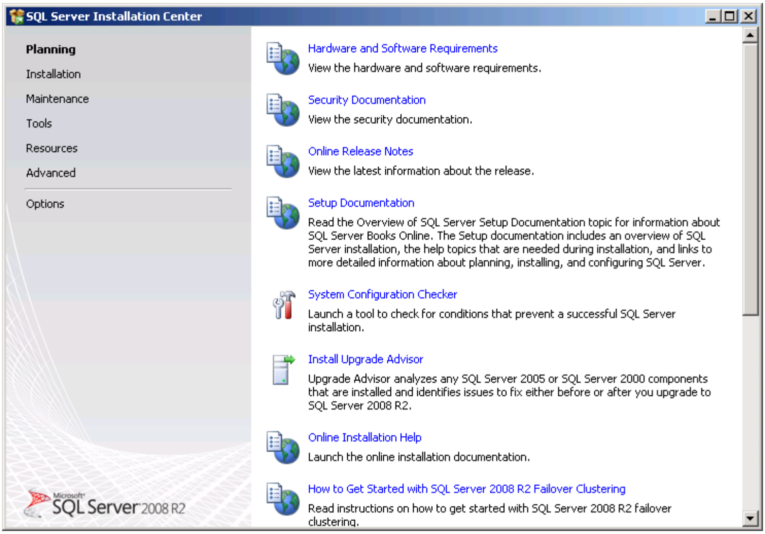
Finally, applications might also call for the installation of certain SQL Server features and specify configuration settings for certain parameters. Obviously, requirements like these can affect not only your server hardware purchasing decisions but also the process of installing and configuring SQL Server 2008 R2.

Installing SQL Server 2008 R2

Although the requirements of your selected applications might require special handling, a typical example of a basic SQL Server 2008 R2 installation proceeds as follows:

1. Log on to your secondary server using a domain account with network Administrator privileges.

2. Insert your SQL Server 2008 R2 for Small Business disk into the DVD-ROM drive and run the Setup.exe file on the disk when the system prompts you to do so. When the User Account Control dialog box appears, click *Continue*. The SQL Server Installation Center window appears.



Hardware and Software Requirements
View the hardware and software requirements.

Security Documentation
View the security documentation.

Online Release Notes
View the latest information about the release.

Setup Documentation
Read the Overview of SQL Server Setup Documentation topic for information about SQL Server Books Online. The Setup documentation includes an overview of SQL Server installation, the help topics that are needed during installation, and links to more detailed information about planning, installing, and configuring SQL Server.

System Configuration Checker
Launch a tool to check for conditions that prevent a successful SQL Server installation.

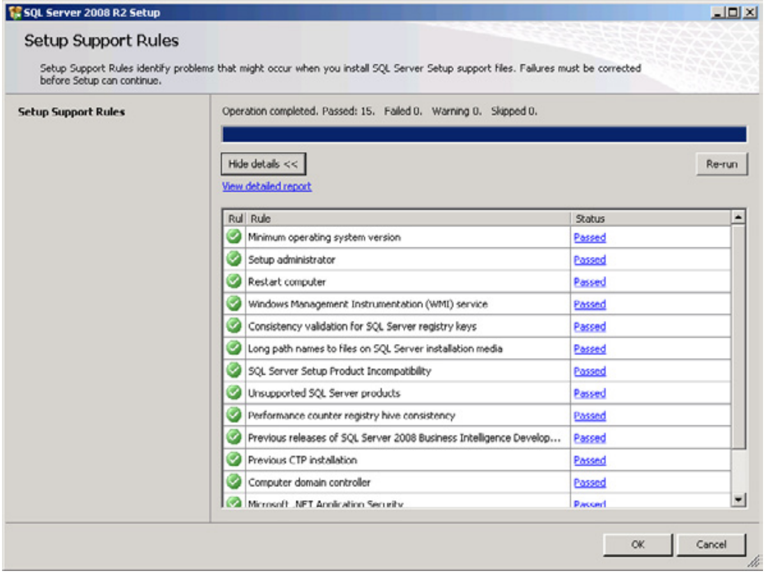
Install Upgrade Advisor
Upgrade Advisor analyzes any SQL Server 2005 or SQL Server 2000 components that are installed and identifies issues to fix either before or after you upgrade to SQL Server 2008 R2.

Online Installation Help
Launch the online installation documentation.

How to Get Started with SQL Server 2008 R2 Failover Clustering
Read instructions on how to get started with SQL Server 2008 R2 failover clustering.

NOTE **If your server does not have the latest versions of Microsoft .NET Framework and Windows Installer installed, the setup program offers to install them for you. This process takes several minutes and requires you to restart the computer. After the computer restarts, run the Setup.exe program on the SQL Server 2008 R2 disk again.**

3. Click *System configuration checker*. The program checks 14 elements to determine whether your server is ready to install SQL Server and then displays a Setup Support Rules dialog box containing the results.



SQL Server 2008 R2 Setup

Setup Support Rules

Setup Support Rules identify problems that might occur when you install SQL Server Setup support files. Failures must be corrected before Setup can continue.

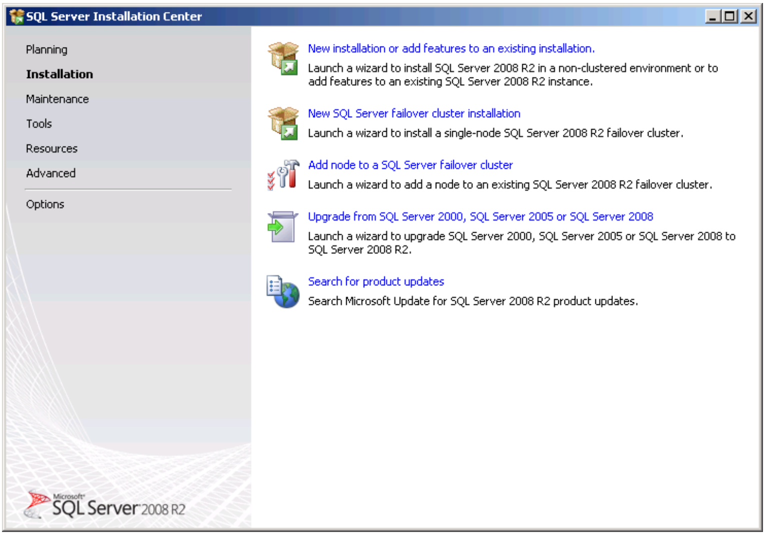
Setup Support Rules

Operation completed. Passed: 15. Failed 0. Warning 0. Skipped 0.

Rul	Rule	Status
✓	Minimum operating system version	Passed
✓	Setup administrator	Passed
✓	Restart computer	Passed
✓	Windows Management Instrumentation (WMI) service	Passed
✓	Consistency validation for SQL Server registry keys	Passed
✓	Long path names to files on SQL Server installation media	Passed
✓	SQL Server Setup Product Incompatibility	Passed
✓	Unsupported SQL Server products	Passed
✓	Performance counter registry hive consistency	Passed
✓	Previous releases of SQL Server 2008 Business Intelligence Develop...	Passed
✓	Previous CTP installation	Passed
✓	Computer domain controller	Passed
✓	Microsoft .NET Application Security	Passed

If your system fails to pass any of the tests, correct the problem and rerun the *System configuration checker.*

4. Once the system has passed all the tests, click *OK* to return to the SQL Server Installation Center window.
5. In the left column, click *Installation*. The Installation page of the SQL Server Installation Center appears.



SQL Server Installation Center

New installation or add features to an existing installation.
Launch a wizard to install SQL Server 2008 R2 in a non-clustered environment or to add features to an existing SQL Server 2008 R2 instance.

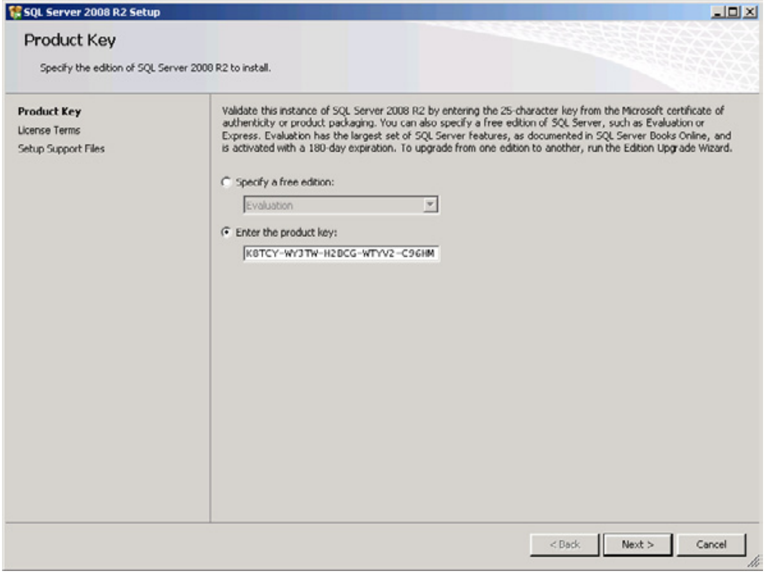
New SQL Server failover cluster installation
Launch a wizard to install a single-node SQL Server 2008 R2 failover cluster.

Add node to a SQL Server failover cluster
Launch a wizard to add a node to an existing SQL Server 2008 R2 failover cluster.

Upgrade from SQL Server 2000, SQL Server 2005 or SQL Server 2008
Launch a wizard to upgrade SQL Server 2000, SQL Server 2005 or SQL Server 2008 to SQL Server 2008 R2.

Search for product updates
Search Microsoft Update for SQL Server 2008 R2 product updates.

6. Click *New installation or add features to an existing installation*. The SQL Server 2008 Setup Wizard appears and displays the Setup Support Rules dialog box again, this time checking seven elements that are required before the installation can proceed.
7. If your system passes all seven tests, click *OK*. If not, correct the problems indicated and click *Re-Run* until the system passes all seven tests. Then click *OK*. The Product Key page appears.



SQL Server 2008 R2 Setup

Product Key

Specify the edition of SQL Server 2008 R2 to install.

Validate this instance of SQL Server 2008 R2 by entering the 25-character key from the Microsoft certificate of authenticity or product packaging. You can also specify a free edition of SQL Server, such as Evaluation or Express. Evaluation has the largest set of SQL Server features, as documented in SQL Server Books Online, and is activated with a 180-day expiration. To upgrade from one edition to another, run the Edition Upgrade Wizard.

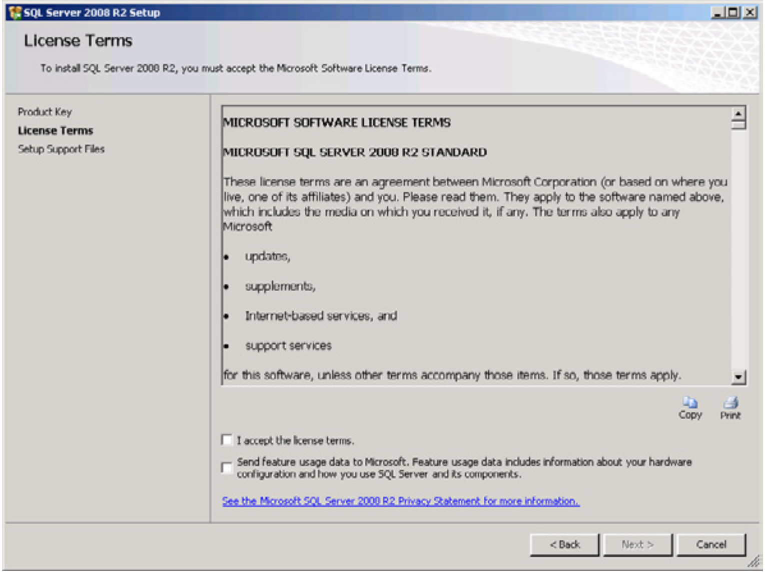
○ Specify a free edition:

Evaluation

● Enter the product key:

K8TCY-WYJTW-H2BCG-WTYV2-C96HM

8. Click the *Enter the product key* option and type the SQL Server 2008 product key supplied with your Windows SBS 2011 package.
9. Click *Next*. The License Terms page appears.



License Terms

To install SQL Server 2008 R2, you must accept the Microsoft Software License Terms.

MICROSOFT SOFTWARE LICENSE TERMS

MICROSOFT SQL SERVER 2008 R2 STANDARD

These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to the software named above, which includes the media on which you received it, if any. The terms also apply to any Microsoft

- updates,
- supplements,
- Internet-based services, and
- support services

for this software, unless other terms accompany those items. If so, those terms apply.

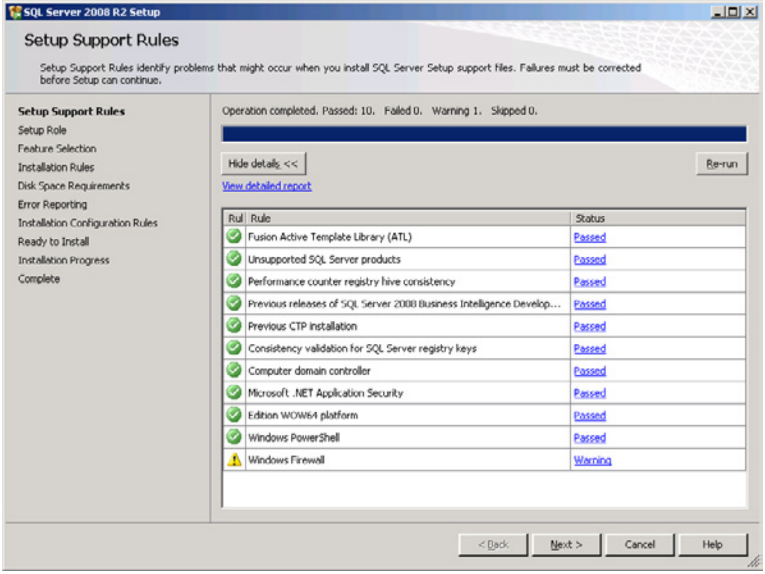
□ I accept the license terms.

□ Send feature usage data to Microsoft. Feature usage data includes information about your hardware configuration and how you use SQL Server and its components.

See the Microsoft SQL Server 2008 R2 Privacy Statement for more information.

10. Select the *I accept the license terms* check box and click *Next*. The Setup Support Files page appears.

11. Click *Install* to continue. The wizard installs the setup support files and displays the Setup Support Rules page, which contains the results of the installation.



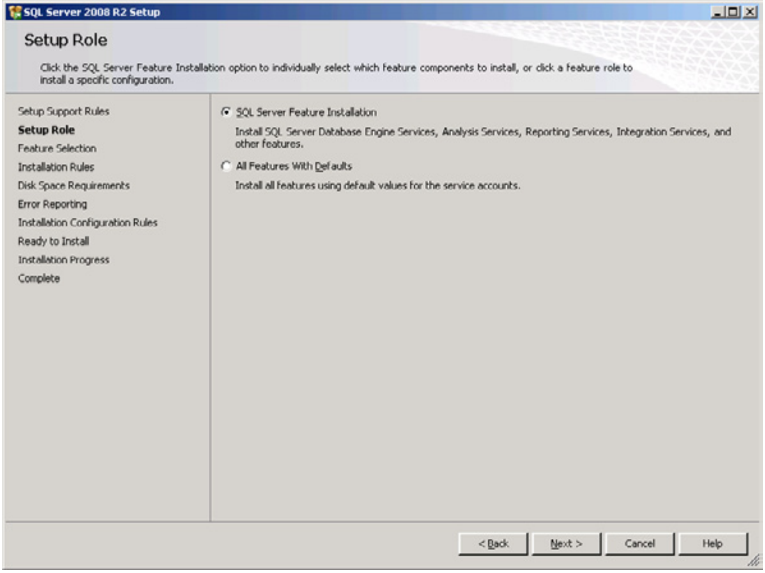
Setup Support Rules

Setup Support Rules identify problems that might occur when you install SQL Server Setup support files. Failures must be corrected before Setup can continue.

Operation completed. Passed: 10. Failed 0. Warning 1. Skipped 0.

Rul	Rule	Status
✓	Fusion Active Template Library (ATL)	Passed
✓	Unsupported SQL Server products	Passed
✓	Performance counter registry hive consistency	Passed
✓	Previous releases of SQL Server 2008 Business Intelligence Develop...	Passed
✓	Previous CTP installation	Passed
✓	Consistency validation for SQL Server registry keys	Passed
✓	Computer domain controller	Passed
✓	Microsoft .NET Application Security	Passed
✓	Edition WOW64 platform	Passed
✓	Windows PowerShell	Passed
⚠	Windows Firewall	Warning

12. Click *Next*. The Setup Role page appears.



Setup Role

Click the SQL Server Feature Installation option to individually select which feature components to install, or click a feature role to install a specific configuration.

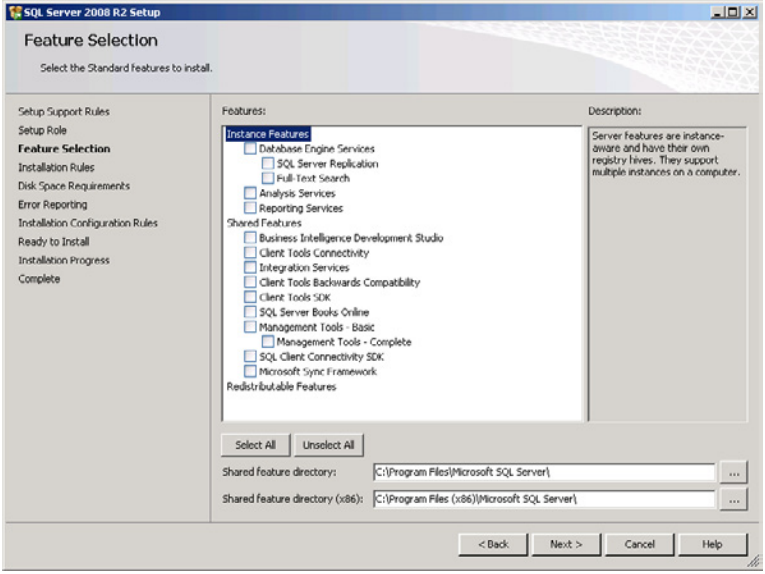
● SQL Server Feature Installation

Install SQL Server Database Engine Services, Analysis Services, Reporting Services, Integration Services, and other features.

○ All Features With Defaults

Install all features using default values for the service accounts.

13. Click *Next* to accept the default setting. The Feature Selection page appears.



Feature Selection

Select the Standard features to install.

Features:

Instance Features
- □ Database Engine Services
  - □ SQL Server Replication
  - □ Full-Text Search
- □ Analysis Services
- □ Reporting Services

Shared Features
- □ Business Intelligence Development Studio
- □ Client Tools Connectivity
- □ Integration Services
- □ Client Tools Backwards Compatibility
- □ Client Tools SDK
- □ SQL Server Books Online
- □ Management Tools - Basic
  - □ Management Tools - Complete
- □ SQL Client Connectivity SDK
- □ Microsoft Sync Framework

Redistributable Features

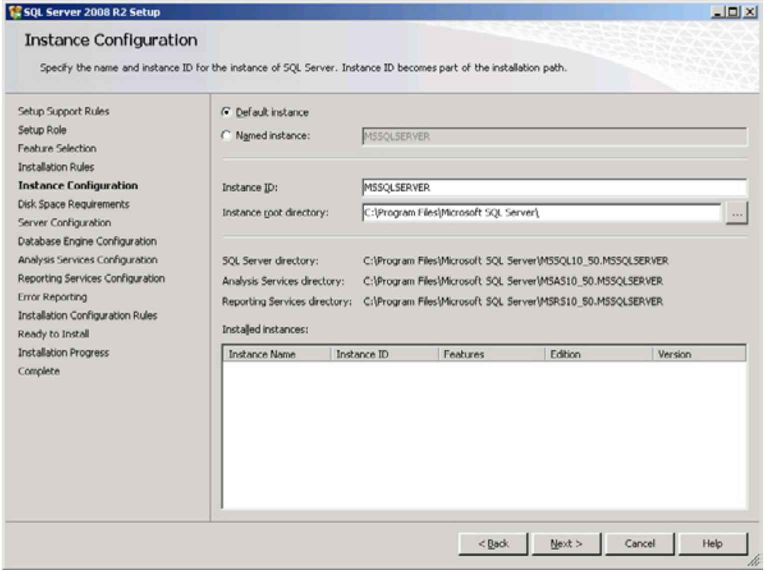
Description:

Server features are instance-aware and have their own registry hives. They support multiple instances on a computer.

Shared feature directory: C:\Program Files\Microsoft SQL Server\

Shared feature directory (x86): C:\Program Files (x86)\Microsoft SQL Server\

14. Select the check boxes for the following components:
    - *Database engine services*
    - *Analysis services*
    - *Reporting services*
    - *Management tools—Basic*
15. Click *Next*. The Installation Rules page appears.
16. If your installation passes all the required rules, click *Next* to proceed. The Instance Configuration page appears.



Instance Configuration

Specify the name and instance ID for the instance of SQL Server. Instance ID becomes part of the installation path.

● Default instance

○ Named instance: MSSQLSERVER

Instance ID: MSSQLSERVER

Instance root directory: C:\Program Files\Microsoft SQL Server\

SQL Server directory: C:\Program Files\Microsoft SQL Server\MSSQL10_50.MSSQLSERVER

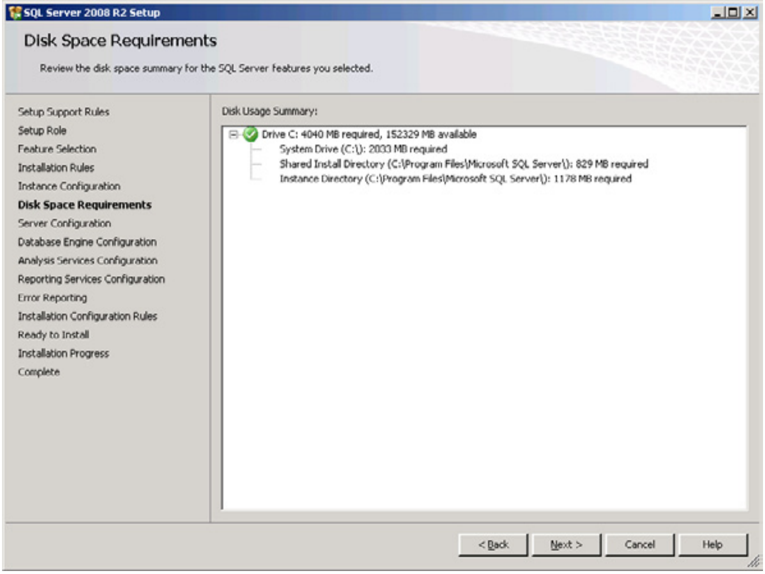
Analysis Services directory: C:\Program Files\Microsoft SQL Server\MSAS10_50.MSSQLSERVER

Reporting Services directory: C:\Program Files\Microsoft SQL Server\MSRS10_50.MSSQLSERVER

Installed instances:

Instance Name	Instance ID	Features	Edition	Version

17. Click *Next* to accept the default settings. The Disk Space Requirements page appears.



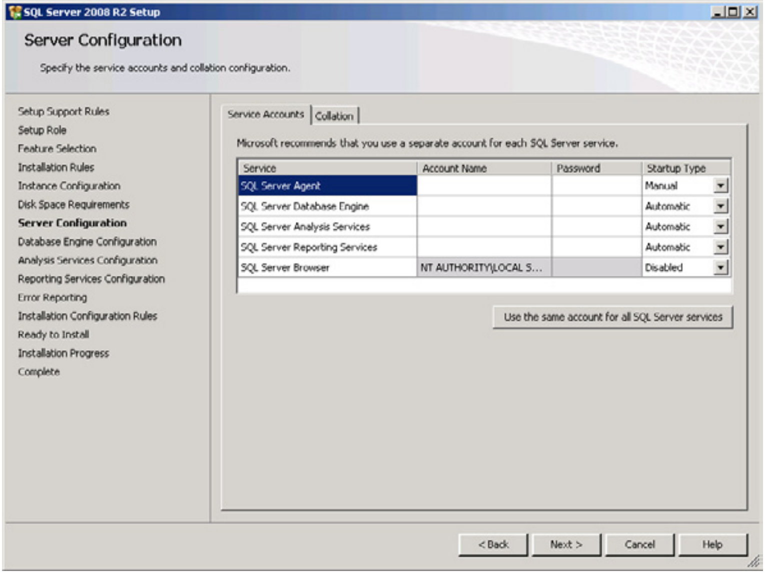
Disk Space Requirements

Review the disk space summary for the SQL Server features you selected.

Disk Usage Summary:

```
Drive C: 4040 MB required, 152329 MB available
    System Drive (C:\): 2033 MB required
    Shared Install Directory (C:\Program Files\Microsoft SQL Server\): 829 MB required
    Instance Directory (C:\Program Files\Microsoft SQL Server\): 1178 MB required
```

18. Click *Next*. The Server Configuration page appears.



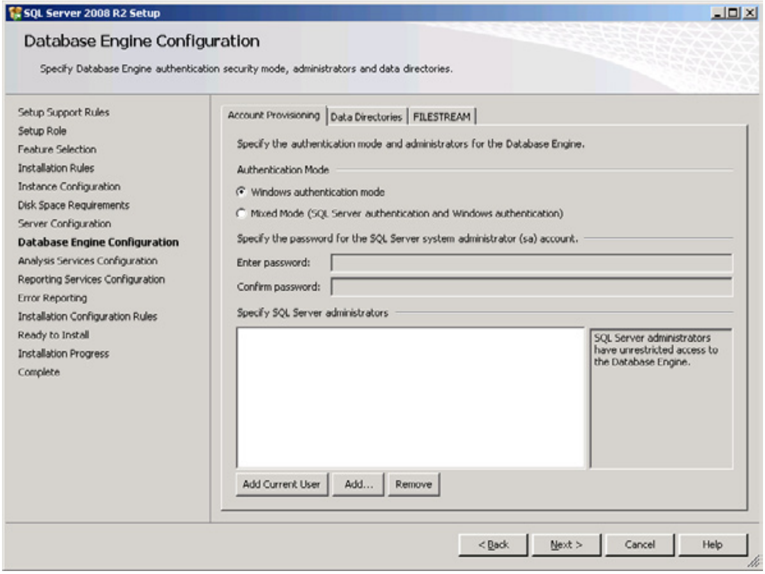
Server Configuration

Specify the service accounts and collation configuration.

Microsoft recommends that you use a separate account for each SQL Server service.

Service	Account Name	Password	Startup Type
SQL Server Agent			Manual
SQL Server Database Engine			Automatic
SQL Server Analysis Services			Automatic
SQL Server Reporting Services			Automatic
SQL Server Browser	NT AUTHORITY\LOCAL S...		Disabled

19. Specify an account name and password for each of the SQL Server services and click *Next*. The Database Engine Configuration page appears.



SQL Server 2008 R2 Setup

Database Engine Configuration

Specify Database Engine authentication security mode, administrators and data directories.

Specify the authentication mode and administrators for the Database Engine.

Authentication Mode

● Windows authentication mode

○ Mixed Mode (SQL Server authentication and Windows authentication)

Specify the password for the SQL Server system administrator (sa) account.

Enter password:

Confirm password:

Specify SQL Server administrators

SQL Server administrators have unrestricted access to the Database Engine.

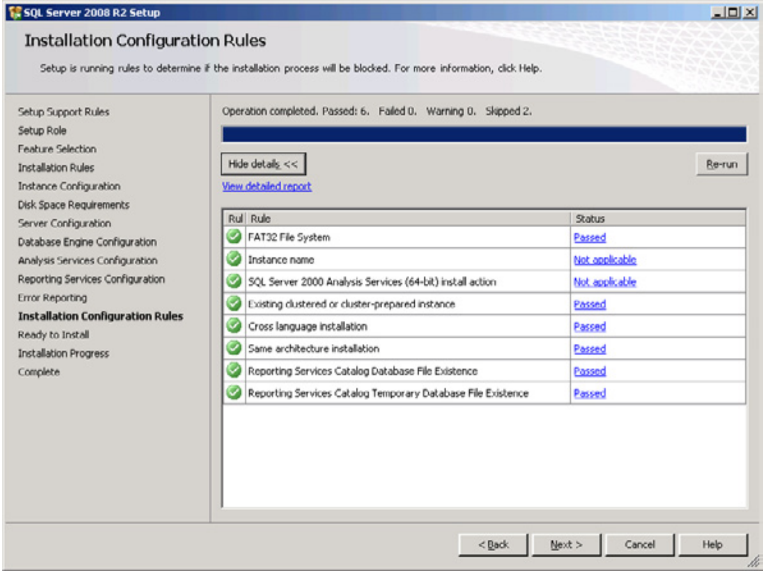
20. Click *Add current user* and then click *Next* to accept the default *Windows authentication mode* option. The Analysis Services Configuration page appears.

21. Click *Add current user* and then click *Next*. The Reporting Services Configuration page appears.

22. Click *Next* to accept the default *Install the native mode default configuration* option. The Error Reporting page appears.

23. Click *Next* to accept the default settings. The Installation Configuration Rules page appears and checks to see whether an installation can proceed based on the settings you supplied.

24. Click *Show details* to display the test results.



SQL Server 2008 R2 Setup

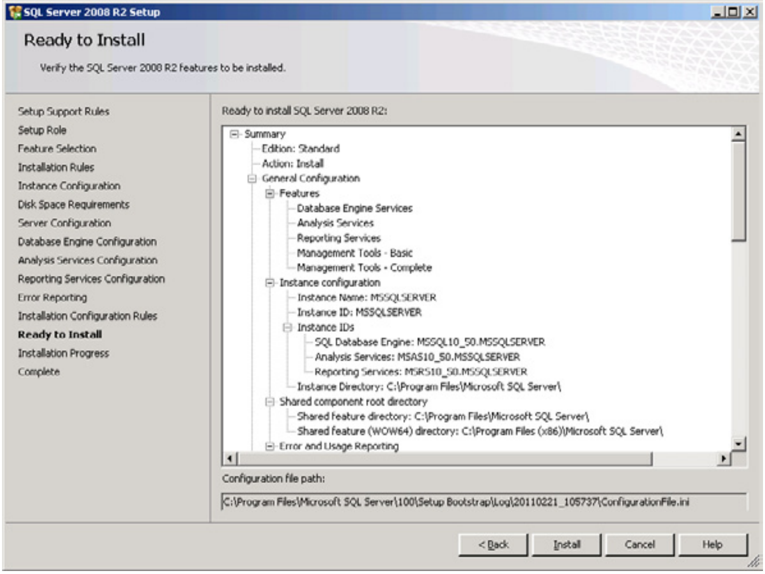
Installation Configuration Rules

Setup is running rules to determine if the installation process will be blocked. For more information, click Help.

Operation completed. Passed: 6. Failed 0. Warning 0. Skipped 2.

Rul	Rule	Status
✓	FAT32 File System	Passed
✓	Instance name	Not applicable
✓	SQL Server 2000 Analysis Services (64-bit) install action	Not applicable
✓	Existing clustered or cluster-prepared instance	Passed
✓	Cross language installation	Passed
✓	Same architecture installation	Passed
✓	Reporting Services Catalog Database File Existence	Passed
✓	Reporting Services Catalog Temporary Database File Existence	Passed

25. Click *Next*. The Ready To Install page appears.



SQL Server 2008 R2 Setup

Ready to Install

Verify the SQL Server 2008 R2 features to be installed.

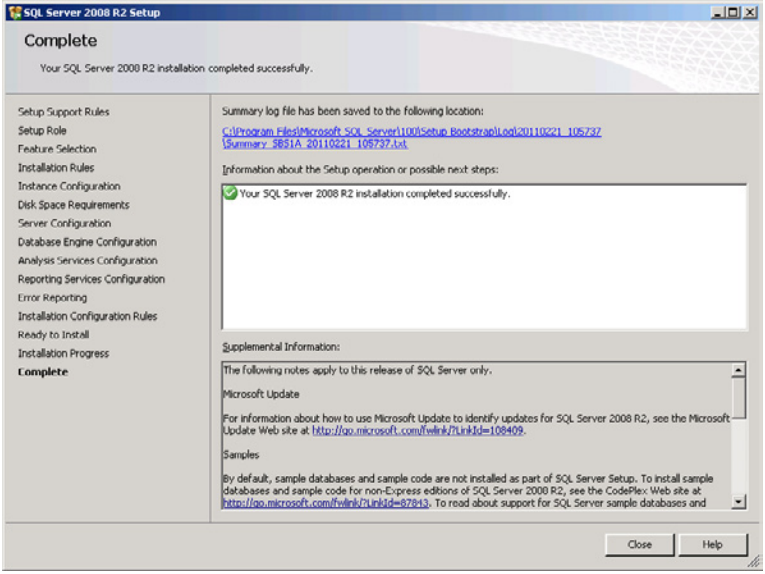
Ready to install SQL Server 2008 R2:

```
⊟ Summary
   Edition: Standard
   Action: Install
 ⊟ General Configuration
   ⊟ Features
       Database Engine Services
       Analysis Services
       Reporting Services
       Management Tools - Basic
       Management Tools - Complete
   ⊟ Instance configuration
       Instance Name: MSSQLSERVER
       Instance ID: MSSQLSERVER
     ⊟ Instance IDs
         SQL Database Engine: MSSQL10_50.MSSQLSERVER
         Analysis Services: MSAS10_50.MSSQLSERVER
         Reporting Services: MSRS10_50.MSSQLSERVER
       Instance Directory: C:\Program Files\Microsoft SQL Server\
   ⊟ Shared component root directory
       Shared feature directory: C:\Program Files\Microsoft SQL Server\
       Shared feature (WOW64) directory: C:\Program Files (x86)\Microsoft SQL Server\
   ⊟ Error and Usage Reporting
```

Configuration file path:

C:\Program Files\Microsoft SQL Server\100\Setup Bootstrap\Log\20110221_105737\ConfigurationFile.ini

26. Click *Install*. The wizard installs SQL Server 2008 R2 and displays the Complete page, showing the overall results of the installation.



Complete

Your SQL Server 2008 R2 installation completed successfully.

Summary log file has been saved to the following location:

C:\Program Files\Microsoft SQL Server\100\Setup Bootstrap\Log\20110221_105737
\Summary_SB51A_20110221_105737.txt

Information about the Setup operation or possible next steps:

✓ Your SQL Server 2008 R2 installation completed successfully.

Supplemental Information:

The following notes apply to this release of SQL Server only.

Microsoft Update

For information about how to use Microsoft Update to identify updates for SQL Server 2008 R2, see the Microsoft Update Web site at http://go.microsoft.com/fwlink/?LinkId=108409.

Samples

By default, sample databases and sample code are not installed as part of SQL Server Setup. To install sample databases and sample code for non-Express editions of SQL Server 2008 R2, see the CodePlex Web site at http://go.microsoft.com/fwlink/?LinkId=87843. To read about support for SQL Server sample databases and

27. Click *Close*. The wizard closes.

Index

About the Author

CRAIG ZACKER is a writer, editor, and educator whose computing experience began in the days of teletypes and paper tape. After making the move from minicomputers to PCs, he worked as a network administrator and PC support technician while operating a freelance desktop publishing business. After earning a Master's degree in English and American Literature from New York University, Craig worked extensively on the integration of Windows operating systems into existing internetworks; supported fleets of Windows workstations; and was employed as a technical writer, content provider, trainer, and webmaster for a large software company. Since devoting himself to writing and editing full time, Craig has authored or contributed to dozens of books on operating systems, networking topics, and PC hardware.

He has also developed educational texts for college courses, created online training courses for the web, and published articles with top industry publications.