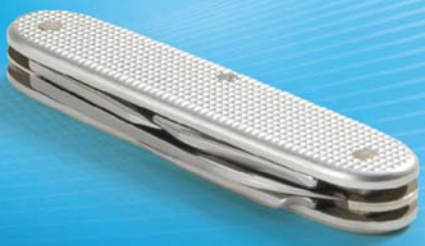
Foreword by Andrew Mason
Principal Program Manager Lead, Windows Server Core

William R. Stanek
Series Editor

Microsoft

Windows Server® 2008 Server Core



Mitch Tulloch, MVP
with the Windows Server Core Team at Microsoft®

Administrator's Pocket Consultant

PUBLISHED BY
Microsoft Press
A Division of Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052-6399

Library of Congress Control Number: 2008935157

Printed and bound in the United States of America.

1 2 3 4 5 6 7 8 9 QWE 3 2 1 0 9 8

Distributed in Canada by H.B. Fenn and Company Ltd.

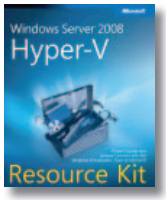
A CIP catalogue record for this book is available from the British Library.

Microsoft Press books are available through booksellers and distributors worldwide. For further information about international editions, contact your local Microsoft Corporation office or contact Microsoft Press International directly at fax (425) 936-7329. Visit our Web site at www.microsoft.com/mspress. Send comments to mspinput@microsoft.com.

Acquisitions Editor: Martin DelRe
Developmental Editor: Karen Szall
Project Editor: Carol Vu
Editorial Production: ICC Macmillan, Inc.
Technical Reviewer: Bob Dean; Technical Review services provided by Content Master, a member of CM Group, Ltd.
Cover: Tom Draper Design

Body Part No. X15-12261

Windows Server 2008—Resources for Administrators



Windows Server® 2008 Hyper-V™ Resource Kit

Robert Larson and Janique Carbone with the Windows Virtualization Team at Microsoft® and Sharon Crawford

ISBN 9780735625174

Windows Server 2008 Administrator's Pocket Consultant

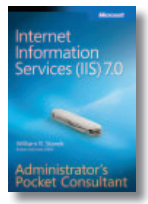
William R. Stanek

ISBN 9780735624375

Windows Server 2008 Terminal Services Resource Kit

Christa Anderson and Kristin L. Griffin with the Microsoft Presentation Hosted Desktop Virtualization Team

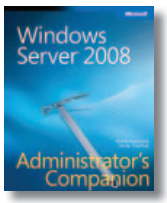
ISBN 9780735625853



Internet Information Services (IIS) 7.0 Administrator's Pocket Consultant

William R. Stanek

ISBN 9780735623644



Windows Server 2008 Administrator's Companion

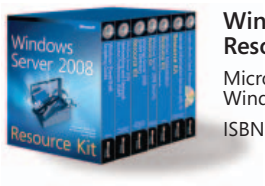
Charlie Russel and Sharon Crawford

ISBN 9780735625051

Internet Information Services (IIS) 7.0 Resource Kit

Volodarsky, Londer, Hill, et al. with the Microsoft IIS Team

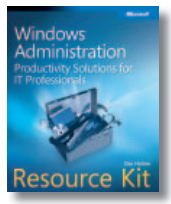
ISBN 9780735624412



Windows Server 2008 Resource Kit

Microsoft MVPs with Microsoft Windows Server Team

ISBN 9780735623613



Windows® Administration Resource Kit: Productivity Solutions for IT Professionals

Dan Holme

ISBN 9780735624313

Windows Server 2008 Security Resource Kit

Jesper M. Joahansson and MVPs with the Microsoft Security Team

ISBN 9780735625044

Microsoft Windows PowerShell Step by Step

Ed Wilson

ISBN 9780735623958

microsoft.com/mspress

Microsoft Press

Contents at a Glance

Table of Contents

Acknowledgments

Huge thanks first of all to Andrew Mason, Principal Program Manager for the Server Core program at Microsoft, for reviewing all my chapters for technical accuracy and for patiently responding to my numerous questions.

Much thanks as well to the following individuals: to my friend and colleague Jason Miller, MVP, who assisted me in developing and testing the Hyper-V content for this book; to James O'Neill, IT Pro Evangelist at Microsoft UK, who reviewed the Hyper-V content and provided helpful advice; and to Bob Dean, the technical reviewer for this project, who went above and beyond the call of duty in helping ensure the content is accurate. Special thanks also to Bill Noonan, Mark Kitris, and the members of the CSS Global Technical Readiness Team (GTR) at Microsoft for the invaluable assistance they provided on this project.

Thanks also to Karen Szall, the development editor at Microsoft Press for this book, and Carol Vu, the project editor at Microsoft Press, both of whom I've enjoyed working with on this project and hope to do so again in the future. Thanks also to Martin DelRe, who first approached me about being involved in this project.

Thanks as well to my friend and agent, Neil Salkind of Salkind Literary Agency, which is part of Studio B Productions, Inc.

And finally, thanks to my wife, Ingrid, for her encouragement and support during this project.

Foreword

By Andrew Mason
Principal Program Manager Lead, Windows Server Core

As Windows Server has continued to evolve, increasing functionality with each release, it became apparent that there was a need for additional deployment flexibility. Windows Server is a general-purpose operating system, but it is frequently deployed to provide a fixed function on a network, such as a DNS Server, File Server, Active Directory Domain Services domain controller, and so on. In these deployments, more functionality than necessary is often installed for a single server role to run, and a common customer request has been to allow the installation of just what is needed. The result of this is the new Server Core installation option in Windows Server 2008.

Server Core is an exciting and big step forward that allows customers more flexibility in how they deploy, manage, maintain, and secure a Windows Server installation. You may have heard that Server Core is a minimal, GUI-less interface, or even that it is a Windows without windows installation of Windows Server. As you will see as you go through this book, Server Core is much more than just the removal of the Windows shell. The way I like to describe Server Core is that it is a slice off the bottom of the operating system, providing a subset of the full functionality. To that end, customers are finding a variety of ways to take advantage of the many benefits Server Core provides. Some of the benefits you will find include a reduction in the number of software updates required to maintain the operating system (OS), a smaller attack surface, its relative simplicity (there's less to configure, so there's less to misconfigure), and the fact that it can be used to extend the life of older hardware.

As you delve into Server Core in this book, you may wonder why some functionality was included while other functionality was left out of Server Core. The best way to explain that in the limited space I have is to state the goal we had in designing Server Core: to provide customers with a minimal installation option that reduces management, maintenance, and the security attack surface while running the network infrastructure server roles and still being manageable with the same set of tools. To achieve this, a lot of time was spent on the management side to ensure Server Core is manageable and fits seamlessly in with the management infrastructures that customers are already using with Windows Server. We included functionalities such as Windows Installer, so that the Microsoft Windows Installer (.msi) packages for management agents can be used to install the agents the same way they are on a full Windows Server installation. However, including functionality in Server Core while trying to maintain these goals is very much a tightrope walk that requires some hard decisions and some omissions until dependencies can be changed.

This book will be an invaluable resource for administrators wanting to understand how to install, configure, and manage a Server Core installation. It is a resource that you can refer to for end-to-end deployments of Server Core, as well as for guidance on using specific server roles and useful tips for working with Server Core.

The Server Core team is very proud of what we were able to accomplish and hope you will take advantage of its benefits in your environment.

Introduction

Welcome to the *Windows Server 2008 Server Core Administrator's Pocket Consultant*. Server Core is a new installation option available for Windows Server 2008 that has a reduced servicing footprint and is designed for running a specific set of server roles for dedicated use. Enterprises have been asking for a book like this for a while, because Server Core can help branch offices, data centers, and other environments significantly reduce the cost involved with deploying and managing servers running Microsoft Windows. I hope you find that this book meets your needs and answers any questions you may have about Server Core; feel free to use my personal contact info found later in this Introduction to send me questions.

Who Is This Book For?

The target audience for the *Windows Server 2008 Server Core Administrator's Pocket Consultant* is administrators and staff of enterprise IT departments who need to learn how to deploy, configure, manage, and maintain Server Core computers in various roles, including domain controllers, infrastructure servers, Web servers, and other supported roles. The book assumes that you have at least a couple of years' experience managing servers running Windows in various roles, that you are familiar with most of the administrative tools used to manage servers running Windows, and that you have at least some experience trying to administer such servers from the command line.

Because most administrators who work with servers running Windows tend to be comfortable using administrative tools like Microsoft Management Console (MMC) consoles for managing their servers, this book focuses to a large extent on showing how you can perform many administrative tasks from the command line. This choice of focus was obvious for two reasons. First, when you log on to Server Core, all you see is a command prompt—there's no desktop! That means no MMC consoles either, but of course, you can use most MMC consoles remotely to manage Server Core from another computer, and that's covered too. But second, I didn't want to reinvent the wheel because über-author William Stanek has already published an excellent book called the *Windows Server 2008 Administrator's Pocket Consultant,* which explains in detail how to use these various MMC consoles to manage different roles and features on servers running Windows Server 2008. The result is that this present book is intended to complement Stanek's book instead of supplant it, and I encourage you to buy both books and use them together as a comprehensive quick reference for administering all aspects of the Windows Server 2008 platform.

How This Book Is Organized

Although this book is intended mainly as a quick lookup reference of how to perform administrative tasks, you can also read the book from cover to cover and gain a good understanding of the capabilities, features, and occasional quirks of Server Core. Whatever way you use it—as a task reference or for learning purposes—you'll benefit from using the most comprehensive resource available on administering Server Core.

The overall flow of this book looks like this:

- Chapter 1 provides a brief introduction to the platform and should be read in its entirety if you are new to Server Core.
- Chapters 2 and 3 cover manual and unattended deployment methods and various post-deployment configuration tasks that you may need to perform.
- Chapter 4 looks at the various roles and features that you can install on Server Core and explains how to deploy them both manually and during unattended installation.
- Chapters 5 and 6 explain the various tools and methods that you can use to administer Server Core, including using the local command line, Remote Desktop, the Windows Remote Shell, MMC consoles, Group Policy, and, to a limited extent, Windows PowerShell.
- Chapters 7 through 12 examine in detail each of the server roles that you can install on Server Core and how to install, configure, and manage each role using the tools and methods described in Chapters 5 and 6.
- Finally, Chapter 13 describes how to maintain various aspects of Server Core, including managing services, devices, processes, scheduled tasks, event logs, software updates, and management agents.

Conventions Used in This Book

Many elements have been used in this book to help keep the text clear and easy to follow. Commands within text that you can type to perform different tasks are styled in **bold** type. Commands with their command output are styled in `monospace` type to make them more visible, and I've included typical output of many commands so you can know what to expect when you use them. And new terms being introduced are styled in *italic* type.

I've also included the following elements where they can be helpful:

- **Note** Provides additional detail or a sidelight on the topic under discussion
- **Caution** Informs you of things to be aware of so you can avoid potential pitfalls
- **Tip** Gives you some pointers that you'll probably want to know because it will make your job easier

- **Best Practices** Offers advice that you should follow to maintain supportability for your configuration
- **More Info** Directs you to where you can get more information about the subject being discussed

Other Server Core Resources

While this book is intended as a comprehensive resource on administering Server Core, there are several other resources out there that you can use if this book doesn't provide you with all the information you need. I've already mentioned the *Windows Server 2008 Administrator's Pocket Consultant,* which complements this book—Stanek's book focuses on GUI administration, while this book concentrates on how you can do things from the command line. Another book you may find useful is the *Windows Command-Line Administrator's Pocket Consultant, Second Edition*, also by William Stanek, which explains the syntax of different Windows commands. Both these books are published by Microsoft Press and are available from booksellers everywhere.

For a quick introduction to administering Server Core, you can read the "Server Core Installation Option of Windows Server 2008 Step-By-Step Guide" in the Windows Server 2008 Technical Library on Microsoft TechNet at *http://technet.microsoft.com/en-us/windowsserver/default.aspx*

There are also several blogs that contain some excellent posts on administering Server Core. The two I've found most useful are Andrew Mason's "Server Core" blog on TechNet (*http://blogs.technet.com/server_core/*) and the Server Core posts on Sander Berkouwer's "The Things That Are Better Left Unspoken" blog (*http://blogs.dirteam.com/blogs/sanderberkouwer/*).

Finally, if you want to interact with other administrators who are working with Server Core, the best place to do so is the Server Core forum on TechNet at *http://forums.technet.microsoft.com/en-US/winservercore/threads/*. Feel free to post your questions and comments there, or better yet, answer questions posted by others.

Contact the Author

You may feel free to contact me if you have comments, questions, or suggestions regarding anything in this book. While I respond to all queries from readers and will do my best to answer your question to your satisfaction, I cannot provide readers with technical support. Please send your questions to the alias *sc@mtit.com*, where they will be queued for my attention; expect a reply within one or two days. You can also check my Web site *http://www.mtit.com* for links to numerous articles and tips I've written. Please check these out because the answer to your question or problem may already be published in one of these.

Support

Every effort has been made to ensure the accuracy of this book. Microsoft Press provides corrections for books through the World Wide Web at the following address: *http://www.microsoft.com/mspress/support*.

If you have comments, questions, or ideas about this book, please send them to Microsoft Press using either of the following methods:

Postal mail:

Microsoft Press

Attn: *Windows Server 2008 Server Core Administrator's Pocket Consultant* Editor

One Microsoft Way

Redmond, WA 98052-6399

E-mail:

mspinput@microsoft.com

Please note that product support isn't offered through the mail addresses. For support information, visit Microsoft's Web site at *http://support.microsoft.com/*.

Chapter 6

Remote Management

Server Core can be managed remotely using a variety of approaches, including using Remote Desktop or TS Remote App, using Microsoft Management Console (MMC) snap-ins and the Remote Server Administration Tools (RSAT), using Windows Remote Shell (WinRS), using Group Policy, and, to some extent, using Windows PowerShell. This chapter examines each of these remote administration methods and demonstrates how to set them up and use them to manage Server Core.

Using Remote Desktop

You can use Remote Desktop (also known as Terminal Services for Administration) to administer a Server Core installation remotely in exactly the same way you would administer it from the local console of the server. By default, Remote Desktop is disabled on Server Core, so before you can use Remote Desktop to manage a Server Core installation remotely, you must first enable Remote Desktop on the server. This can be done in several ways, as the next sections illustrate.

Enabling Remote Desktop Using Scregedit.wsf

You can use the Scregedit.wsf script to enable Remote Desktop on your Server Core installation by logging on locally to your server and doing the following:

```
C:\Users\Administrator> cscript %windir%\system32\scregedit.wsf /ar 0
Microsoft (R) Windows Script Host Version 5.7
Copyright (C) Microsoft Corporation. All rights reserved.

Registry has been updated.
```

To verify that the registry change has been made, do this:

```
C:\Users\Administrator>cscript %windir%\system32\scregedit.wsf /ar /v
Microsoft (R) Windows Script Host Version 5.7
Copyright (C) Microsoft Corporation. All rights reserved.

System\CurrentControlSet\Control\Terminal Server fDenyTSConnections
View registry setting.
0
```

A value of 0 for the fDenyTSConnections registry value means that Remote Desktop is enabled on the system, while a value of 1 means that Remote Desktop is disabled. If you later decide you want to disable Remote Desktop on your Server Core installation, type **cscript %windir%\system32\scregedit.wsf /ar 1** at a command prompt.

Tip If your current directory is C:\Windows\System32, you can shorten these commands by omitting the %Windir%\System32\ portion of them.

Enabling Remote Desktop using Scregedit.wsf also automatically enables the Remote Desktop rule group in Windows Firewall.

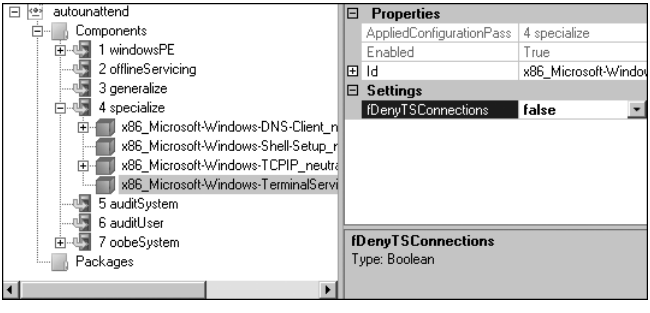
Enabling Remote Desktop Using an Answer File

You can use an answer file to enable Remote Desktop during an unattended install of Server Core. You do this as follows:

1. Add the following component to the specialize configuration pass of your answer file:

   Microsoft-Windows-TerminalServices-LocalSessionManager

2. In the Properties pane, click the box to the right of the fDenyTSConnections setting; a drop-down arrow appears. Click the drop-down arrow and select False, as shown here.



3. Add the following component to the oobeSystem configuration pass of your answer file:

   Microsoft-Windows-Shell-Setup\FirstLogonCommands\SynchronousCommand

4. In the Properties pane, type **C:\Windows\system32\netsh advfirewall firewall set rule group="Remote Desktop" new enable=yes** in the box beside CommandLine and type **1** (or another number if you are running multiple FirstLogonCommands) in the box beside Order.

Tip You can also use WinRS to enable Remote Desktop remotely on a Server Core installation. See the section "Using WinRS to Administer Server Core in a Domain," later in this chapter, for more information.

Using Scregedit.wsf to Require Network Level Authentication for Remote Desktop

By default, when Remote Desktop is enabled on Server Core, computers running versions of Microsoft Windows earlier than Windows Vista are allowed to connect. You can use the Scregedit.wsf script to prevent computers running versions earlier than Windows Vista from connecting to Server Core using Remote Desktop by logging on locally to your server and doing the following:

```
C:\Users\Administrator>cscript %windir%\system32\scregedit.wsf /cs 1
Microsoft (R) Windows Script Host Version 5.7
Copyright (C) Microsoft Corporation. All rights reserved.

Registry has been updated.
```

Doing this increases the security of your Server Core installation by requiring that the client you are using to administer Server Core uses Network Level Authentication. For more information, see the section "Configuring Remote Desktop to Require Network Level Authentication," in Chapter 3, "Initial Configuration."

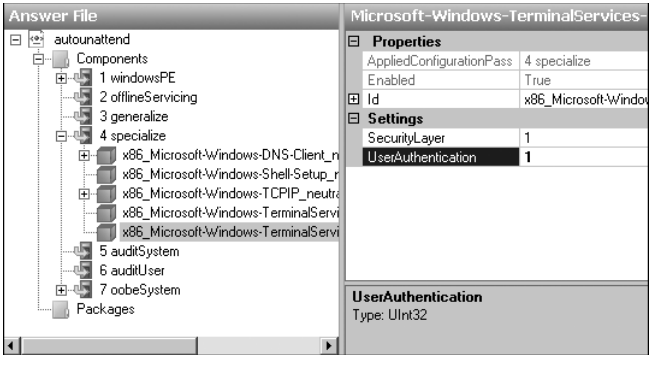
Using an Answer File to Require Network Level Authentication for Remote Desktop

You can use an answer file to require that Network Level Authentication be used for Remote Desktop connections. You do this as follows:

1. Add the following component to the specialize configuration pass of your answer file:

   Microsoft-Windows-TerminalServices-RDP-WinStationExtensions

2. In the Properties pane, click the box to the right of the UserAuthentication setting and type **1** to require Network Level Authentication, as shown here.



You can also configure the SecurityLayer setting to specify how your server and Remote Desktop clients authenticate each other prior to a Remote Desktop connection being established. The possible values for this setting are shown in Table 6-1.

Table 6-1 The SecurityLayer Setting Values

SecurityLayer	Result
0	Remote Desktop Protocol (RDP) is used by the server and the client for authentication prior to a Remote Desktop connection being established. Use this setting if you are working in a heterogeneous network environment.
1	The server and the client negotiate the method for authentication prior to a Remote Desktop connection being established (this is the default value). Use this setting if all your client computers are running Windows.
2	Transport Layer Security (TLS) is used by the server and the client for authentication prior to a Remote Desktop connection being established. Use this setting for maximum security.

Using Remote Desktop to Administer Server Core

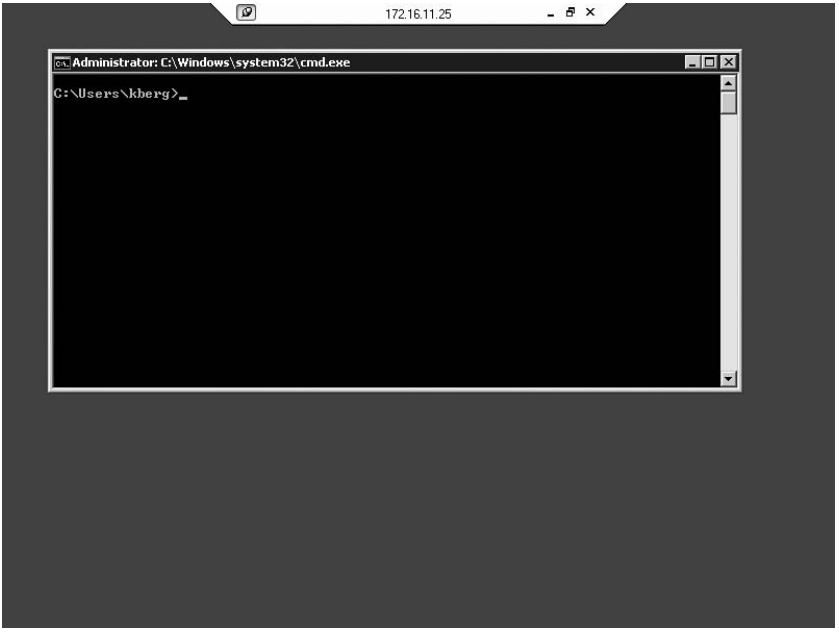
To use Remote Desktop to administer a Server Core installation, log on to a computer running Windows Vista or Windows Server 2008 and do the following:

1. Press the Windows key+R to open the Run text box.
2. Type **mstsc** and press Enter to open Remote Desktop Connection.
3. Type the name, either NetBIOS or Fully Qualified Domain Name (FQDN), or the Internet Protocol (IP) address of your Server Core installation in the Computer text box.
4. Click Options and type the name of a user account that has administrative privileges on the Server Core installation. Be sure to type this user name in the form *servername\username* (if the server belongs to a workgroup) or *domainname\username* (if the server belongs to a domain), as shown here.

5. Click Connect. When the Windows Security dialog box appears, type the password for the user account you are using to administer Server Core, as shown here.

6. Select Remember My Credentials if you want Credential Manager to save the credentials for this user.

7. Click OK. After a few moments, Remote Desktop Connection should connect to your remote Server Core installation (as shown here), and you then can administer your server using the same methods described in Chapter 5, "Local Management."



8. When you are finished administering your server, type **logoff** to end the Terminal Services session with the remote server.

Note Like the Full installation option of Windows Server 2008, the Server Core installation option supports two simultaneous Terminal Services connections for remote administration.

Using TS Remote App for Publishing Cmd to Administer Server Core

You don't have to use the full version of Remote Desktop to administer Server Core remotely. Instead, you can use Terminal Services RemoteApp to publish the Server Core command interpreter (Cmd) so that it can be started on another computer. That way, the command prompt running on Server Core programs can be accessed remotely using Terminal Services and appear as if it is running on your local

administrator workstation. TS RemoteApp programs run side by side with local programs and can be maximized or minimized just as local programs can be.

To use TS Remote App to publish Cmd running on Server Core, do the following:

1. On the Server Core installation you want to manage, enable Remote Desktop using one of the methods described earlier in this chapter. Then enable the Remote Administration rule group in Windows Firewall by typing the following command:

   netsh advfirewall firewall set rule group="Remote Administration" new enable=yes

2. Now install the Terminal Server role service of the Terminal Services role on a computer running Windows Server 2008. Alternatively, you can install the Terminal Server Tools component of RSAT on a computer running Windows Server 2008, which you can then use as a Terminal Services management station.

3. On your terminal server (or on your Terminal Services management station), click Start, Administrative Tools, Terminal Services, and finally TS RemoteApp Manager to open the TS RemoteApp console on your terminal server.

4. Click Connect To Computer in the right Actions pane to open a Select Computer dialog box. Select the Another Computer option and type or browse to the name of your Server Core computer. Click OK. Your TS RemoteApp Manager console is now connected to the Server Core computer.

5. In the Actions pane, click Add RemoteApp Programs, Next, and Browse to open the Choose A Program dialog box. Browse the local file system of the Server Core computer using the connection to the C$ administrative share on that computer until you find and select the C$\Windows\System32\Cmd.exe file. Click Open, Next, and finally Finish.

6. In the RemoteApp Programs list, right-click Cmd.exe and select Create .rdp File from the drop-down menu to start the RemoteApp Wizard. Click Next twice and then click Finish. The folder C:\Program Files\Packaged Programs opens on your Server Core computer, displaying the .rdp file for Cmd.

7. Double-click the .rdp file and click Connect. The Windows Security dialog box appears. Type credentials that have administrative privileges on the remote Server Core installation and then click OK.

8. Click Run to run Cmd.exe on the remote Server Core installation and display the remote command interpreter as a command-prompt window on your desktop. You can also copy the .rdp file to any computer using the RDC 6.0 client or later and use it to connect to your Server Core installation and open the command prompt on the Server Core computer.

Managing Terminal Services on Server Core

You can use the following two MMC snap-ins for remotely managing Terminal Services (Remote Desktop for Administration) on Server Core:

- Terminal Services Manager
- Terminal Services Configuration

You can use these snap-ins on a Full installation of Windows Server 2008 that has the Terminal Services role installed, or you can use them on a computer running Windows Vista or Windows Server 2008 that has the RSAT installed.

You can also manage Terminal Services (Remote Desktop for Administration) from the command prompt on a Server Core installation. Table 6-2 lists the commands that you can use to manage Terminal Services locally on Server Core.

Table 6-2 Commands Available for Locally Managing Terminal Services on Server Core

Command	Description
Change logon	Enables or disables logons to a terminal server
Logoff	Logs a user off a session and deletes the session
Msg	Sends a message to a user or group of users
Query process	Displays information about processes running on a terminal server
Query session	Displays information about sessions on a terminal server
Query user	Displays information about user sessions on a terminal server
Tscon	Connects to another existing terminal server session
Tsdiscon	Disconnects a client from a terminal server session
Tskill	Ends a process
Shutdown	Shuts down a terminal server

For example, to display all Terminal Services sessions on a Server Core installation named SEA-SC2, do this:

```
C:\Users\tallen>query session /server:SEA-SC2
 SESSIONNAME       USERNAME                 ID  STATE   TYPE        DEVICE
 services                                    0  Disc
 console           tallen                    1  Active
 rdp-tcp#0         Administrator             2  Active  rdpwd
 rdp-tcp                                 65536  Listen
```

The output of the Query Session command shows that administrator Tony Allen (tallen@contoso.com) is logged on locally to the Server Core installation, while the default Administrator account (either a built-in local or a domain account) is logged on remotely using a Remote Desktop session.

To log the remote Administrator off of the Server Core installation forcibly, log off session 2 as follows:

```
C:\Users\tallen>logoff 2 /server:SEA-SC2
```

Verify the result:

```
C:\Users\tallen>query session /server:SEA-SC2
 SESSIONNAME       USERNAME                 ID  STATE   TYPE        DEVICE
 services                                    0  Disc
 console           tallen                    1  Active
 rdp-tcp                                 65536  Listen
```

Using WinRS

You can use WinRS to administer a Server Core installation remotely from the command line. WinRS is a command-line tool included in both Windows Vista and the Full installation of Windows Server 2008, which relies on Windows Remote Management (WinRM) to execute remote commands, especially for headless servers. WinRM is Microsoft's implementation of the WS-Management protocol, a standard Simple Object Access Protocol (SOAP)–based, firewall-friendly protocol that enables hardware and operating systems from different vendors to interoperate. You can think of WinRM as the server side and WinRS the client side of WS-Management.

Configuring WinRM on Server Core

To enable WinRM on a Server Core installation, you need to run a configuration command that creates a "listener" that can respond to WinRS commands issued from other computers. The configuration command also opens an exception for WinRM in Windows Firewall. To enable WinRM, do the following:

```
C:\Users\tallen>winrm quickconfig
WinRM is not set up to allow remote access to this machine for management.
The following changes must be made:

Create a WinRM listener on HTTP://* to accept WS-Man requests to any IP
on this machine.
Enable the WinRM firewall exception.

Make these changes [y/n]? y

WinRM has been updated for remote management.

Created a WinRM listener on HTTP://* to accept WS-Man requests to any IP
on this machine.
WinRM firewall exception enabled.
```

Note For more information on configuring WinRM, type **winrm help config** at a command prompt.

Using WinRS to Administer Server Core in a Domain

The basic syntax for WinRS commands is as follows:

winrs –r:*target command*

where *target* is the name (NetBIOS or FQDN) of the Server Core installation that has had WinRM enabled on it, and *command* is any command string that you want to execute on the Server Core installation. For example, to use WinRS to enable Remote Desktop remotely on a Server Core installation named SEA-SC2, type the following command on any computer running Windows Vista or on a Full installation of Windows Server 2008:

winrs –r:SEA-SC2 cscript %WINDIR%\system32\scregedit.wsf /ar 0

When you type this command on a computer running Windows Vista, for example, the command is executed remotely on the targeted Server Core installation and the command output is piped back to the command shell on your computer running Windows Vista:

```
C:\Users\Administrator>winrs -r:SEA-SC2 cscript %windir%
\system32\scregedit.wsf /ar 0
Microsoft (R) Windows Script Host Version 5.7
Copyright (C) Microsoft Corporation. All rights reserved.

Registry has been updated.
```

You can do anything using WinRS that you can do at the local command prompt on Server Core. For example, you can perform the initial configuration of your Server Core installation, install and uninstall roles and features on your server, and perform other tasks.

Note For more information on the syntax of WinRS commands, type **winrs /?** at a command prompt.

Using WinRS to Administer Server Core in a Workgroup

You can use WinRS to administer a Server Core installation that belongs to a workgroup. Before you can do this, however, you must add the name of your computer to the TrustedHosts table of WinRM on your Server Core installation. For example, to enable a computer running Windows Vista named SEA-DESK155 to execute

commands remotely on your Server Core installation using WinRM, type the following on your Server Core computer:

```
C:\Users\Administrator>winrm set winrm/config/client @{TrustedHosts=
"SEA-DESK155"}
Client
    NetworkDelayms = 5000
    URLPrefix = wsman
    AllowUnencrypted = false
    Auth
        Basic = false
        Digest = true
        Kerberos = true
        Negotiate = true
        Certificate = true
    DefaultPorts
        HTTP = 80
        HTTPS = 443
    TrustedHosts = SEA-DESK155
```

Requirements for Using WinRS

To use WinRS to administer a Server Core installation remotely, each of the following must be true:

- Your local computer must be running either Windows Vista or a Full installation of Windows Server 2008.
- You must enable a WinRM listener on the Server Core installation, and you must open the WinRM exception in Windows Firewall on the Server Core installation; the Winrm quickconfig command can be used to do this.
- You must execute your WinRS commands using administrator credentials on the Server Core installation. If you are not currently logged on to your computer using such credentials, you can use the Net use command to connect to the Server Core computer using such credentials. For example, to connect to a Server Core installation named SEA_SC2 using the credentials of administrator Tony Allen (tallen@contoso.com), type **net use \\SEA-SC2\IPC$ /u:CONTOSO\tallen** at a command prompt. Type Tony's password when prompted to do so, and then you can execute commands remotely on the Server Core installation using WinRS.
- Commands or scripts that are executed using WinRS must have no user interface dependencies. This means that you cannot execute commands that prompt you to Press Any Key when they are typed at the local console or require any other interactive response.

Configuring WinRM and WinRS Using Group Policy

You can use Group Policy to configure security for both WinRM and WinRS. The relevant policy settings are found in the following locations:

- Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management (WinRM)
- Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Shell

Using MMC Snap-ins and RSAT

You can use Microsoft Management Console (MMC) snap-ins to administer a Server Core installation remotely from a Full installation of Windows Server 2008. You can also install RSAT on either Windows Vista or a Full installation of Windows Server 2008 and use these tools to administer Server Core. The advantage of using RSAT is that it gives you the full complement of MMC consoles; by comparison, on a Full installation of Windows Server 2008, you may be missing some consoles because of certain roles and features not being installed on your server. Using MMC snap-ins or RSAT allows you to administer a Server Core installation the same way that you administer a Full installation—without the need of learning the syntax of many command-line utilities.

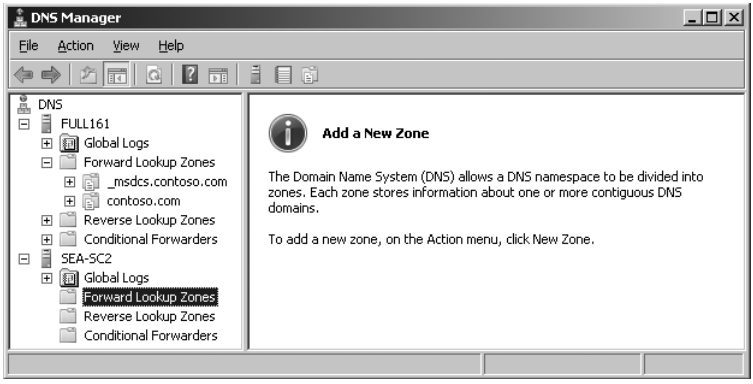
Using MMC Consoles to Administer Server Core in a Domain

When you install a server role on a Server Core installation, the appropriate firewall ports needed to manage that role remotely using MMC snap-ins are opened automatically. This means that when you type **start /w ocsetup DNS-Server-Core-Role** at a command prompt on a Server Core installation, the command installs the DNS Server role and enables the Windows Management Instrumentation (WMI) and DNS Service rule groups to allow the DNS snap-in running on another computer to connect to Server Core.

For example, to use the DNS console found under Administrative Tools on a domain controller named FULL161 to administer a Server Core DNS server named SEA-SC2, perform the following steps:

1. On the domain controller, click Start, Administrative Tools, and then DNS to open the DNS Manager console.
2. Right-click the root node of the console and select Connect To DNS Server.
3. In the Connect To DNS Server dialog box, select The Following Computer and type **SEA-SC2** in the text box. Click OK.

4. The DNS Manager console connects to DNS server SEA-SC2. Expand the console tree to display the configuration of DNS server SEA-SC2, as shown here.



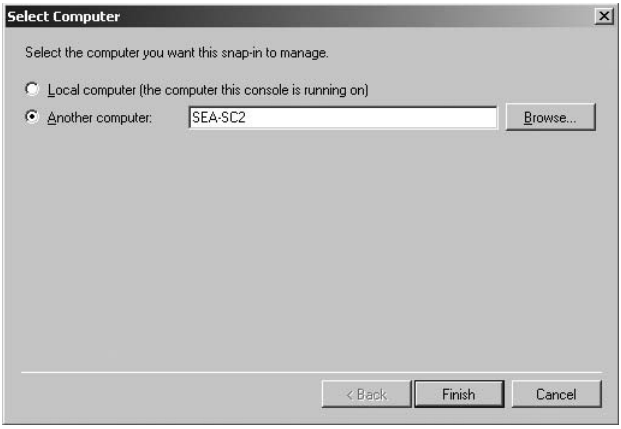
Changing the Focus of an MMC Console

Most (but not all) MMC consoles found under Administrative Tools can have their focus changed to administer a different computer than the local one on which they are being used. Examples of consoles that can have their focus changed include Active Directory Users And Computers, Computer Management, DHCP, DNS, and Event Viewer. Examples of consoles whose focus cannot be changed include Server Manager, Windows Firewall With Advanced Security, and Windows Server Backup.

Using MMC Snap-ins to Administer Server Core

You can also add MMC snap-ins to a new MMC console to administer Server Core remotely. For example, to use the Windows Firewall With Advanced Security snap-in to manage the firewall remotely on a Server Core installation named SEA-SC2, do the following:

1. Press the Windows key+R, type **mmc**, and click OK to open an empty MMC console.
2. Click File, and then click Add/Remove Snap-in. Scroll down the list of snap-ins and double-click Windows Firewall With Advanced Security to select it. When the Select Computer dialog box appears, choose Another Computer and type **SEA-SC2** in the text box, as shown here.



3. Click Finish, and then click OK to add the snap-in to the console. Expand the console tree to view the configuration of Windows Firewall on your Server Core installation.

Some MMC snap-ins require that you also open ports in the firewall on Server Core to use these snap-ins to administer Server Core remotely. For example, for the previous procedure to work, you must first enable the Windows Firewall Remote Management rule group in the firewall on your Server Core installation. This can be done by typing the following command at your Server Core command prompt:

netsh advfirewall firewall set rule group="Windows Firewall Remote Management" new enable=yes

Table 6-3 lists some of the more commonly used MMC snap-ins and the firewall rule group that must be enabled to use these snap-ins to manage Server Core remotely. The general syntax for enabling a rule group in Windows Firewall is as follows:

netsh advfirewall firewall set rule group="*Name of rule group*" new enable=yes

Table 6-3 Rule Groups You Must Enable in Windows Firewall to Allow Remote Management by an MMC Snap-in

MMC Snap-in	Rule Group
Event Viewer	Remote Event Log Management
Services	Remote Service Management
Shared Folders	File And Printer Sharing
Task Scheduler	Remote Scheduled Tasks Management
Reliability And Performance	Performance Logs And Alerts File And Printer Sharing
Windows Firewall With Advanced Security	Windows Firewall Remote Management

Best Practices The simplest way to configure Windows Firewall on Server Core is to enable remote management of Windows Firewall and then use the Windows Firewall With Advanced Security snap-in on a computer running Windows Vista to make further configuration changes to your firewall. You can also use Group Policy to configure Windows Firewall once the Windows Firewall Remote Management rule group is enabled on your Server Core installation. For more information on using the Windows Firewall With Advanced Security snap-in, see *http://technet.microsoft.com/en-us/network/bb545423.aspx*.

Some MMC snap-ins require further configuration of your Server Core installation before you can use them to administer your server. The following sections describe several of these snap-ins and the additional configuration that they require on the server before they will work remotely against it.

Using the Device Manager Snap-in

To allow the Device Manager snap-in to administer Server Core remotely, perform the following steps:

1. On your Server Core computer, enable the Remote Administration rule group in Windows Firewall.
2. On a Full installation of Windows Server 2008, open a new MMC console by pressing the Windows key+R, typing **mmc**, and clicking OK.
3. Click File, and then Add/Remove Snap-in to open the Add Or Remove Snap-ins dialog box.
4. Double-click Group Policy Object Editor to display the Group Policy Wizard.
5. Click Browse, select Another Computer, and type or browse to the name of your Server Core computer. Then click OK, Finish, and finally OK again. The Group Policy Object Editor is now connected to your Server Core computer.
6. Browse the console tree to find and enable the following policy setting:

   Computer Configuration\Policies\Administrative Templates\System\Device Installation\Allow Remote Access To The PnP Interface.
7. Close the Group Policy Object Editor. Then, on your Server Core computer, type **shutdown −r −t 0** at the command prompt to restart the server.

Note Device Manager can operate only in "view only" mode when run from a remote computer as described here.

Using the Disk Management Snap-in

To allow the Disk Management snap-in to administer Server Core remotely, perform the following steps:

1. Enable the Remote Volume Management rule group in Windows Firewall on your Server Core installation.
2. Start the Virtual Disk Service (VDS) by typing **sc start vds** at the command prompt. You can also type **sc config vds start= auto** to configure the service to start automatically each time the computer boots.

Using the IP Security Policy Management Snap-in

To allow the IP Security Policies snap-in to administer Server Core remotely, type the following command at the command prompt of your Server Core installation:

cscript %windir%\system32\scregedit /im 1

Using the Reliability And Performance Snap-in

No additional configuration is needed to use the Reliability And Performance snap-in, but it can monitor only performance data, not reliability data, on a remote Server Core installation.

Enabling Any MMC Snap-in to Administer Server Core

You can allow any MMC snap-in to administer Server Core remotely by enabling the Remote Administration rule group in Windows Firewall on your Server Core installation. To do this, type the following command:

netsh advfirewall firewall set rule group="Remote Administration" new enable=yes

As described in the section "Using MMC Consoles to Administer Server Core in a Domain," earlier in this chapter, some snap-ins require additional configuration to get them to work properly for remotely administering Server Core.

Using MMC Snap-ins to Administer Server Core in a Workgroup

To use MMC snap-ins to administer a Server Core installation that belongs to a workgroup, you need to perform the following actions on your Server Core installation:

1. Enable the required rule groups in Windows Firewall (see the previous section for details).
2. Use Cmdkey to specify different credentials for MMC connections.

For example, to use the Services snap-in on a computer running Windows Vista to administer the services on a Server Core installation named SEA-SC1 that belongs to a workgroup, perform the following steps:

1. On your Server Core installation, type the following command to enable the Remote Service Management rule group in Windows Firewall:

   netsh advfirewall firewall set rule group="Remote Service Management" new enable=yes

2. Open a command prompt on your computer running Windows Vista and type the following command:

   cmdkey /add:SEA-SC1 /user:Administrator /pass:Pa$$w0rd

   In this command, the local Administrator account on SEA-SC1 has the password **Pa$$w0rd.**

3. Open the Services console under Administrative Tools (or add the Services snap-in to an empty MMC console), right-click the root node, and select Connect To Another Computer. Type **SEA-SC1** in the dialog box and then click OK.

You can now manage services remotely on your stand-alone Server Core installation from either a stand-alone or domain-joined computer running Windows Vista or Windows Server 2008.

Note Cmdkey is not needed for certain consoles, including Event Viewer and Scheduled Tasks.

Using RSAT to Administer Server Core in a Domain

Windows Server 2003 included the Administration Tools Pack (Adminpak.msi), which provided server management tools that allowed administrators to manage Windows 2000 Server and Windows Server 2003 family servers remotely. The Administration Tools Pack could be installed on workstations running Windows XP to provide administrators with a full set of MMC consoles on their workstations for administering servers across their network.

With Windows Server 2008, however, the Administration Tools Pack has been replaced with the Remote Server Administration Tools (RSAT), which enables administrators to manage Windows Server 2008 roles and features remotely from a computer running Windows Vista with Service Pack 1 (SP1). RSAT is included as an optional feature on all editions of Windows Server 2008, and versions of RSAT for installing on 32-bit and 64-bit versions of Windows Vista SP1 Business, Enterprise, and Ultimate editions are available for download from the Microsoft Download Center at

http://www.microsoft.com/downloads/. For detailed information concerning the downloadable version of RSAT and the administrative tools it includes, see *http://support.microsoft.com/kb/941314*.

Using RSAT on either Windows Vista or a Full installation of Windows Server 2008, you can administer roles and features remotely on a Server Core installation the same way that you would administer them on a Full installation of Windows Server 2008.

Note RSAT cannot be installed on Server Core.

Installing RSAT on a Full Installation of Windows Server 2008

To install RSAT on a Full installation of Windows Server 2008, perform the following steps:

1. Start the Add Features Wizard from either Server Manager or Initial Configuration Tasks.
2. Expand the Remote Server Administration Tools check box and select the check boxes under it for the specific role and feature administration tools that you want to install on your server. Alternatively, you can select the Remote Server Administration Tools check box to install all the role and feature administration tools on your server.

Installing RSAT on Windows Vista SP1

To install RSAT on Windows Vista with Service Pack 1, perform the following steps:

1. Download the appropriate Windows Installer (.msi) package (either 32-bit or 64-bit) by using the links found at *http://support.microsoft.com/kb/941314*.
2. Double-click the downloaded Windows Update Standalone Installer package (Windows6.0-KB941314-x86.msu or Windows6.0-KB941314-x64.msu) to start the Setup wizard. Follow the prompts to complete the installation.
3. Open Control Panel and click Programs.
4. Under Programs And Features, click Turn Windows Features On Or Off. Respond to the User Account Control prompt as required.
5. In the Windows Features dialog box, scroll down and expand the Remote Server Administration Tools check box, then select the check boxes under it to install the remote administration snap-ins and tools that you want to install. You can also install all role and feature administration tools by selecting the Remote Server Administration Tools check box. Click OK when finished.

6. Configure your Start menu to display the Administration Tools shortcut by right-clicking Start and clicking Properties. Then on the Start Menu tab, click Customize, scroll down to System Administrative Tools, and select Display On The All Programs Menu And The Start Menu. Click OK when finished.

Note Installing RSAT also provides additional snap-ins that you can add to a blank MMC console.

Using RSAT to Administer Server Core Remotely in a Domain

You can use the RSAT tools to administer roles and features remotely on a Server Core installation that belongs to the same domain as your management workstation. As described in the section "Using MMC Snap-ins to Administer Server Core," earlier in this chapter, you may need to configure Windows Firewall on your remote Server Core installation for some RSAT tools to be able to connect.

For example, to use RSAT on a computer running Windows Vista in the contoso.com domain to manage the DNS Server role on a Server Core installation named SEA-SC2 that belongs to the same domain, follow these steps:

1. On your Server Core installation, begin by enabling the necessary rule groups in Windows Firewall to allow remote administration of roles and features on the server. To allow remote administration of all roles and features on the server, type the following command:

   netsh advfirewall firewall set rule group="Remote Administration" new enable=yes

   As described in the section "Using MMC Consoles to Administer Server Core in a Domain," earlier in this chapter, some snap-ins require additional configuration to get them to work properly for remotely administering Server Core.

2. Click Start, Administrative Tools, and then DNS to open the DNS Manager console. Before the console opens, a Connect To DNS Server dialog box appears. Select the The Following Computer option, type **SEA-SC1**, and click OK. DNS Manager opens and lets you remotely manage your Server Core DNS server.

Tip When you install RSAT using the procedures outlined earlier in this section, some MMC consoles found under Administrative Tools (such as the Windows Firewall With Advanced Security) cannot have their focus changed. To administer Windows Firewall remotely on a Server Core installation, you can open a blank MMC, add the Windows Firewall With Advanced Security snap-in, and change the focus of the snap-in so you can manage Windows Firewall on the remote Server Core installation.

Using RSAT to Administer Server Core Remotely in a Workgroup

You can use the RSAT tools to administer roles and features remotely on a Server Core installation that belongs to a workgroup. As described in the section "Using MMC Snap-ins to Administer Server Core," earlier in this chapter, you may need to configure Windows Firewall on your remote Server Core installation for some RSAT tools to be able to connect.

For example, to use RSAT on a computer running Windows Vista to manage the DNS Server role on a stand-alone Server Core installation named SEA-SC1, do this:

1. On your Server Core installation, begin by enabling the necessary rule groups in Windows Firewall to allow remote administration of roles and features on the server. To allow remote administration of all roles and features on the server, type the following command:

   netsh advfirewall firewall set rule group="Remote Administration" new enable=yes

   As described in the section "Using MMC Consoles to Administer Server Core in a Domain," earlier in this chapter, some snap-ins require additional configuration to get them to work properly for remotely administering Server Core.

2. Open a command prompt on your Windows Vista computer and type the following command:

   cmdkey /add:SEA-SC1 /user:Administrator /pass:Pa$$w0rd

   In the previous command, the local Administrator account on SEA-SC1 has the password Pa$$w0rd.

3. Click Start, Administrative Tools, and then DNS to open the DNS Manager console. Before the console opens, a Connect To DNS Server dialog box appears. Select the The Following Computer option, type **SEA-SC1**, and click OK. DNS Manager opens and lets you remotely manage your Server Core DNS server.

Using Other GUI Tools

You can use other graphical user interface (GUI) tools besides MMC snap-ins to manage certain aspects of Server Core remotely. These tools include the following:

- Windows Explorer
- Task Scheduler
- Registry Editor

The following procedures assume that your remote Server Core installation belongs to the same domain as your Windows Vista management workstation. If your Server Core installation belongs to a workgroup, type the command **cmdkey /add:*servername***

/user:*username* /pass:*password* to provide administrator credentials (that is, *username* and *password*) for these tools to be able to manage your Server Core installation (*servername*) remotely.

Using Windows Explorer Remotely

You can use Windows Explorer on a computer running Windows Vista or a computer running a Full installation of Windows Server 2008 to manage the file system remotely on a Server Core installation. To do this, follow these steps:

1. On the Server Core installation, enable the Remote Administration rule group in Windows Firewall by typing the following command:

   netsh advfirewall firewall set rule group="File and Printer Sharing" new enable=yes

2. On the computer from which you want to manage your Server Core installation's file system remotely, press the Windows key+R, type ***servername*\C$** (where *servername* is the name of your Server Core installation), and click OK. Specify credentials that have administrative privileges on the Server Core installation if you are prompted to do so.

3. Windows Explorer opens a new window focused on the root of the system drive on your Server Core installation. You now can browse the system drive on your remote server, create or delete files and folders, and perform other operations depending upon your level of privileges.

You can use the previous procedure with any share, whether administrative or user-created. You can also use the Net use command to map persistent network drives to shares on your remote Server Core installation. For example, you can type **net use Z: *servername*\C$ /persistent:yes** at the command prompt, where *servername* is the name of your remote Server Core installation.

Using Task Scheduler Remotely

You can use Task Scheduler on a computer running Windows Vista or a computer running a Full installation of Windows Server 2008 to create, delete, configure, and manage tasks remotely on a Server Core installation. To do this, follow these steps:

1. Click Start, All Programs, Accessories, and then System Tools, and open Task Manager on your computer running Windows Vista.

2. Right-click the root node in Task Scheduler and select Connect To Another Computer.

3. Type the name of the remote Server Core installation and click OK.

Using Registry Editor Remotely

You can use Registry Editor on a computer running Windows Vista or a computer running a Full installation of Windows Server 2008 to edit the registry on a Server Core installation remotely. To do this, follow these steps:

1. Press the Windows key+R, type **regedit**, and click OK to open Registry Editor on your computer running Windows Vista.
2. Select File, and then Connect Network Registry.
3. Type the name of the remote Server Core installation and click OK.

Using Group Policy

You can use Group Policy to manage Server Core remotely the same way that you manage any other computer running Windows. You cannot install Group Policy MMC consoles on Server Core; you must manage Server Core remotely using Group Policy MMC consoles on another computer, such as a Full installation of Windows Server 2008 or a computer running Windows Vista with RSAT installed.

For more information on using Group Policy to manage Active Directory–based networks, see http://technet.microsoft.com/en-us/windowsserver/grouppolicy/default.aspx.

Group Policy Tools on Server Core

Server Core does include two command-line Group Policy tools:

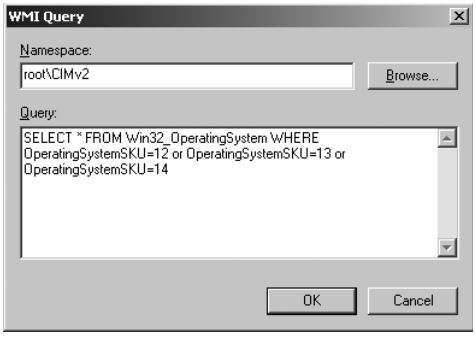
- **Gpupdate** Used to refresh local Group Policy settings and Group Policy settings stored in Active Directory Domain Services. Detailed syntax for using this command can be found at *http://technet.microsoft.com/en-us/library/bb490983.aspx* or by typing **gpupdate /?** at a command prompt.
- **Gpresult** Used to display Resultant Set of Policy (RSoP) information. Detailed syntax for using this command can be found in the Windows Server 2008 Command Reference (available from the Microsoft Download Center, as cited earlier in this chapter) or by typing **gpresult /?** at a command prompt.

Using WMI Filters to Administer Server Core with Group Policy

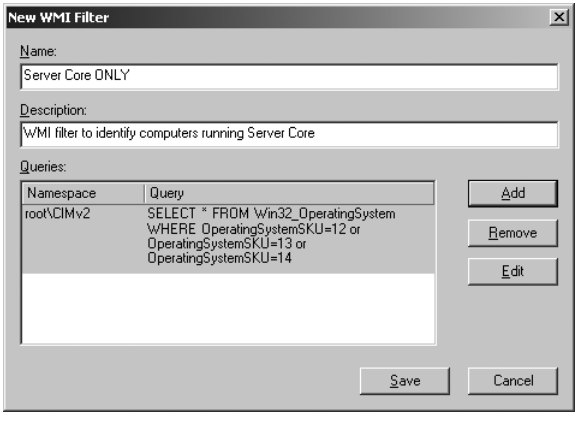
You can use WMI filters to ensure that the policy settings contained in a particular Group Policy Object (GPO) are applied only to Server Core installations. WMI filters are used to determine the scope of Group Policy based on computer attributes such as operating system and free hard disk space.

To create a WMI filter that will cause the Seattle SC GPO to be applied only to Server Core computers, perform the following steps:

1. On your domain controller, open Group Policy Management from Administrative Tools.
2. Right-click the WMI Filters node in the console tree and select New.
3. Click Add and type the information in the screenshot shown here to create a WMI Query Language (WQL) query that uses the OperatingSystemSKU property of the Win32_OperatingSystem WMI class to determine whether a given computer is running Server Core Standard (13), Enterprise (14), or Datacenter (15) edition.

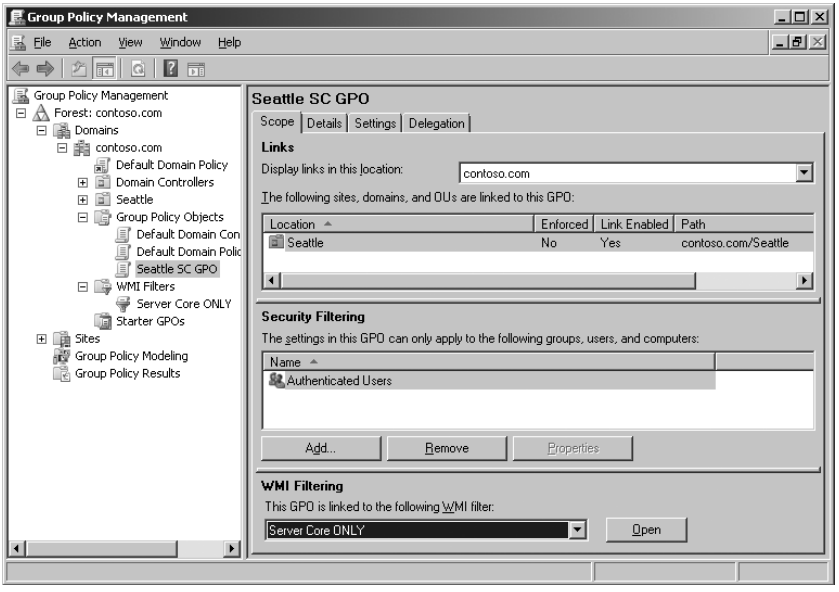


4. Click OK to add the WQL query to your WMI filter and type a name and description for your filter, as shown here.



5. Click Save to save your WMI filter.
6. Under Group Policy Objects, select Seattle SC GPO.

7. On the Scope tab, under WMI Filtering, select Server Core ONLY and click Yes when the dialog box appears, as shown here. The WMI filter is now linked to the GPO.



When Group Policy is processed by a computer targeted by the GPO, the WQL query contained in the WMI filter is evaluated against the WMI repository on the targeted computer. If the query evaluates as True, the GPO is applied; if the query evaluates as False, the GPO is not applied.

Note GPOs can have only one WMI filter, but you can link a single WMI filter to multiple GPOs.

Managing Local Group Policy on Server Core

You can manage local Group Policy on Server Core by using the Group Policy Object Editor running on a Full installation of Windows Server 2008 or on a computer running Windows Vista SP1. To do this, follow these steps:

1. Open a new MMC console by pressing the Windows key+R, typing **mmc**, and clicking OK.
2. Click File, and then Add/Remove Snap-in to open the Add Or Remove Snap-ins dialog box.
3. Double-click Group Policy Object Editor to display the Group Policy Wizard.

4. Click Browse, select Another Computer, and type or browse to the name of the remote Server Core computer.
5. Click OK, Finish, and finally OK again. Group Policy Object Editor is now connected to your remote Server Core computer, and you can browse local policy on the computer and configure it as desired.

Using Windows PowerShell

You can use Windows PowerShell to administer Server Core remotely, but only if you use WMI in your PowerShell commands. PowerShell WMI commands typically take the following form:

Get-WMIObject *WMIclass* -computername *servername*

where *WMIclass* is the WMI class you want to access and *servername* is the name of the remote Server Core installation.

> **Tip** To display a list of all WMI classes supported on a remote Server Core installation, type **Get-WMIObject –list –computername *servername*** at the PowerShell command prompt.

Here is an example of using PowerShell (running on a computer running Windows Vista on which PowerShell 1.0 has been installed) to display a list of services installed on a Server Core installation named SEA-SC2 that belongs to the same domain. Perform the following steps:

1. On the Server Core installation, enable the Windows Management Instrumentation (WMI) rule group in Windows Firewall by typing the following command:

   netsh advfirewall firewall set rule group="Windows Management Instrumentation (WMI)" new enable=yes

2. On the computer running Windows Vista, open the PowerShell command prompt by clicking Start, All Programs, Windows PowerShell 1.0, and finally Windows PowerShell.
3. Use the command shown here to display a list of services installed on SEA-SC2:

```
PS C:\Users\tallen> Get-WMIObject Win32_Service -computername SEA-SC2


ExitCode  : 0
Name      : AeLookupSvc
ProcessId : 964
StartMode : Auto
State     : Running
Status    : OK

ExitCode  : 1077
```

```
Name      : AppMgmt
ProcessId : 0
StartMode : Manual
State     : Stopped
Status    : OK
. . .
```

Note You cannot install Windows PowerShell 1.0 locally on Server Core.

For a quick introduction to using Windows PowerShell, see the Windows PowerShell Getting Started Guide on MSDN at http://msdn.microsoft.com/en-us/library/aa973757(VS.85).aspx.

Index

Symbols

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

Z