Server Core Remote Management
How to be effective in remotely managing Server Core installations of Windows Server 2008
Sander Berkouwer and Joachim Nässlander
Version 1.0
First published online in November 2009.

Copyright Sander Berkouwer and Joachim Nässlander. The rights of Sander Berkouwer and Joachim Nässlander to be identified as the authors of this work has been asserted by them in accordance with the Copyright, Designs and Patents Act 1988.

All rights reserved. No part of this publication may be reproduced, stored or introduced into a retrieval system, or transmitted, in any form, or by any means (electronic, mechanical, photocopying, recording or otherwise) without the prior written consent of the publisher. Any person who does any unauthorized act in relation to this publication may be liable to criminal prosecution and civil claims for damages.

This document is provided for informational purposes only and Microsoft makes no warranties, either express or implied, in this document. Information in this document, including URL and other Internet Web site references, is subject to change without notice. The entire risk of the use or the results from the use of this document remains with the user.

Active Directory, Microsoft, MS-DOS, Windows, Windows NT, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. All other trademarks are property of their respective owners.
Preface
Server Core installations of Windows Server 2008 are popular subjects on the Internet. A lot has been written about them. Microsoft has published a step-by-step guide and both Microsoft Press and Sybex have published a book on Server Core. However, after reading these materials Joachim and I found a lot of information is still missing, especially when it comes to managing Server Core installations remotely. This is why we produced this whitepaper to give you a bit more insight in how to achieve this.

This whitepaper contains information on remotely managing your Windows Server 2008 Server Core installations, using the following methods:

- Microsoft Management Console (MMC) Snap-ins
- Remote Server Administration Tools (RSAT)
- Remote Desktop Protocol (RDP)
- Windows Remote Management (WinRM) using the Windows Remote Shell (WinRS)
- Secure Shell (SSH)

In this whitepaper we will also discuss the best remote management method for common situations, so you can pick the remote management method for every situation.

Enjoy!

About the authors

Sander Berkouwer
Sander Berkouwer is a MCSA, MCSE and Microsoft Most Valuable Professional (MVP) on Directory Services. Working for OGD, a Dutch IT services provider he has ample experience with deploying and maintaining Windows, Windows Server and other Microsoft technologies with hundreds of environments, ranging from four to forty thousand seats.

You can read more from Sander at his blog: http://blogs.dirteam.com/blogs/sanderberkouwer/

Joachim Nässlander
Joachim Nässlander is a Microsoft Most Valuable Professional (MVP) on Cluster, with a strange interest in Server Core. He is employed by Knowledge Factory as a IT-Expert, after spending time as a consultant for various companies in Sweden.

Over the years Joachim has participated in several Microsoft Technology Adoption Programs (TAPs).

You can read more from Joachim at his blog: http://www.nullsession.com
Contents
Preface ................................................................................................................................. 2
Brief introduction to Server Core ......................................................................................... 4
Server Core by default .......................................................................................................... 5
  The Administrator password ............................................................................................ 5
  The Windows firewall ....................................................................................................... 6
Overview of remote management methods ........................................................................ 7
Remotely managing your Server Core using Compmgmt.msc ............................................ 8
  Computer Management .................................................................................................. 8
  Delegation Considerations ............................................................................................ 10
  Logon Considerations ................................................................................................... 11
Remotely managing your Server Core using RSAT .............................................................. 12
  Installing RSAT ........................................................................................................... 12
  Selecting RSAT features ............................................................................................... 13
  Displaying Administrative Tools .................................................................................. 15
  Using the Remote Server Administration Tools ............................................................ 15
Remotely managing your Server Core using RDP ............................................................... 18
  Enabling Remote Desktop ............................................................................................ 18
  Filtering the use of Remote Desktop ........................................................................... 19
  Securing Remote Desktop ............................................................................................ 19
  Using Remote Desktop .................................................................................................. 20
Remotely managing your Server Core using WinRM and WinRS ....................................... 21
  WinRM ......................................................................................................................... 21
  WinRS ........................................................................................................................... 23
Tips and tricks ..................................................................................................................... 23
Remotely managing your Server Core using SSH ............................................................... 25
  Server side configuration .............................................................................................. 25
  Client side configuration ............................................................................................... 28
**Brief introduction to Server Core**

When you install Windows Server 2008, a choice is presented to you. You can choose to install a Full installation or install a Server Core installation of the product. A Server Core installation of Windows Server 2008 is a highly optimized installation when you compare it to a Full installation. It is optimized for infrastructure tasks.

While Server Core installations have commonly been described as “Windows without Windows”, this classification is not entirely true. While most well-known Graphical User Interface (GUI) elements are missing from Server Core installations (like the Start button and the notification area), some graphical tools are still available, the login screen is identical to a Full installation and most programs, designed for a Full installation will install and run on a Server Core installation of Windows Server 2008.
Server Core by default
By default a Server Core installation of Windows Server 2008 has:

- An empty Administrator password
- The Windows Firewall enabled and most inbound traffic blocked

Understanding the default Windows Server 2008 installation, helps understand the underlying technologies and steps to perform to allow remote management of the box.

The Administrator password
An empty Administrator password is a security measure. Because the administrator account is the only account on a default Windows installation and an account without a password cannot be used as a network credential, authenticated access to the fresh installation from the network is impossible.

After you first install Windows Server 2008, in either a full or Server Core installation, you are required to change the Administrator password to a password that meets the complexity requirements. These requirements by default are:

- The password is at least six characters long.
- The password contains characters from three of the following four categories:
  - English uppercase characters (from A through Z)
  - English lowercase characters (from a through z)
  - Base 10 digits (from 0 through 9)
  - Non-alphanumeric characters (for example: !, $, #, or %)
- The password does not contain three or more characters from the user’s account name. If the account name is less than three characters long, this check is not performed because the rate at which passwords would be rejected would be too high. When checking against the user’s full name, several characters are treated as delimiters that separate the name into individual tokens: commas, periods, dashes, hyphens, underscores, spaces, number signs (#), and tab characters. Each token that is three or more characters long is searched for in the password, and if it is present, the password change is rejected. For example, the name “Erin M. Hagens” would be split into three tokens: “Erin,” “M,” and “Hagens.” Because the second token is only one character long, it would be ignored. Therefore this user could not have a password that included either “erin” or “hagens” as a substring anywhere in the password. None of these checks are case-sensitive.
The Windows firewall
By default the Windows Firewall in Windows Server 2008, both Full and Server Core installations, is enabled. It does not allow most of the inbound traffic, except traffic that is needed for basic network connectivity. For instance, DHCP traffic is allowed, since it offers basic network connectivity to download updates from both Windows and Microsoft Update without the need to configure a static IP address.

One thing to know about the Windows firewall is that you may feel the feature is pretty hard to circumvent. Many IT Professionals have made their standard practice to disable the Windows Firewall service. However, this will not prevent the Windows firewall from blocking most-used ports by malicious software. Disabling the Windows firewall Operational Mode, however, will have the desired effect.

While disabling the firewall, may be seen as a common practice for test environments, Microsoft recommends not turning off the Windows firewall on production servers. Instead, leave the firewall enabled and enable exceptions. That way, the box will still be protected from traffic on unmonitored or unwanted ports. Many criteria can be set per Windows firewall rule to merely permit the traffic per host, network, port, direction, type and encryption status.
Overview of remote management methods
This whitepaper contains information on remotely managing your Windows Server 2008 Server Core installations, using the following methods:

- Microsoft Management Console (MMC) Snap-ins
- Remote Server Administration Tools (RSAT)
- Remote Desktop Protocol (RDP)
- Windows Remote Management (WinRM) using the Windows Remote Shell (WinRS)
- Secure Shell (SSH)

The remaining question is which method to use in which situation:

Is your environment a mixed environment?
When your environment contains Windows XP and Windows Server 2003 hosts, you can't use many features in the Computer Management MMC (compmgmt.msc) Snap-ins or the Event Viewer from these hosts. The Remote Server Administration Tools (RSAT) cannot be used as well and the Windows Server 2003 Adminpak doesn't offer management of all Server Core features.

Use RDP or SSH from Windows XP and Windows Server 2003.
From Windows Vista SP1 and Windows Server 2008 you can use any method.

Does your environment consist of different routed subnets?
When your Server Core installation of Windows Server 2008 and your Windows Vista box are on different subnets you can't use many of the Computer Management MMC (compmgmt.msc) Snap-ins.

Use RDP or SSH in routed environments.

Does your environment consist of different domains or workgroups?
Many tools reuse your credentials to authenticate with the Server Core installation. cmdkey.exe provides a way to use alternative credentials, but these won't always work well with certain MMC Snap-ins.

Use WinRM / WinRS, RDP or SSH in multi-domain and workgroup environments.
Remotely managing your Server Core using Compmgmt.msc

The best management tools available for Windows Server are Microsoft’s own Microsoft Management Console (MMC) Snap-Ins, which have been around since the Windows NT4 Option pack and have been improved in functionality ever since. While the functionality of version 3.0 of the Microsoft Management Console (MMC) framework has increased to embrace Windows Server 2008, there are some pitfalls in remotely managing your Server Core installations using the most common Snap-Ins.

Computer Management

The most common remote management scenarios will be based on the Snap-Ins contained in the Computer Management Microsoft Management Console Snap-In (compmgmt.msc) on Windows Vista and Windows Server 2008. These Snap-Ins are:

- System Tools
  - Task Scheduler (taskschd.msc)
  - Event Viewer (eventvwr.msc)
  - Shared Folders (fsmgmt.msc)
  - Local Users and Groups (lusrmgr.msc)
  - Reliability and Performance (perfmon.msc)
  - Device Manager (devmgmt.msc)

- Storage
  - Disk Management (diskmgmt.msc)

- Services and Applications
  - Services (services.msc)
  - WMI Control (wmimgmt.msc)

Most of the Computer Management Tools can be easily accessed on Server Core by simply opening up the firewall to allow Remote Management and redirecting the Computer Management Microsoft Management Console Snap-In (compmgmt.msc) to your Server Core server.

The command to use on the console of your Server Core box should look something like:

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

This will open up the three rules in the group that allow Remote Management.

1. System Tools

The following five MMC Snap-Ins in the System Tools folder inside the Computer Management Microsoft Management Console Snap-In (compmgmt.msc) are now unlocked:

- Task Scheduler (taskschd.msc)
- Event viewer (more on that below) (eventvwr.msc)
- Shared Folders (fsmgmt.msc)
- Performance Monitor (perfmon.msc)
- Device Manager (devmgmt.msc)
Reliability Monitor
The firewall rule will enable you to use the System Tools inside the Computer Management Microsoft Management Console Snap-In (compmgmt.msc). There's one exception though: the Reliability Monitor in the Reliability and Performance folder. (perfmon.msc) This tool is not available in Server Core and thus cannot be managed remotely. The Performance Monitor works though.

Event Viewer
A little while ago I wrote a blogpost on handling events in Server Core. Using the Event Viewer Snap-In (eventvwr.msc) is considerably more useful in most scenarios compared to using wevtutil.exe. Event Log Subscriptions and Event Forwarding might prove even more useful. In the mentioned blogpost I explained how to configure WinRM and the Event Viewer MMC Snap-In (eventvwr.msc) in a Windows Vista or Windows Server 2008 box to use these features.

Device Manager
By default the Device Manager (devmgmt.msc) is read-only. You can circumvent this default behavior by enabling remote management of the PnP interface through policies. This policy setting is located underneath Computer Configuration, Administrative Templates, System, Device Installation. It is called Allow remote access to the PnP interface.

You can change this policy by redirecting your Group Policy Editor (gpedit.msc) to your Server Core box (as described here) or using Group Policies within Active Directory. Don't forget to issue the gpupdate command on the console of your Server Core box when you want the policy to take effect promptly.

2. Storage
Disk Management (diskmgmt.msc) is a remote management item requiring a little tinkering. By default it won't work unless both machines are part of the same domain, (take a look at the Logon Considerations below for a workaround) both machines have the Remote Disk Management exception enabled for the Windows Firewall and the box to remotely manage has the Virtual Disk service started. (by default this service is set to start manual on Server Core)

Configuring the Virtual Disk Service
Because the Virtual Disk service is set to start manual on Server Core installations of Windows Server 2008, you need to set the service to start automatically and after that start the service. You can accomplish this using the following two commands from the console of your Server Core box:

```
sc config vds start=auto
net start vds
```

Enabling exceptions in the firewalls
Enabling the service is not enough. You need to enable the Remote Disk Management exception on the Server Core machine and the machine you're managing your Server Core from. That's right: both boxes.
Since NetSh is available on Windows Vista, full installations of Windows Server 2008 and Server Core installations of Windows Server 2008 you can simply type the following command on the managing box and the manageable box:

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

Now you're ready to begin using the Disk Management portion of the Computer Management MMC Snap-In.

3. Services and Applications

In the context of Server Core management the only two interesting things to mention in the Services and Application folder of Computer Management is the Services MMC Snap-in (services.msc) and the WMI Snap-In (wmimgmt.msc). They work just like the Snap-ins on Full installations of Windows Server 2008.

Delegation Considerations

If delegation is used in your scenario you can actually use the Windows Firewall to finely grained control who from where has access to what. The Windows Firewall in Windows Server 2008 actually has a lot of firewall rules (and rule groups) that are extremely useful for delegation.

These rule groups work, without enabling any other rule group to perform specific management tasks:

- Remote Event Log Management
- Remote Scheduled Task Management
- Remote Service Management
- Windows Firewall Remote Management
- Performance Logs and Alerts

You can enable each of these groups using the command above. For example, to allow Windows Firewall Remote Management, simply type the following command on the console of your Server Core box:

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

Delegation can be extremely useful when combined with the Advanced Firewall security. The latter allows you to filter the usage of the open Management firewall rules based on:

- Allow all connections, or only encrypted connections
- Specify specific programs or services the rule applies (not available for built-in rules)
- Specify specific ports or protocols the rule applies (not available for built-in rules)
- Specify which local IP address the rule applies to
- Specify which firewall profile (domain, private, local) the rule applies to
- Specify which type of connections (LAN, Wireless, Remote access) the rule applies to
• Specify which remote IP address (range) the rule applies to
• Only allow connections from specific computers
• Only allow connections from specific users

Logon Considerations
In certain scenarios you will need to provide additional credentials. These scenarios might include: (but are not limited to)

• The server to be managed and the client/server from which you want to manage the server are not part of the same domain and there is no trust between the domains.
• The server to be managed and the client/server from which you want to manage the server are part of a workgroup configuration
• You have setup your environment according to the principle of Least Administrative Privilege and use a (non-administrative) user account on your workstation and want to be able to manage your Server Core installation from the workstation.

Using Cmdkey
In first two scenarios you can use Cmdkey.exe. This tools enables you to create, list and delete stored usernames and passwords or credentials. In this case you want to use cmdkey to create a stored username and password for the remote server on the client/server you want to use to remotely manage the server. The command will look something like:

    cmdkey /add:ServerName /user:Servername\administrator /pass:*

    **Note:**
    This command will ensure the entered username and password will be used by default to access the server over the network. In some situations this will pose a security risk.

Alternatively you can use the User Accounts portion of the Control Panel to administer these network passwords. When you open User Accounts, there is a shortcut named Manage your network passwords. When you click the shortcut you can add, remove, and edit network passwords. It also allows for backing up and restoring your list with Stored User Names and Passwords.
**Remotely managing your Server Core using RSAT**

The Remote Server Administration Tools (RSAT) for Windows Vista add remote Server Core administration functionality to Windows Vista and can be used in that manner, when you know your way around them.

The Tools have some rough edges, some missing functionality (by default mostly) and most of them can't even be used with Server Core installations of Windows Server 2008, but they fulfill most remote administration wishes. When used in conjunction with the tools from Computer Management (compmgmt.msc), you too can enjoy the bountiful joys of remote management from the comfort of anywhere you'd like. (in my case: my sunny backyard)

**Installing RSAT**

In order to use the Remote Server Administration Tools (RSAT) you need to download the standalone setup package from the Microsoft Download servers, install the update package and after installation use the Programs and Feature control panel applet to actually install the parts of the Remote Server Administration Tools (RSAT) you'd wish to use.

**Fulfilling system requirements**

In order to run the Remote Server Administration Tools (RSAT) for Windows Vista you'll need a box with Windows Vista Business, Windows Vista Enterprise or Windows Vista Ultimate installed with Service Pack 1 in one of the languages mentioned below.

**Downloading the standalone setup package**

While the Remote Server Administration Tools (RSAT) are available in English since March 24th 2008 only a few days ago Microsoft released the RSAT in the following languages:

<table>
<thead>
<tr>
<th>Language</th>
<th>Code</th>
<th>Package download X86</th>
<th>Package download X64</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chinese - Simplified</td>
<td>zh-CN</td>
<td>Chinese - China</td>
<td>Chinese - China</td>
</tr>
<tr>
<td>Chinese - Hong-Kong</td>
<td>zh-HK</td>
<td>Chinese - Hong Kong SAR</td>
<td>Chinese - Hong Kong SAR</td>
</tr>
<tr>
<td>Chinese - Traditional</td>
<td>zh-TW</td>
<td>Chinese - Taiwan</td>
<td>Chinese - Taiwan</td>
</tr>
<tr>
<td>Czech</td>
<td>cs-CZ</td>
<td>Czech - Czech Republic</td>
<td>Czech - Czech Republic</td>
</tr>
<tr>
<td>Dutch</td>
<td>nl-NL</td>
<td>Dutch - Netherlands</td>
<td>Dutch - Netherlands</td>
</tr>
<tr>
<td>French</td>
<td>fr-FR</td>
<td>French - France</td>
<td>French - France</td>
</tr>
<tr>
<td>German</td>
<td>de-DE</td>
<td>German - Germany</td>
<td>German - Germany</td>
</tr>
<tr>
<td>Hungarian</td>
<td>hu-HU</td>
<td>Hungarian - Hungary</td>
<td>Hungarian - Hungary</td>
</tr>
<tr>
<td>Italian</td>
<td>it-IT</td>
<td>Italian - Italy</td>
<td>Italian - Italy</td>
</tr>
<tr>
<td>Korean</td>
<td>ko-KR</td>
<td>Korean - Korea</td>
<td>Korean - Korea</td>
</tr>
<tr>
<td>Polish</td>
<td>pl-PL</td>
<td>Polish - Poland</td>
<td>Polish - Poland</td>
</tr>
<tr>
<td>Portuguese (Brazil)</td>
<td>pt-BR</td>
<td>Portuguese - Brazil</td>
<td>Portuguese - Brazil</td>
</tr>
</tbody>
</table>
Installing the package
Since you're a server administrator (what else would you need the Remote Server Administration Tools for) I won't bore you with how to double click the standalone setup package. (*.msu file) You all know how to download stuff, relocate it, run it and get through the UAC messages, right? If not, just read this Microsoft Knowledge Base article...

Selecting RSAT features
Once you've installed the package you can begin selecting features from the Remote Server Administration Tools using the Programs and Feature control panel applet. Simply:

1. Go to the Control Panel and select Programs and Features or begin typing Programs and Features in the search field of the Start Menu
2. Select Turn Windows features on or off in the taskpane.
3. Press Continue when you have User Account Control (UAC) enabled
4. Scroll down to Remote Server Administration Tools and select the features corresponding to your remote management wishes:
Selecting Applicable Tools

Server Core offers only a subset of the Roles and Features you can install on a Full Installation of Windows Server 2008. The interesting features in the context of Server Core installations of Windows Server 2008 are:

- Bitlocker Drive Encryption Tools
- Failover Clustering Tools
- Group Policy Management Tools
- Network Load Balancing Tools
- Active Directory Domain Services Tools
  - Active Directory Domain Controller Tools
- Active Directory Lightweight Directory Services Tools
- DHCP Server Tools
- DNS Server Tools
- File Services Tools
  - Distributed File System Tools
  - Share and Storage Management Tools
The other tools in the collection of Remote Server Administration Tools (RSAT) do not apply to Server Core installations of Windows Server 2008.

**Displaying Administrative Tools**

By default a Windows Vista box will not display the Administrative Tools in the Start Menu. When you’re comfortable with the Administrative Tools folder being accessible through the Control Panel and the Search field of the Start Menu just use those.

To display the Administrative Tools in the All Programs list and/or on the Start Menu follow the steps below:

1. Right-click on the Pearl (Start button) and select Properties from the context menu.
2. On the Start Menu tab click the button labeled 'Customize' next to the Start Menu (This menu style gives you easy access to your folders, favorite programs, and search.) radio button.
3. Scroll all the way down in the list.
4. Under the System Administrative Tools header select one of the two other options:
5. Display on the All Programs menu
6. Display on the All Programs menu and the Start menu
7. Press OK to close the Customize Start Menu window
8. Press OK to close the Taskbar and Start Menu Properties window

**Using the Remote Server Administration Tools**

Now that we’ve managed to install the Remote Server Administration Tools package on our Windows Vista management workstation and made the Administrative Tools folder visible where we can reach it with as little as three mouse-clicks, let's dive into the tools I've been using the most in my Server Core environments:

**Active Directory Domain Services Tools**

The Active Directory Domain Services tools in the Role Administration Tools folder apply to the Active Directory Domain Services Role. It consist of two tools. Only the Active Directory Domain Controller Tools are of interest for a Server Core Domain Controller. Once installed you should find these tools in the Administrative Tools folder of your Windows Vista box:

- Active Directory Domains and Trusts (domain.msc)
- Active Directory Sites and Services (dssite.msc)
- Active Directory Users and Computers (dsa.msc)
- ADSI Edit (adsiedit.msc)

These tools work largely as you would expect them to on Windows XP to administer a Windows Server 2003 environment. (You can even use the tools to administer a Windows Server 2003 Active Directory environment!) There are a few exceptions though:
- No Exchange Server Management integration
  - Exchange Server 2003: workaround available
  - Exchange Server 2007: install the Exchange Management Console
- No Terminal Services integration
  (by default, workaround available)
- No Windows Deployment Services integration
  (by default, workaround available)
- No Attribute Editor when managing Windows Server 2003 environment
  (by default, workaround available)

**Group Policy Management Tools**

As you may recall installation of Service Pack 1 for Windows Vista uninstalls the Group Policy Management Console (gpmc.msc). This would have been inexcusable if the Remote Server Administration Tools (RSAT) wouldn't provide a better tool. In fact: The Group Policy Management Tools in the Feature Administration Tools folder for the Remote Server Administration Tools (RSAT) provide the successor to our beloved Group Policy Management Console: Group Policy Management (gpmc.msc)

Although this tool's MMC Snap-In name resembles the Group Policy Management Console it is greatly enhanced with the integration of:

- Starter Group Policy Objects (Starter GPOs)
- Group Policy Preferences
- Group Policy Management Editor (gpme.msc)

The Group Policy Management Tools are a good companion to the Active Directory Domain Services Tools above and can be used in Active Directory environments.

**DNS Server Tools**

When you install the DNS Server Tools from the Role Administration Tools section of the Remote Server Administration Tools (RSAT) you find a new shortcut in your Administrative Tools folder called DNS, which points to dnsmgmt.msc. With this tool you can remotely manage your Server Core DNS Server to your heart's content.

Even though the Remote Management Console isn't all that different to the Management Console in the adminpak.msi for Windows Server 2003 there is one major difference between the DNS Server in Windows Server 2003 and the DNS Server in Windows Server 2008: Full IPv6 integration. The Cable Guy has more information.
DHCP Server Tools
The DHCP Server Tool, called DHCP (dhcpmgmt.msc) also received a IPv6 revamp and is now fully ready to serve both IPv4 and IPv6 addresses to clients asking for them. The tool is actually divided into two different DHCP servers you can run (and stop) independently of each other, create and reconcile scopes independently on and can define classes on independently. (Authorization is still handled on the server level though) 2 DHCP servers for the price of own!

Tip:
When this tool doesn't automatically work in your environment be sure to set the DHCP Server Service to start automatically on your Server Core box. It doesn't do this by default. Use the Services MMC Snap-In remotely (more info here) or type the following commands on the console of your Server Core box

```
sc \\localhost config DHCPServer start= auto
sc start DHCPServer
```

File Services Tools
The File Services Tools folder inside the Remote Server Administration Tools (RSAT) contains a lot of interesting tools. When you add the Distributed File System Tools and Share and Storage Management Tools you receive the following new shortcuts in your Administrative Tools folder:

- DFS Management (dfsmgmt.msc)
- Share and Storage Manager (storagemgmt.msc)

The third tool that's listed in the Remote Server Administration Tools (RSAT) regarding File Services is the File Server Resource Manager. Since you can't install the File Server Resource Manager on a Server Core box, this tool cannot be pointed towards a Server Core file server and is therefor useless for managing Server Core boxes.

Share and storage management
The Share and Storage Management MMC Snap-In (storagemgmt.msc) is tool that is only supported to remotely manage Windows Server 2008 and above (can't be used to manage Vista though) and it provides an overview of all the shares and volumes on the server. The Share and Storage Management MMC Snap-In (storagemgmt.msc) provides much more information than the Shared Folders MMC Snap-In inside Computer Management (compmgmt.msc) does and can be seen as its successor.

It's almost a shame this tool is much harder to get working than the Shared Folders Snap-In. This is because of the Volume Management features which requires the Virtual Disk Service (VDS) to be properly configured and some firewall exceptions to be enabled on both the server and your Windows Vista workstation as pointed out here. To accomplish this, type the following command at both boxes:

```
sc \\localhost config vds start= auto
sc start vds
netsh advfirewall firewall set rule group="Remote Volume Management" new enabled=yes
```
Remotely managing your Server Core using RDP

Not all system administrators feel comfortable on the command line and most system administrators don’t feel comfortable behind the console of their servers in their airconditioned and windowless (no pun intended) datacenters for longer periods of time.

The Remote Desktop is one of the most common used ways to remotely manage Windows Servers nowadays in environments without delegation. Although Server Core doesn't utilize explorer.exe as its shell and doesn't offer the Computer Properties screen to enable Remote Desktop or select users to remote desktop towards the server, Server Core does offer Remote Desktop. The only restriction is you’re only granted one simultaneous Remote Desktop session... (instead of two in the Full installation)

Enabling Remote Desktop

From the command line
To enable Remote Desktop you can use the SCregEdit.wsf script in the System32 subfolder of your Windows folder. Simply type the following commands:

\n
```bash
cd C:\windows\system32
cscript SCregEdit.wsf /AR 0
```

This command will also automatically create the Firewall exception for you. This makes using SCregEdit.wsf the preferred method for enabling Remote Desktop for lazy admins.

Using the registry
The Remote Desktop can also be enabled using the Registry. To enable it change the data for the DWORD registry key fDenyTSConnection from 1 to 0. This key is located in the Registry in the following location:

```
HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server
```

Changing this value will not automatically open up the firewall to allow Remote Desktop traffic. (This might even be what you want if you have high standards) Take a look here to open up the firewall to allow RDP traffic to and from specific subnets and other advanced firewall options.

You need to restart your Server Core box before you can actually use Remote Desktop when you enable it this way. On the other side you can use this method to enable Remote Desktop remotely, which might save you a nice bit of much dreaded exercise when walking up and down to the serverroom.

Using policies
You can also enable Remote Desktop using Group Policy Objects in your Active Directory environment, which might be useful when you want to enable Remote Desktop on loads of Windows Servers.

To enable Remote Desktop using a Group Policy first open the Group Policy. Browse down the Computer Configuration, Administrative Templates, Windows Components until you reach Terminal Services. Double-click the Allows users to connect remotely using Terminal Services setting and select Enabled.
Setting a Group Policy will not automatically or immediately allow you to Remote Desktop to your Server Core box. First of all your Server Core firewall will not allow you to talk to your Server Core box on TCP port 3389 until you open it up. Secondly, you’ll have to wait until the Group Policy Background Refresh has taken place (90 minutes by default) or issue the following command on the console of your Server Core box:

```
gpupdate
```

**Filtering the use of Remote Desktop**

Filtering can be done in two ways:

- On IP addresses using Firewall rules
- On accounts allowed to use Remote Desktop

**On IP addresses**

The first way is based upon the Windows Advanced Firewall. When you use NetSh in the advfirewall context you can specify the remoteip for which you want to enable the Remote Desktop rulegroup. You can use the following command:

```
Netsh advfirewall firewall set rule group="Remote Desktop" new enable=yes remoteip=Context
```

Where *Context* might for instance be localsubnet or any.

**On users**

Configuring Remote Desktop can also be done by selecting users that are allowed to use Remote Desktop. While the Administrator account is allowed by default, you might want to enable other users to use Remote Desktop. This is configured through membership of the Remote Desktop Users local group on the Server Core box. You can add users to the local group using the commandline tool net localgroup or using a Group Policy Object.

Inside a Group Policy Object browse to the Computer Configuration, then Windows Settings and Security Settings, until you reach Restricted Groups. Right-click Restricted Groups and then click Add Group.

Type Remote Desktop Users in the Enter the object names to select text box and then click Check Names. Or, click Advanced, and then click Find Now to list all available groups. Click the Remote Desktop Users group and then click OK. Click OK in the Add Groups dialog box to close it. The Remote Desktop Users Properties dialog box is then displayed. Click Add in the Members of this group section of the dialog box. Don't forget to add Administrator, since a Restricted Group will delete the memberships already in the group. Click OK twice to close the open screens.

**Securing Remote Desktop**

Luckily in Windows Server 2008 Remote Desktop is configured by default to negotiate encryption with the client, so if both support it, it will be used to encrypt the traffic between the server and the administrator's PC, so malicious users won't be able to sniff important keystrokes.
When the people you want to enable to connect to your Server Core box are using previous versions of the Remote Desktop program (older thin clients are notorious) you need to enable Windows Server 2008 to allow these clients. Microsoft introduced a new Credential Security Service Provider (CredSSP) in Windows Vista and Windows Server 2008, but the old clients won’t work with it, because it’s more restrictive. Effectively you enable the old way of User Authentication for Terminal Services. If you can avoid it, it would be best.

To allow older clients and therefore disable CredSSP for Terminal Services, type the following command on the console of your Server Core box:

```bash
cd C:\windows\system32
cscript SCregEdit.wsf /CS 0
```

**Using Remote Desktop**

To use Remote Desktop type the following command on the workstation from which you want to connect to your Server Core installation:

```bash
Mstsc.exe /v:ServerCore
```

Where `ServerCore` can be the NetBIOS name, DNS name or even IP address of your Server Core box.
Remote managing your Server Core using WinRM and WinRS

Windows Remote Management and the Windows Remote Shell are really good tools and can make your life as a system administrator much easier. In the light of Server Core this combination of tools will not generate as much traffic as RDP’ing into a Windows Server 2008 box and can be scheduled. This might make it the ideal solution for day to day system management. (Unfortunately security is a real pain in the behind if both machines aren't in the same Active Directory domain. You'll need to type away some commands to make it work.)

WS-Management is a specification of a SOAP-based protocol for the management of servers, devices, applications and more. The specification is based on DMTF open standards and Internet standards for Web Services and was published in March, 2005 by a group of companies, including AMD, Dell, Intel, Microsoft, Sun MicroSystems and others.

WS-Management provides a common way for systems to access and exchange management information across the IT infrastructure. The specification is quite rich, supporting much more than get/set of simple variables, and in that it is closer to WBEM or Netconf than to SNMP. A mapping of the DMTF-originated Common Information Model into WS-Management was also defined.

One of the most common uses for Windows Remote Management is the Remote Shell, (WinRS) that can be used to execute a program on a remote host.

WinRM

Windows Remote Management is the server part answering the Remote Shell. In Windows Server 2008 it is not enabled by default, which is good from a security point of view.

Determining whether WinRM is configured or not

Windows Remote Management is installed by default on Windows Server 2008 and the WinRM service is set to start (delayed) automatically. The only way to determine whether Windows Remote Management is installed is by examining the output of the following command:

```
WinRM enumerate winrm/config/listener
```

or (shorter, but with the same effect)

```
WinRM e winrm/config/listener
```

When this command has no output, it means no listeners are configured and Windows Remote Management is not configured.

Enabling Windows Remote Management

Using the command line

To enable Windows Remote Shell on a server running a Server Core installation, type the following command at the command prompt of the Server Core box:

```
WinRM quickconfig
```
or (shorter, but with the same effect)

```
WinRM qc
```

The command questions whether you really want to enable Windows Remote Management:

```
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

Make these changes [y/n]?
```

Press y to continue or n to cancel.

This command will perform a couple of actions. First of all it will check whether the Windows Remote Management service is started and set to start automatically. After that it creates listeners for all the network connections to accept Windows Remote Shell connections with default settings. It will also open up port 80 in the Windows Firewall.

If configuration is successful, the following output is displayed:

```
WinRM has been updated for remote management. WinRM service type changed to delayed auto start. WinRM service started. Created a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this machine.
```

**Using Group Policies**

When you place Server Core boxes in a separate Organizational Unit in your Active Directory environment you can manage Windows Remote Management centrally.


Do not forget to also open up TCP 80 on the firewall.

**Default settings**

The default settings of Windows Remote Management might not suit your needs. You can change on which network interfaces Windows Remote Management listens, change the URI's and change whether WinRM will use HTTP (TCP 80) or HTTPS (TCP 443)

While WinRM listens on port 80 by default, it doesn’t mean traffic is unencrypted. Traffic by default is only accepted by WinRM when it is encrypted using the Negotiate or Kerberos SSP. Enabling HTTPS is not a security measure per se. It is needed when you want to use the Windows Remote Shell (WinRS) from a host that is not in the same domain as the Server Core box. (unless you use the trick below)
Windows Remote Shell is enabled by default within Windows Remote Management. For Windows Remote Shell the default settings are:

- Maximum of 5 concurrent users
- Maximum of 2 shells per user
- Maximum of 80MB memory usage per shell
- Maximum of 5 processes per shell

**Disabling Windows Remote Management**
To disable Windows Remote Management you need to remove the listener. The following command can be used:

```
WinRM delete winrm/config/listener?IPAdress=*+Transport=HTTP
```

**WinRS**
On another computer, at a command prompt, use WinRS.exe to run commands on a server running a Server Core installation. For example, type:

```
winrs -r:ServerName cmd.exe
```

Where `ServerName` is the name of the server running a Server Core installation with Windows Remote Management. This will result in a remote prompt where you can happily type away your commands.

**Tips and tricks**

**Workaround for non-domain situations**
When the Server Core box and the remote host are not members of the same domain you can’t connect to the Server Core box using WinRS, because of the built-in security measures. Run the following commands to lower security:

**Note:**
You seriously cripple the built-in security of Windows Server 2008 after running the following commands. Only apply these commands to test situations.

On the Windows server Core box
Run the following commands on the console of the Server Core box to lower security:

```
WinRM set winrm/config/service/auth @{Basic="true"}
WinRM set winrm/config/client @{TrustedHosts="<local>"}
WinRM set winrm/config/client @{TrustedHosts="RemoteHost"}
```

Where `RemoteHost` is the host you want to be able to connect to the server.
**On the remote host**
Start the Command Prompt with elevated privileges. On machines with User Account Control enabled this is easily achieved by pressing the Start button, typing cmd and press CTRL and SHIFT together with Enter to run the command. Run the following commands on the remote host to lower security:

```plaintext
WinRM set winrm/config/service/auth @{Basic="true"}
WinRM set winrm/config/client @{TrustedHosts="<local>"}
WinRM set winrm/config/client @{TrustedHosts="ServerName"}
```

Where `ServerName` is the name of the server running a Server Core installation with Windows Remote Management.

To open the Remote Shell use the following command:

```plaintext
winrs -r:"ServerName": –u:Domain\Username –p:Password cmd.exe
```

Where `Domain\Username` is the name of an account with administrative rights on the server running a Server Core installation with Windows Remote Management and `Password` is the password for the account.

**Trick to get the hostname displayed**
Using the Windows Remote Shell might get confusing pretty fast, since the prompt doesn't show where you're connected to or whether you're connected at all. There are some giveaways though:

- When you type exit your command window doesn't close
- The WinRS command is displayed in the title of your command prompt window

This can become very painful when you decide to shutdown a server and turn off the wrong server accidentally...

Arlindo Alves, the Belgian IT Pro Evangelist, has a good trick to display some extra information on the command prompt, which also works when using the Windows Remote Shell. I suggest you read his blog post on it. It entails adding an Extended String value named prompt to the following registry key:

```
HKLM\System\CurrentControlSet\Control\Session Manager\Environment
```

He fills his prompt with all kinds of stuff (which doesn't seem to get passed through completely using WinRS) but I simply add the following data to the value:

```
[IdentificationString]$s$g
```

Where `IdentificationString` is an identification string that accurately describes what the server is all about. (which in my case differs from the hostname)
Remotely managing your Server Core using SSH

Since Microsoft has been criticized by Linux adepts for its inability to modularize Windows like Linux and Server Core installations are pretty much the first incarnation of Microsoft's vision in this territory, let's go a little further into uncharted territory and start managing Server Core using PuTTY over SSH. SSH is the default management method for Linux boxes.

**Tools**

I'll be setting up OpenSSH on a x86 version of a Server Core installation of Windows Server 2008 Standard. To install it I'll simply use Cygwin package 1.5.25-15, which can be downloaded from the Cygwin Website. On the client level I'll use PuTTY 0.60, which can be downloaded from the PuTTY Download Page for free.

In the table below are the versions of the tools used:

<table>
<thead>
<tr>
<th>Tool</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cygwin installer</td>
<td>2.573.2.2</td>
</tr>
<tr>
<td>OpenSSH</td>
<td>5.1p1-3</td>
</tr>
<tr>
<td>DiffUtils</td>
<td>2.8.7-1</td>
</tr>
<tr>
<td>PuTTY</td>
<td>0.60</td>
</tr>
</tbody>
</table>

**Server side configuration**

**Download Cygwin**

To install Cygwin you can use the Installation Wizard (setup.exe) from the website. It weighs 405 KB.

This Installation Wizard was previously available as a FTP download, but recently the Cygwin people decided to stick with website hosting only, allowing the program to retrieve the files and packages it needs using FTP. This step makes installing Cygwin on a Server Core installation slightly more difficult, because you now need a browser to download it.

On the other hand it offers the ability to combine the Installation Wizard and the necessary packages on a different host than your Server Core installation, which might be useful when your Server Core box can't access the Internet or you want to deploy loads of SSH servers to manage your Server Core boxes and don't want to strain your Internet connection too much.

**Get the Cygwin installer on your Server Core**

After you've downloaded the Cygwin Installation Wizard you need to transfer the file to your Server Core installation. You can use various methods, including: (but not limited to)

- Copying the file to a USB or other portable rewritable media
- Burn the file onto a CD or DVD media
- Convert the file to a ISO file and mount it on your Server Core box (using DRAC/ILO)
• Place the file on a SMB File Share and map a drive to it on your Server Core box
• Place the file on an internally available FTP Server and grab it using ftp.exe.

**Run the software installer**

To start the installation change your prompt to the directory where setup.exe resides and type setup.exe. The Installation Wizard should appear. Perform the following steps:

• In the Cygwin Net Release Setup Program screen, which serves as a Welcome screen press Next >.
• In the Choose a Download Source select the Install from Internet (downloaded files will be kept for future re-use) option. When you have previously used the Download without Installing option to leech the 16 MB needed for OpenSSH and other utilities and distributed these files with setup.exe you can specify the Install from Local Directory option. Press Next >.
• In the Select Root Install Directory screen type a directory to install Cygwin in, or accept the default location of C:\Cygwin. Under Install For verify All Users is selected. Under Default Text File Type verify Unix / binary is selected.
• Press Next > when done.
• When you’ve selected to Install from Internet (step 2) specify the Local Package Directory on the Select Local Package Directory screen where you want the Cygwin Installation Wizard to store the installation files it downloads. Afterwards press Next >.
• In the Select Your Internet Connection screen choose from Direct Connection and Use HTTP/FTP Proxy to best describe your connection to the Internet and press Next >.
• In the Choose A Download Site screen select a mirror site close to your location to download the remainder of the setup files from. Check the Cygwin Mirror Sites page for more information on the mirrors. Press Next > when done.
• In the Select Packages screen open the Net category and scroll down until you reach the openssh: The OpenSSH Server a... entry. Click on the Skip button thingy in the second column to change it. OpenSSL will be installed automatically as well, which is fine. Also open the Utils category and scroll down until you reach the Diffutils. Install these. Press Next >.
• When you receive a window stating you also need to download a couple of packages your packages depend on (dependencies) choose the recommended setting to install these and press Next >.
• Wait for the Cygwin Installation Wizard to download the necessary packages. Wait a little longer for the Cygwin Installation Wizard to install the programs. In the Create Icons screen deselect the Create icon on Desktop and Add icon to Start Menu options. We won’t be needing them. Press Finish when done.

I noticed my Server Core box downloaded 16,5 MB from the mirror website.
Configure OpenSSH
Type the following command in the folder where you installed Cygwin (refer to step 3) and run the following command:

    Cygwin.bat

On the first run this will make Cygwin perform a couple of basic steps regarding the skeleton files before it will display its prompt. On the prompt type the following commands:

    chmod +r /etc/passwd
    chmod +r /etc/group
    chmod 755 /var
    ssh-host-config

Answer the following questions:

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Should privilege separation be used?</td>
<td>yes</td>
</tr>
<tr>
<td>Should this script attempt to create a new local account 'sshd'?</td>
<td>yes</td>
</tr>
<tr>
<td>Do you want to install sshd as a service?</td>
<td>yes</td>
</tr>
<tr>
<td>Enter the value of CYGWIN for the deamon : [ntsec]</td>
<td>ntsec</td>
</tr>
<tr>
<td>Do you want to use different name?</td>
<td>no</td>
</tr>
<tr>
<td>Create new privileged user account 'cyg_server'?</td>
<td>yes</td>
</tr>
<tr>
<td>Please enter the password:</td>
<td>Any Password*</td>
</tr>
<tr>
<td>Reenter:</td>
<td>Any Password*</td>
</tr>
</tbody>
</table>

* these two values should meet the password complexity requirements.

You should receive the message when done:

    *** Info: Host configuration finished. Have fun!

Create a Firewall exclusion
The Installation Wizard will not create a firewall exception by default, so you need to make one yourself. Use the following command to do so:

    netsh advfirewall firewall add rule name="OpenSSH Server"  protocol=TCP dir=in localport=22 action=allow
Start the OpenSSH Server
The last step on the server is to start the Open SSH Server, by typing:

```
et start sshd
```

**Note:**
The CYGWIN sshd service is set to start automatically every time you reboot. You will only have to type the above command once. Alternatively to typing the command you could restart your Server Core box.

Client side configuration
On the intended client download a SSH client. PuTTY is by far the most popular SSH client. It is a Graphical SSH client for Windows and the best thing it's free.

Installing PuTTY
After installing and configuring OpenSSH on your Server Core installation you might suspect installing PuTTY on Windows is tricky as well, but it isn't. Technically you can't even install PuTTY: you simply download PuTTY and store putty.exe somewhere. (I've placed putty.exe on my desktop for easy access.)

Running PuTTY
To run PuTTY simple double-click it.

**Note:**
When you've downloaded putty.exe with Internet Explorer and stored it on a NTFS formatted drive you might get a Security Warning. To disable this warning right-click on putty.exe and open its properties. At the bottom of the General tab you'll find a button labeled Unblock next to the text "This file came from another computer and might be blocked to help protect this computer." Pressing the Unblock button will remove the text, the button and the Security Warning.

Connecting with PuTTY
To connect to your Server Core installation of Windows Server 2008 type the IP address or DNS name of your Server Core box in the Host Name (or IP address) field of the PuTTY Configuration Screen and press the Open button.

Log in with your credentials and presto!