1 Installing and Setting Up Windows Server 2019

Contents at a Glance

CHAPTER 1: **An Overview of Windows Server 2019** 7

Extra! Extra! Read All About It! Seeing What's New in Windows Server 2019 8

Deciding Which Windows Server 2019 Edition Is Right for You . . . 12

Walking the Walk: Windows Server 2019 User Experiences 13

Seeing What Server Manager Has to Offer 15

Windows Admin Center: Your New Best Friend 17

CHAPTER 2: **Using Boot Diagnostics** 21

Accessing Boot Diagnostics 21

Using a Special Boot Mode 25

Performing a Memory Test 30

Using the Command Prompt. 32

Working with Third-Party Boot Utilities 32

CHAPTER 3: **Performing the Basic Installation** 35

Making Sure You Have What It Takes. 36

Performing a Clean Install 40

Upgrading Windows 43

Performing a Network Install with Windows Deployment Services 46

CHAPTER 4: **Performing Initial Configuration Tasks**. 47

Understanding Default Settings 48

Getting an Overview of the Configuration Process 49

Providing Computer Information 50

Updating Windows Server 2019 60

Customizing Windows Server 2019 64

Configuring Startup Options with BCDEdit 70

IN THIS CHAPTER

- » Getting an overview of the features new to Windows Server 2019
- » Making sense of the Windows Server 2019 editions
- » Looking at the different Windows Server 2019 user experiences
- » Recognizing the benefits of Server Manager
- » Working with the Windows Admin Center

Chapter 1
An Overview of Windows Server 2019

Windows Server 2019 is the latest version of Microsoft's flagship server operating system. This chapter has something for everyone. If you're already familiar with Windows Server, I discuss the new features that Windows Server 2019 brings to the table. If you haven't worked with Microsoft Server operating systems much before, you'll appreciate the information on the editions and user experiences that you can use, depending on your needs.

Extra! Extra! Read All About It! Seeing What's New in Windows Server 2019

With each new version of Windows Server, Microsoft introduces new and innovative technologies to improve administration or add needed functionality. Here are some of the new features in Windows Server 2019:

- **App Compatibility Feature on Demand (FoD) for Server Core:** The App Compatibility FoD package includes a set of binaries that improve compatibility for applications that require some of the graphical tools that haven't historically been available with Server Core. To use these capabilities, you need to install the FoD package from Microsoft; it's available as an optional package download from the Microsoft Evaluation Downloads page (`www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2019`) in the form of an ISO image file. Just search for Windows Server Core Features on Demand, and ensure that you download the same version of FoD as the version of Server Core that you're going to install or you've already installed. All you need to do is copy the ISO image file to the local storage on the server or to a shared storage location. Then you can use PowerShell to mount the ISO with the `Mount-DiskImage` command. This will give you the ability to use Internet Explorer 11, Event Viewer, Performance Monitor, Resource Monitor, Device Manager, Microsoft Management Console (MMC), File Explorer, Windows PowerShell ISE, and Failover Cluster Manager, and it will add support for SQL Server Management Studio.
- **Improvements to clustering:** Several improvements have been made in regards to clustering in Windows Server 2019:
  - Cluster Sets is a new technology that allow you to group multiple clusters. These clusters may just be compute or storage, or they may be hyperconverged (both storage and compute) clusters. This allows the movement of virtual machines (VMs) across different clusters, which, in turn, allows you to do maintenance tasks with little to no impact to the uptime of the VMs. To use the Cluster Sets feature, you create a VM and point it to a *unified namespace* (a name that is shared and provides access across multiple storage systems) for the cluster set. From there, the VM will be assigned to a cluster, and the cluster will assign it to a specific node.
  - File Share Witness is a file share that can be used to reach quorum in a clustering scenario. It received two enhancements in Windows Server 2019. The first enhancement enables the Failover Cluster Manager to block the creation of a file share witness if Distributed File System (DFS) is being used. An error message will also be displayed letting you know that this is not supported because it can cause stability issues in your cluster if your file share witness is put on a DFS share.

  The second enhancement to File Share Witness enables you to use a file share witness in scenarios that were not previously supported — for example, when you have poor Internet connections to remote locations, when you don't have shared drives, when you don't have a domain controller connection (for instance in a demilitarized zone [DMZ]), or in a workgroup or cross-domain cluster where there is no Active Directory–based cluster name.

TECHNICAL STUFF

  The DMZ is the area where you'll typically locate public-facing systems like web servers. It's essentially a lower-trust network being exposed to an untrusted network, like the Internet.

  - Moving clusters between domains no longer results in the cluster being destroyed. Two new PowerShell cmdlets were created that allow you to move a cluster from one domain to another domain.

  - Failover Clustering will no longer use NT LAN Manager (NTLM) for authentication. Instead, you'll use Kerberos and certificates to manage authentication on your failover clusters.

- **Improvements to containers:** You may be aware that containers were added in Windows Server 2016. The underlying technology used on Windows Server for containers is Docker. (To learn more about containers and Docker, turn to Book 8.)

  New container capabilities have been added in Windows Server 2019:

  - You can use group managed service accounts (gMSA) to access network resources. The container's host name doesn't need to be the same as the gMSA. You can use the gMSA on both Windows and Hyper-V isolated containers.

  - Applications that have specific communications needs such as support for Serial Peripheral Interface (SPI), Inter-Integrated Circuit (I^{2}C), general-purpose input/output (GPIO), and universal asynchronous receiver-transmitter/communication (UART/COM) port can now be containerized. Host Device Access allows you to assign a simple bus to Windows Server containers. This is especially useful for Internet of Things (IoT) devices like sensors and other peripheral devices.

  - A third container image has been created that resolves application programming interface (API) dependencies that were not available in Server Core.

  - You can now deploy Kubernetes on Windows Server 2019. The master node still needs to be on Linux, but you can configure worker nodes to run on Windows Server. If you're in a Windows-centric shop and you're trying to automate processes, or you're just looking for a container orchestration solution, Kubernetes is a great one to go with. You can find lots of great resources on Kubernetes if it's something you're interested in. Because it's such a large topic, I don't cover it in this book.

- **Congestion control:** Windows Server 2019 includes Low Extra Delay Background Transport (LEDBAT), a network congestion control provider. As the name suggests, LEDBAT can find available network bandwidth for running updates and other network-intensive jobs. When the network is not in use, it can consume all the bandwidth. When the network is in use, it gives up bandwidth for your users and applications so that they don't experience network delays.
- **Security enhancements:** There are three enhancements made to security in Windows Server 2019, expanding on work done in Windows Server 2016 when Windows Defender was officially introduced to the server operating system. These enhancements are as follows:
  - **Windows Defender Advanced Threat Protection (ATP):** Provides visibility to attack activities that target memory and kernel-level areas, as well as the ability to respond to compromised systems. It also aids in forensics investigations and can be used to collect data about the system remotely.
  - **Windows Defender ATP Exploit Guard:** ATP Exploit Guard has similar capabilities to Host Intrusion Prevention Systems (HIPS). It's designed to protect systems from multiple methods of attack, as well as block suspicious behavior that is often seen in compromises involving malware. The exploit protection capability replaces the older Enhanced Mitigation Experience Toolkit (EMET) that was previously offered by Microsoft.
  - **Windows Defender Application Control:** This feature was actually released in Windows Server 2016, but customer feedback provided to Microsoft conveyed that it was difficult to deploy. The version that ships with Windows Server 2019 comes with default policies built in to address some of the hardships that organizations faced. Microsoft applications are allowed to run by default, and executables that are known to be able to bypass code integrity checks are blocked.
- **Software-defined networking (SDN) enhancements:** There were several improvements within the area of SDN:
  - One of the great improvements in security was made by introducing the Encrypted Networks feature, which provides end-to-end encryption and is configured on a per-subnet basis.
  - High-performance gateways allow for the network throughput to be increased up to six times. This is really great for hybrid scenarios where some systems are on-premises and others are in Azure.
  - Access control lists were introduced for the SDN fabric and can be applied automatically. This can improve the security of your SDN.

  - Your Hyper-V hosts can now generate firewall logs in the appropriate format for Azure Network Watcher.
  - IPv6 support was added, including all the security features available with the traditional IPv4 SDN.
  - Virtual network peering was introduced, to give you a method to allow separate virtual networks to communicate.
- **Shielded VMs:** The concept of the shielded VM was introduced in Windows Server 2016. If you want to learn more about shielded VMs, turn to Book 7. Some cool new features available with Windows Server 2019 include the following:
  - The ability to run shielded VMs on systems that have intermittent connectivity to the Host Guardian Service (HGS)
  - The ability to enable VMConnect enhanced session mode and PowerShell Direct to aid in troubleshooting efforts
  - Support for shielded VMs running Linux operating systems
- **Improvements in storage:** Storage Spaces Direct (S2D) was introduced in Windows Server 2016 Datacenter edition. This was a great step in the direction of hyperconverged architectures. It allows for locally attached storage to be leveraged to create highly available and easily scalable software-defined storage. If you want to learn more about this feature and other storage-related topics, check out Book 2, Chapter 2.

  Some of the new features added in Windows Server 2019 include the following:

  - **New PowerShell cmdlets:** These cmdlets simplify volume management and the retrieval of performance history when using Storage Spaces Direct.
  - **Storage Migration Service:** Storage Migration Service allows you to inventory existing servers for their data, security, and network settings, and then migrates those settings to a new modern server using Server Message Block (SMB). This is a *huge* win for you if you have some old file servers hanging around still because it simplifies the migration to a newer and more supported operating system. The new system takes over the identity of the old server — your users won't even know anything happened!
  - **Improvements to Storage Replica:** Storage Replica was initially released in Windows Server 2016 Datacenter edition and allows for synchronous and asynchronous block replication between servers and/or clusters. With Windows Server 2019, Storage Replica has been made available in the Standard edition as well as the Datacenter edition.

WARNING

The Standard edition version of Storage Replica does have a few limitations that don't exist in the Datacenter version. You'll need to see if these limitations will impact your use case; if they will, be sure to install the Datacenter edition.

- **System Insights:** System Insights is a new feature in Windows Server 2019. It utilizes machine learning to analyze performance data and other metrics on each server. This feature can be especially beneficial if you need to do capacity forecasting for compute, storage, and networking needs. System Insights can be managed through PowerShell or through the newer version of Windows Admin Center.
- **Windows Admin Center:** Windows Admin Center can be used to centrally manage your servers, from viewing performance statistics, reviewing logs, and performing configuration tasks to setting up recovery for your local server to Azure by utilizing Azure Site Recovery. Windows Admin Center can now connect to Server 2008 R2, though with limited functionality. Server 2012, 2012R2, 2016, Windows 10, and of course Windows Server 2019 are fully supported. The tool is browser-based and is designed to complement existing tools, but not necessarily replace them.

Deciding Which Windows Server 2019 Edition Is Right for You

Windows Server 2019 comes in three editions: Essentials, Standard, and Datacenter. In the following sections, I walk you through each edition so you can determine which one is right for you.

Essentials

Windows Server 2019 Essentials is tailored for small businesses of 25 users or less. It operates from a single license that is good for up to 25 users and 50 devices. Although Essentials has been extremely popular with small businesses because of its lower cost, there are rumors on the Microsoft blogs that the 2019 version of Essentials may be the last. This is due in part to the low cost of cloud services, which make for a very viable alternative for small businesses that don't want the additional cost of having to support physical hardware.

Note: You won't see Essentials called out in this book specifically. However, many of the topics I cover in this book can be applied to Essentials.

Standard

The Standard edition is ideal for environments with little to no virtualization or when used as a guest operating system. Features in the Standard edition include the following:

- Up to two Hyper-V containers and unlimited Windows containers
- HGS and Nano Server support
- Storage Replica (with some limitations)

Datacenter

The Datacenter edition has the same features as Standard and some additional features:

- Unlimited Hyper-V containers in addition to the unlimited Windows containers
- Storage Replica (full version) and Storage Spaces Direct
- Shielded VM support

Walking the Walk: Windows Server 2019 User Experiences

Windows Server 2019 has two user experiences to choose from. What you use will depend on the workload you're wanting to support, as well as organizational requirements. In this section, I explain the Desktop Experience and the Server Core experience, as well as some pros and cons of each.

Desktop Experience

Desktop Experience is what you would consider to be the standard graphical user interface (GUI) that you may have used in previous versions of the Windows Server operating systems. It allows you to interact with the system with buttons and menus rather than through the command line. Server with Desktop Experience can be managed through Group Policy if attached to an Active Directory domain, and workgroup (non-domain) servers can be managed via local Group Policy.

TIP

Desktop Experience tends to be the easier form of server installation and administration for beginning system administrators, but I highly recommend that you don't rely on the GUI (shown in Figure 1-1). Become a PowerShell ninja instead! PowerShell is a very versatile language and can be used on a variety of systems, including some of the newer versions of Linux.

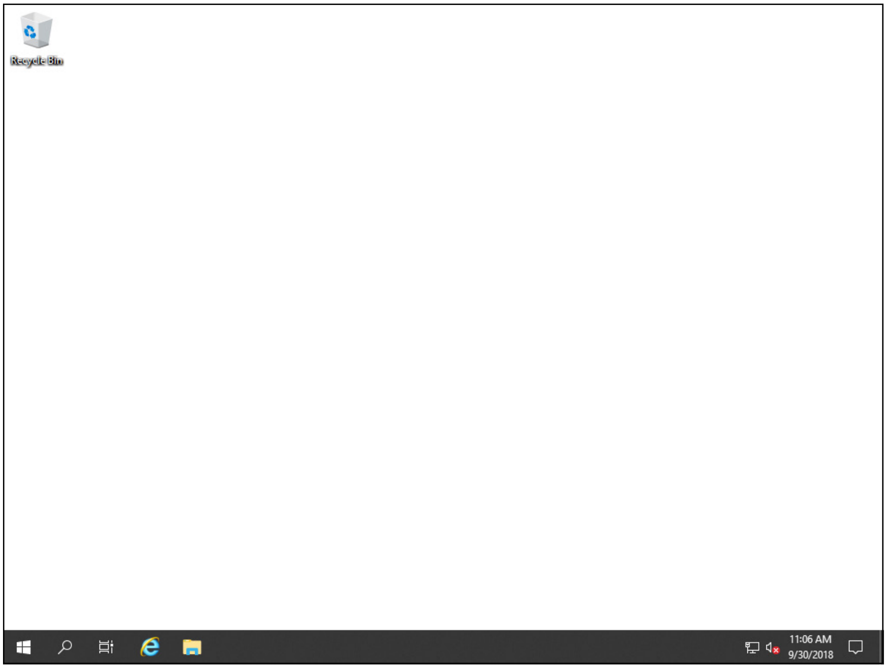
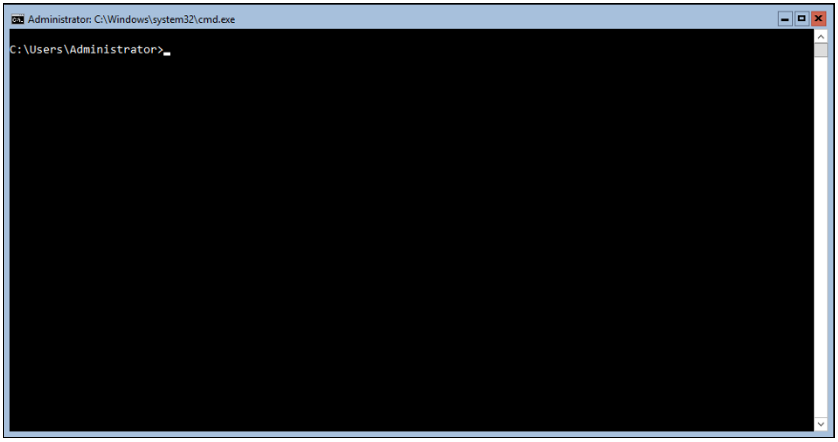


FIGURE 1-1: Server with Desktop Experience.

Server Core

Server Core (shown in Figure 1-2) provides a much simpler interface if you connect to the console. You're greeted by a somewhat familiar-looking command window that prompts you for your username and password. After you've logged in, you get the traditional `C:\` prompt. You can run the traditional command-line commands from this console. Alternatively, by typing **powershell.exe**, you can launch a PowerShell window. Initial configuration is done with the sconfig utility, though it could be done through a PowerShell script or PowerShell Desired State Configuration (DSC). This experience can be managed through Group Policy if attached to an Active Directory domain or through local Group Policy if they're workstation servers.



```
C:\Users\Administrator>_
```

FIGURE 1-2: Server Core.

Nano

Nano provides an even simpler interface and a much more limited console, which is referred to as the Recovery Console. It isn't available through the regular installer on the disc; instead, you have to "build" the image from files available on the disc. Nano has a much smaller footprint, both in disk and compute needs than Desktop Experience or Server Core. Because it has a smaller overall footprint, the attack surface is also reduced. Windows Server Nano 2019 is available only as a container base operating system image, and can only be run as a container on a container host.

Note: You won't really see Nano discussed in depth anywhere in this book because you're far more likely to encounter the Desktop Experience or Server Core installations of Windows Server 2019.

Nano can't be managed through Group Policy. You need to use PowerShell DSC instead if you want to manage Nano at scale. You may be asking why you would even use Nano when it's such a limited version of the operating system. If you need to run container workloads that use .NET, Nano is an excellent candidate because it has been optimized to run .NET Core applications.

Seeing What Server Manager Has to Offer

When you first install Windows Server 2019 and you log in, the first screen that you're greeted with is Server Manager (see Figure 1-3). This screen gives you a central area to do all the configuration tasks you need to do on your server. It presents a handy menu to manage all the roles and features installed on your server as well.

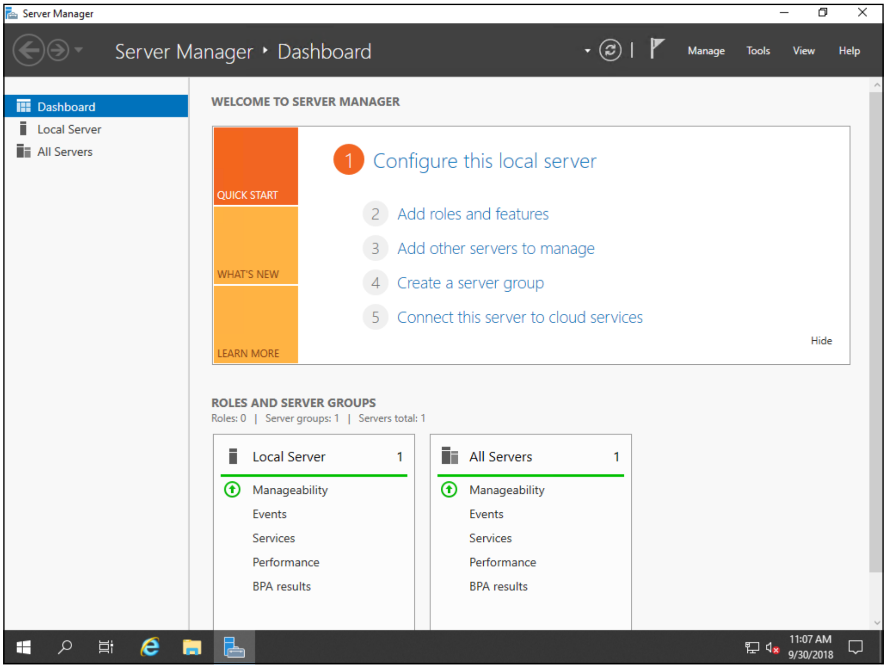


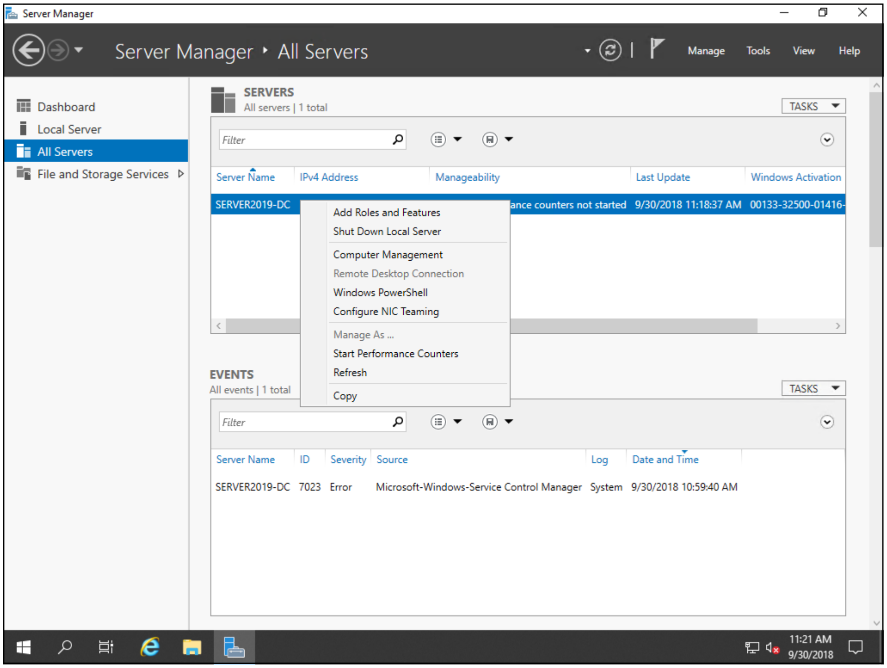
FIGURE 1-3: Server Manager.

Server Manager will allow you to manage remote servers, not just the local server. The remote servers need to be added to Server Manager before they can be managed, and some firewall ports may need to be opened to allow full functionality. After remote servers are added, you can run PowerShell against them and perform basic management tasks like shutting down, connecting via Remote Desktop Protocol (RDP), and so on. You can manage up to 100 remote servers with Server Manager. This number may be lower depending on what you're running on the manage servers. If you're running large workloads, then you may not be able to manage as many.

REMEMBER

Server Manager can be used to manage the same operating system it's installed on, as well as operating systems that are older than what is installed. It can't manage the operating system on a server that is running a newer version of the operating system. For example, a server running Server Manager on Server 2012 R2 can't manage a server running Windows Server 2016.

Figure 1-4 shows some of the options available through the Server Manager menu. You may notice that Remote Desktop Connection is grayed out. This is because I was logged on the server that is in the window.



Server Name	IPv4 Address	Manageability	Last Update	Windows Activation
SERVER2019-DC		ance counters not started	9/30/2018 11:18:37 AM	00133-32500-01416-

Server Name	ID	Severity	Source	Log	Date and Time
SERVER2019-DC	7023	Error	Microsoft-Windows-Service Control Manager	System	9/30/2018 10:59:40 AM

FIGURE 1-4: Managing servers with Server Manager.

Here's a list of some of the more commonly used features of Server Manager:

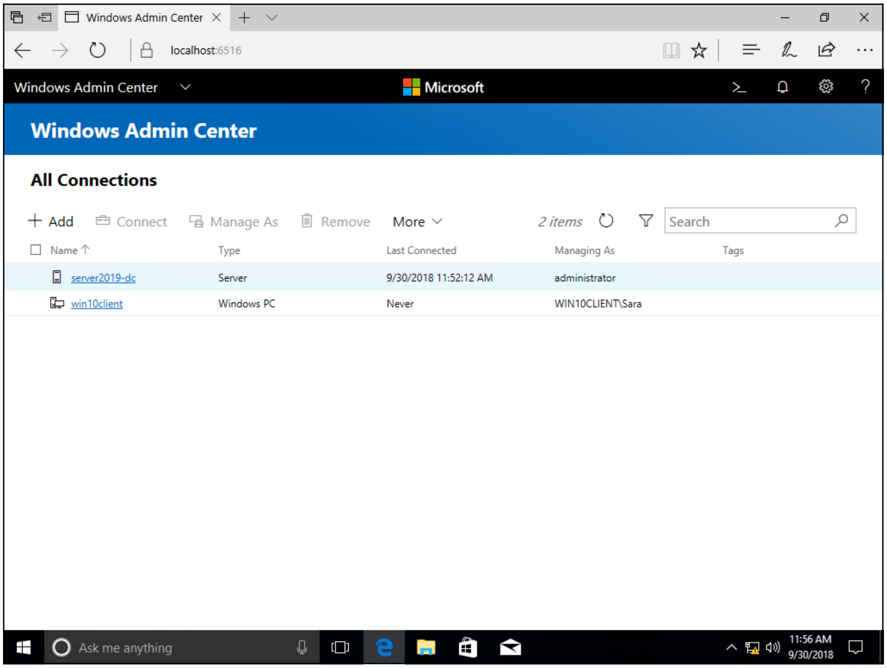
- Managing local and remote servers
- Managing roles and features on servers (To install or remove roles and features, the target system must be running at least Server 2012)
- Starting management tools like Windows PowerShell and MMC snap-ins
- Reviewing events, performance data, and results from the Best Practices Analyzer

Windows Admin Center: Your New Best Friend

Windows Admin Center is a newer server management tool from Microsoft. Microsoft has been investing heavily in Windows Admin Center, and it shows. You can use it to manage your on-premises systems, as well as your systems in Azure. Windows Admin Center is accessible through your browser and allows you to perform nearly all your administrative tasks through the same interface. Best of all, it's free! You just need to pay for the license of the operating system it's running on.

Admin Center has been optimized to administer Windows Server 2019, although it can manage older server operating systems as well. Server 2012 and newer versions feature full support for all functionality, while some limited functionality is provided for Windows Server 2008 R2.

By default, Windows Admin Center uses TCP port 6516, so you need to allow this through your server firewalls depending on how your network is architected. To access the Windows Admin Center Dashboard, you need the hostname of the system that Admin Center is installed on. In Figure 1-5, notice that the address is localhost:6516. That's because I've installed it on a Windows 10 client in Desktop mode. Desktop mode is typically used by a single system administrator, as opposed to Gateway mode, which is available for a larger number of staff.

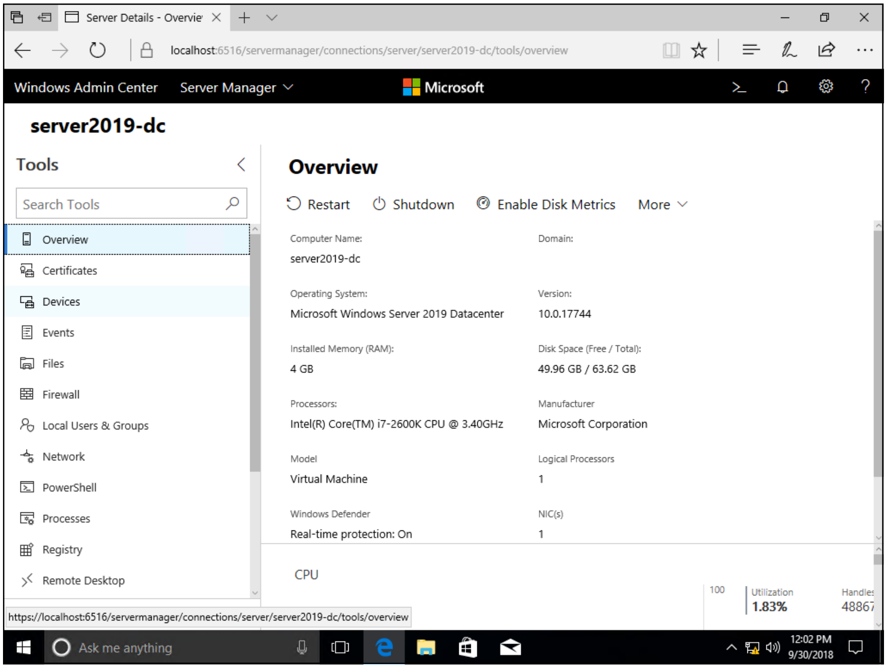


Name	Type	Last Connected	Managing As	Tags
server2019-dc	Server	9/30/2018 11:52:12 AM	administrator	
win10client	Windows PC	Never	WIN10CLIENT\Sara	

FIGURE 1-5: You can see all your connected devices on the All Connections page.

The first screen (refer to Figure 1-5) shows your connected devices.

If you click one of the devices in the list, you get a management view specific to that device. For Figure 1-6, I clicked on server2019-dc. You see an overview of the system as well as some management options. On the left side of the screen, there are many more options you can work from.



server2019-dc

Overview

Computer Name: server2019-dc	Domain:
Operating System: Microsoft Windows Server 2019 Datacenter	Version: 10.0.17744
Installed Memory (RAM): 4 GB	Disk Space (Free / Total): 49.96 GB / 63.62 GB
Processors: Intel(R) Core(TM) i7-2600K CPU @ 3.40GHz	Manufacturer Microsoft Corporation
Model Virtual Machine	Logical Processors 1
Windows Defender Real-time protection: On	NIC(s) 1

CPU

100 Utilization 1.83% Handles 48867

FIGURE 1-6: The Overview page shows, well, an overview of the device you clicked.

Installation of Windows Admin Center is simple. You download the Microsoft Installer (MSI) package from the Microsoft Windows Admin Center website (`www.microsoft.com/en-us/cloud-platform/windows-admin-center`). Before you install it you need to decide if you're simply going to install it on your desktop client or if you want to install it on a server. My recommendation would be to use your desktop if you're just trying it out or if you manage only a few servers. If you're going to use Windows Admin Center in all its glory, install it on a server so that all your administrators can get to it. They'll thank you!

You can install Windows Admin Center on Windows 10 (it needs to have the Fall Anniversary Update 1709) or Windows Server 2016 or newer. To manage older servers — including 2008 R2, 2012, and 2012 R2 — you need to install Windows Management Framework 5.1 on each of those servers.

When you install Windows Admin Center on Windows 10, it's installed in Desktop mode, which means that you access it using `https://localhost:6516`. When Windows Admin Center is installed on a server, it installs in gateway mode which can be accessed with the server name in the URL (for example, `https://servername`).

TECHNICAL STUFF

You can't install Windows Admin Center onto a domain controller. This would be a bad idea anyway! Because Windows Admin Center exposes its services via a web page, it provides a point of attack that would not normally be there.

Some of the coolest features of Windows Admin Center include the following:

- Centralized server management
- Integration with Azure so you can manage on-premises and cloud resources from the same console
- Cluster management tools built into Windows Admin Center
- Showscript, which allows you to see the PowerShell scripts that are being run to do your administrative work

REMEMBER

The only browsers currently supported are Microsoft Edge and Google Chrome. Firefox hasn't been tested, but most of the functionality should work as expected.

IN THIS CHAPTER

- » Figuring out what's going wrong with boot diagnostics
- » Using a special boot mode to bypass server issues
- » Performing a memory test on your server
- » Using the Command Prompt to troubleshoot
- » Troubleshooting with third-party boot utilities

Chapter 2
Using Boot Diagnostics

As a system administrator, you'll get the inevitable call one day about a server that just won't start. Maybe the server is in a continuous boot loop. Maybe the server just hangs. Your mission, should you choose to accept it, is to figure out why the system is having issues starting and then fix the issue.

This chapter discusses basic tools and techniques to troubleshoot issues that are causing your system to not be able to boot properly.

Accessing Boot Diagnostics

The first step to figuring out what's going wrong with your system is to access the boot diagnostic utilities that ship with Windows Server operating systems.

From the DVD

If the server that is having boot issues is a physical server, you can use a DVD or a USB flash drive to access the boot diagnostics menu. It's very rare to have physical media on hand anymore, so, chances are, you'll need to download the ISO file for Windows Server 2019 from the Microsoft website and burn the image to the DVD or USB flash drive.

TECHNICAL STUFF

An ISO file is a duplicate of what's on a physical disc.

After you have the disc ready to go, you need to insert the disc or the USB flash drive into the server and boot from it. You may need to change the boot order on the server so that the boot order will start with the DVD drive or the USB flash drive before the hard drive. You can make this change by accessing the Basic Input/Output System (BIOS). On server systems, this option is available when the system is booting. The key you need to press to access the BIOS will depend on the firmware manufacturer that created the BIOS/UEFI. Some systems simply offer you a boot menu when you press F12, which will allow you to select the DVD drive or USB flash drive for a one-time boot.

When you've figured out how to boot from the DVD or USB flash drive, follow these steps:

1. **Boot from the DVD or USB flash drive.**
2. **When you see the message** `Press any key to boot from CD or DVD`**, press any key.**

   The installation wizard for Windows Server 2019 runs.
3. **On the first screen, click Next.**

   This screen is just asking for language, time and currency format, and keyboard or input method. You can safely accept the defaults.
4. **On the next screen, you see the big Install now button. Don't click that! Instead, look in the lower-left corner for the Repair Your Computer link (see Figure 2-1), and click that.**
5. **On the next screen, click Troubleshoot.**

   This gives you your available options (see Figure 2-2):

   - **System Image Recovery:** Allows you to restore your system from an image created by a backup utility. You'll be asked to choose a target operating system to restore, and then you'll be shown available backups you can use.

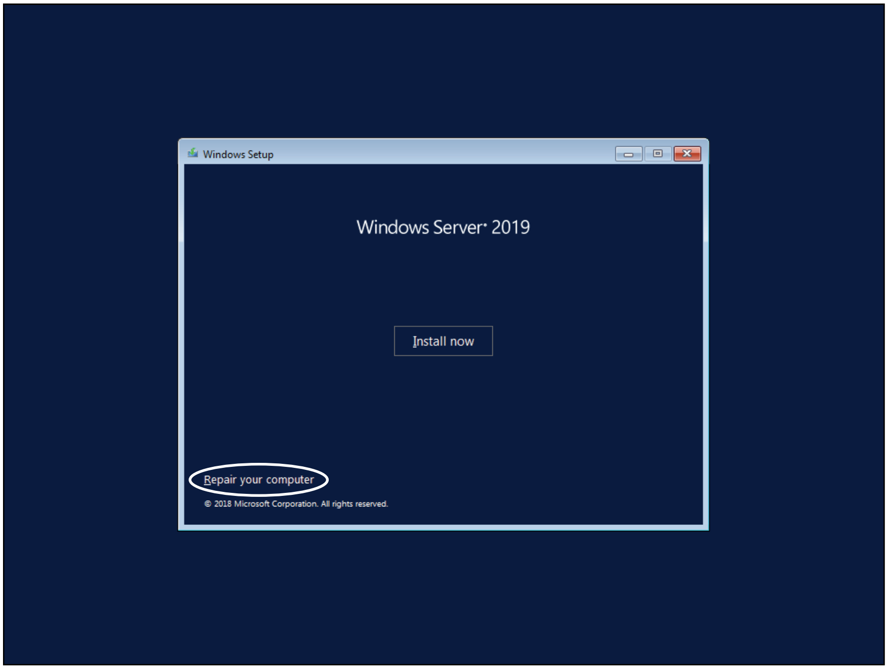
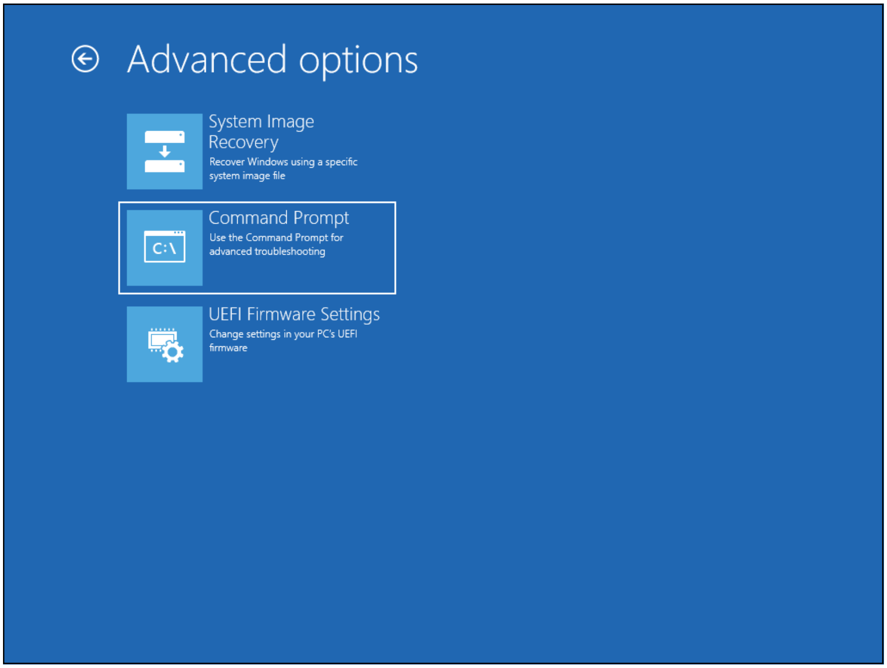


FIGURE 2-1: Look for the Repair Your Computer link in the lower-left corner.



System Image Recovery
Recover Windows using a specific system image file

Command Prompt
Use the Command Prompt for advanced troubleshooting

UEFI Firmware Settings
Change settings in your PC's UEFI firmware

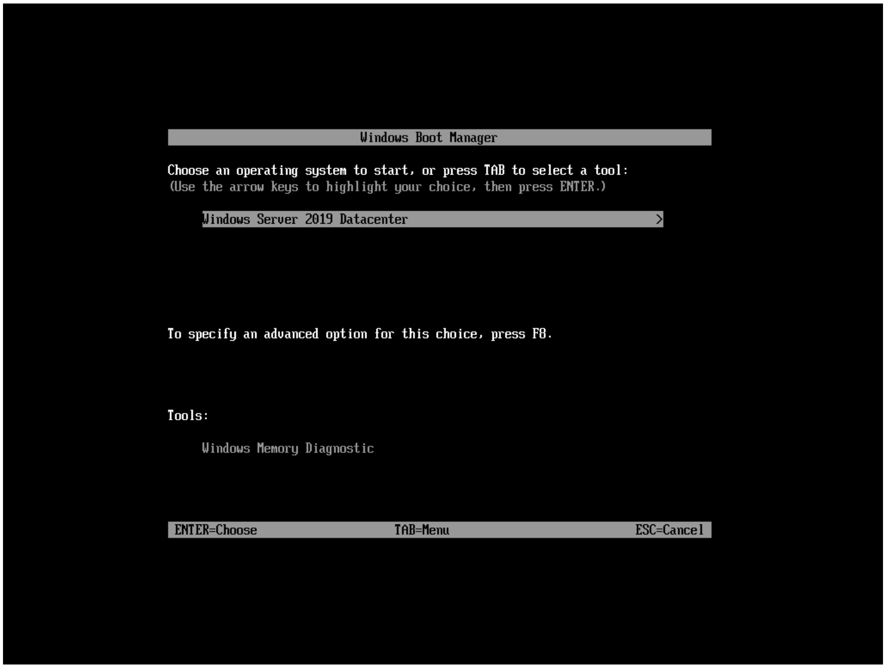
FIGURE 2-2: The Advanced Options screen.

- **Command Prompt:** Allows you to do advanced troubleshooting and is especially helpful if you need to repair boot files. You can use the diskpart utility to work with the drive, and the bootrec command to either rebuild or repair the boot files.
- **UEFI Firmware Settings:** In newer systems, Unified Extensible Firmware Interface (UEFI) has replaced the older BIOS firmware due to the latter's technical limitations and slowness; UEFI is now the preferred firmware to use. In fact, Intel announced that it was planning on dropping support for legacy BIOS firmware in 2020. The UEFI firmware will give you options that vary depending on the system in question, but they include things like enabling or disabling Trusted Platform Module (TPM), using Secure Boot Control, working with Secure Boot Keys, and more.

From the boot menu

In previous versions of the Windows Server operating system, getting to the boot menu meant pressing F8 repeatedly after the system had passed its Power-On Self-Test (POST). As operating systems began to boot more quickly, however, it became more and more difficult to press F8 in time to get to the boot menu. Today, you have a few more options that will get you to the Advanced Boot Options menu:

- If the Windows Server operating system fails several times, it will automatically launch the Advanced Boot Options screen. This is helpful if it never gets to Windows. I don't recommend forcing the operating system to fail several times, however, because you could corrupt the operating system.
- Assuming the system occasionally gets to Windows Server, you can hold down the Shift key while you restart. This gives you the Windows Boot Manager (shown in Figure 2-3). From the Windows Boot Manager, press F8. This will get you to the Advanced Boot Options menu. If you click Repair Your Computer, you get to the smaller menu shown in Figure 2-2.



```
                          Windows Boot Manager

Choose an operating system to start, or press TAB to select a tool:
(Use the arrow keys to highlight your choice, then press ENTER.)

    Windows Server 2019 Datacenter                                >



To specify an advanced option for this choice, press F8.



Tools:

    Windows Memory Diagnostic



ENTER=Choose                    TAB=Menu                  ESC=Cancel
```

FIGURE 2-3: Windows Boot Manager.

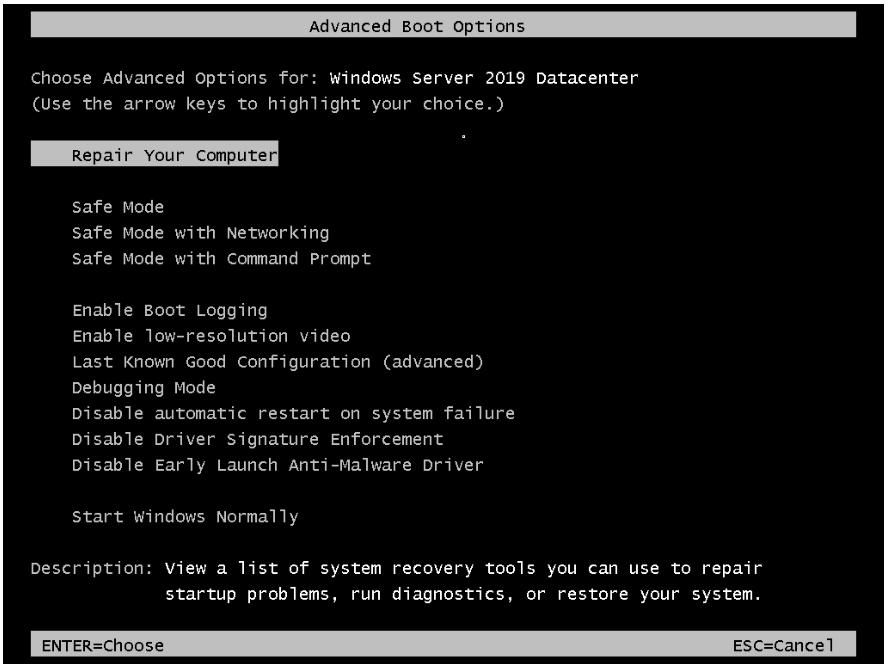
Using a Special Boot Mode

After you've entered the Advanced Boot Options menu, you have quite a few tools that you can choose from to help troubleshoot the system. In the following sections, I walk you through each of the options in the Advanced Boot Options menu (shown in Figure 2-4).

Safe Mode

Safe Mode is almost always my go-to when there are boot issues with a system. Whenever new hardware or software has been installed, or if I suspect that a system may be having issues because of a malware infection, I turn to Safe Mode.

You may be asking, "What is Safe Mode, and why is it such a big deal?" Safe Mode starts Windows with the bare-minimum services and drivers it needs in order to run. Safe Mode is crucial for troubleshooting issues where a bad driver is causing a boot loop. By going into Safe Mode, you can troubleshoot what's wrong with the driver, and uninstall or replace it. Safe Mode is also extremely useful with potential malware infections because the malware may have dependencies it needs to run that are not loaded, which allows you to run malware removal tools and destroy the last bits and pieces of the malicious code from the operating system.



```
                         Advanced Boot Options

Choose Advanced Options for: Windows Server 2019 Datacenter
(Use the arrow keys to highlight your choice.)

    Repair Your Computer

    Safe Mode
    Safe Mode with Networking
    Safe Mode with Command Prompt

    Enable Boot Logging
    Enable low-resolution video
    Last Known Good Configuration (advanced)
    Debugging Mode
    Disable automatic restart on system failure
    Disable Driver Signature Enforcement
    Disable Early Launch Anti-Malware Driver

    Start Windows Normally

Description: View a list of system recovery tools you can use to repair
             startup problems, run diagnostics, or restore your system.

ENTER=Choose                                                  ESC=Cancel
```

FIGURE 2-4: The Advanced Boot Options menu.

The type of Safe Mode I use depends on what I'm needing to accomplish. For instance, if I'm just troubleshooting an issue that I suspect may be related to drivers, most of the time I use regular old Safe Mode. In the following sections, I walk you through the different forms of Safe Mode and why you may want to use each of them.

Safe Mode

This is just regular old Safe Mode. It loads only the basic services and drivers needed for Windows to function and for you to interact with it. Nothing more, nothing less.

In most cases, this regular form of Safe Mode is all you need to troubleshoot and resolve the issue at hand. It has a graphical interface like you're used to seeing in Windows Server, but it has no access to the Internet or other network resources. In essence, it's a stand-alone machine.

Safe Mode with Networking

Safe Mode with Networking is similar to regular Safe Mode, except the system will also load the drivers needed for the network interface card (NIC) to function properly. This is useful if you need to download software from the Internet (for example, drivers or diagnostic software) or over a network share.

Safe Mode with Networking is most useful when you're trying to resolve a software or driver issue. It allows you to download replacement software or replacement drivers while still in Safe Mode. Then you can replace the misbehaving driver or incompatible software with a known good version and then boot successfully.

Safe Mode with Command Prompt

In Safe Mode with Command Prompt, you bypass the Explorer desktop environment. This can be especially useful if the desktop is not displaying properly for whatever reason.

If you like Server Core, you'll like this version of Safe Mode. If you aren't as comfortable with the command window as you would like to be, having a cheat sheet available may help you.

I recommend Safe Mode with Command Prompt when the issue that needs to be fixed has something to do with graphics. The problem may be due to a driver, graphics rendering, or removing a malware infection that relied on graphical components like wallpapers and screensavers.

Enable Boot Logging

If you need to see which drivers were installed as the system started up, you should choose Enable Boot Logging. This will create a file called `ntbtlog.txt`, which lists all the drivers that were installed when the operating system started. The file is stored in your Windows system directory; typically, this will be `C:\WINDOWS`. Incidentally, this is the same list you see flash by on the screen when you boot into Safe Mode.

Enable Low-Resolution Video

This setting is very useful if you're having display issues, most commonly after changing display settings to something your monitor doesn't support. It uses the currently installed video driver but starts with lower resolution (typically 640 x 480) and refresh settings.

Last Known Good Configuration

Last Known Good Configuration is helpful in fixing issues with booting that occur because the Windows Registry has been damaged. Most commonly, this occurs due to user misconfiguration or from updates or patches. When you choose Last Known Good Configuration, the Registry is reverted so that it matches the settings it had the last time the system booted successfully.

WARNING

Any time you use something that modifies the Registry in any way, be extra cautious. There's no way to undo using Last Known Good Configuration. If it doesn't fix the issue, or it makes matters worse, you'll need to restore from a backup.

Directory Services Restore Mode

This option only appears on a server that is a domain controller (and, therefore, it isn't shown in Figure 2-4). Directory Services Restore Mode (DSRM) is a special form of Safe Mode made for domain controllers that allows you to repair or recover an Active Directory database.

TIP

To use this utility you need to know the DSRM password that was set when the domain controller was initially created. If you don't know the password, you can use the ntdsutil tool change the password. You need to have access to the Command Prompt on the system in question to run it.

If all of this is Greek to you, don't worry! I cover Active Directory in depth in Book 2, Chapter 5. For now, think of Active Directory like a special database that stores information on users, computers, sites, and other objects in your network. This database can be crucial to your organization, so knowing how to restore it if it becomes damaged is a very useful skill.

Debugging Mode

If you're a hard-core system administrator and you want to get your feet wet using a kernel debugger, this option is for you!

The *kernel* is a program that is one of the first to run when your server boots (the kernel loads right after the bootloader); it has total control over everything on your system.

Debugging Mode turns on kernel debugging, which allows you to work with the kernel debugger to examine states and processes that are running at the kernel level. This can be very useful for troubleshooting issues with device drivers that cause the infamous blue screen of death (BSOD) and issues with the central processing unit (CPU). You can look at the kernel memory dump on the system that is having the issue, or you can view the kernel memory dump remotely on another system via a serial connection. The information from the Debugging Mode is typically made available over the COM1 port (assuming you have a serial port and it's assigned to COM1).

Disable Automatic Restart on System Failure

Eventually, every system administrator has a system that will continuously try to start, fail, reboot, and then try to start, fail, reboot, and so on. This situation is known as a *boot loop.* If you're experiencing a boot loop on one of your systems, you can get the system to stop automatically restarting by choosing Disable Automatic Restart on System Failure from the Advanced Boot Options menu.

Disabling automatic restart can be very helpful if the system is getting the blue screen of death and you need to get the information being displayed. When the system halts on its next blue screen, you'll have all the time you need to copy down the information.

Disable Driver Signature Enforcement

By choosing the Disable Driver Signature Enforcement option, you're basically telling the system that it's okay to load drivers that aren't digitally signed. Microsoft requires drivers to be digitally signed by default, and will prevent unsigned drivers from running. Microsoft does this because, when a driver is digitally signed, it is seen as being authentic since you can verify from the digital signature that it came from the vendor it claims to be from. Digital signatures also guarantee that the driver has not been altered in any way since it was released from the vendor.

You may be asking, "What is a digital signature?" Digital signatures use a code-signing certificate to encrypt the hash of a file. (Hashes are unique thumbprints — any change to the file will change the hash.). That encrypted hash is then bundled with the certificate and the executable for the driver. When the end user installs the driver, the hash of the file is decrypted with the public key in the certificate. The file gets hashed again on the end user's system, and the new hash is compared to the decrypted hash. If they match, the driver has not been tampered with.

WARNING

If you choose to disable driver signature enforcement, you'll be able to load unsigned drivers. Choose this option at your own risk: You could end up installing malware that presents itself as an unsigned driver.

Disable Early Launch Anti-Malware Driver

Malware that installs after Windows has booted will most likely be seen by the antivirus software that is installed on the system. But the problem is, virus writers began writing malware called *rootkits.* These rootkits can be very difficult to get rid of because they install and execute *before* the operating system has booted. Many of the more sophisticated rootkits began installing drivers that start *really* early in the boot process of the system. This can make them extremely difficult to find and remove.

Microsoft does its best to evolve and respond to threats and prevent them whenever possible. In this case, it came up with the early launch anti-malware (ELAM) driver. Certified antivirus vendors whose products support early launch can get their products' drivers to launch before the Windows boot drivers, which allows them to scan for malicious processes on boot. Pretty cool, right?

But what happens if a legitimate boot driver for Windows gets flagged as malicious? Your server will not boot. So, Microsoft gives you the ability to turn off this feature, by choosing Disable Early Launch Anti-Malware Driver, to allow the boot driver to launch like normal.

WARNING

This feature is a great one to have on, so I would only disable it if you absolutely have to, and then only until the issue is resolved.

Performing a Memory Test

What happens if your server is crashing unexpectedly or throwing blue screens when you least expect it? That can be a difficult question to answer. These symptoms could occur because of corrupted software or because of hardware failure. Memory is a great place to start with your troubleshooting efforts, and Windows Server 2019 includes a built-in memory diagnostic utility, called the Windows Memory Diagnostics Tool.

You can run the Windows Memory Diagnostics Tool by pressing the Windows Key + R, typing **mdsched.exe**, and clicking OK. If you do nothing, the Windows Memory Diagnostics Tool will run in Standard mode. You can interrupt it at any time by pressing F1 to enter the Options screen and change the settings. Your options are as follows (see Figure 2-5):

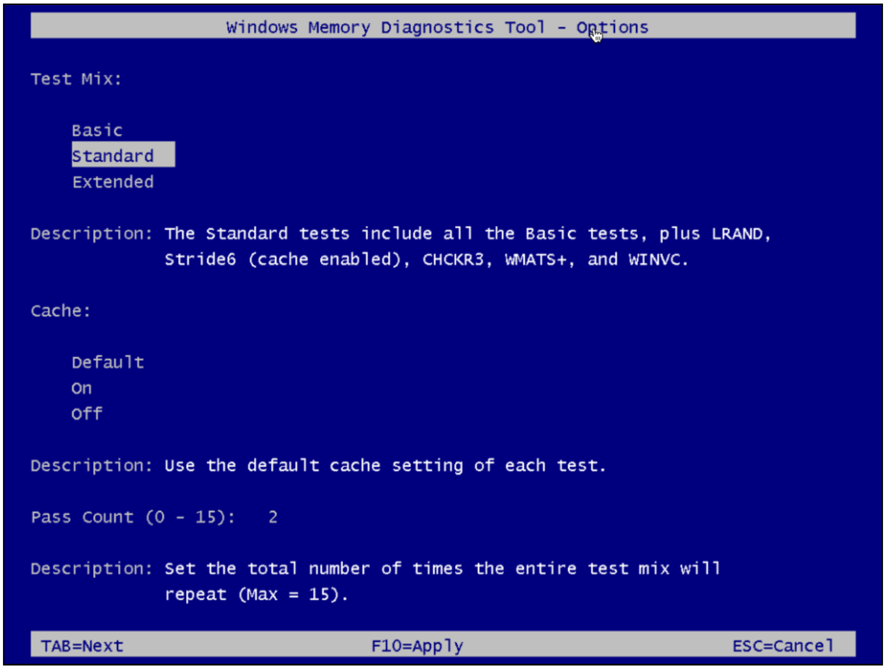
- **Test Mix:** The test mix is the set of tests you want the tool to run:
  - **Basic:** Runs three tests on your memory and is the fastest option.
  - **Standard:** Runs the same tests on your memory as Basic, and adds five additional tests. It takes longer to complete than Basic.
  - **Extended:** Runs the same tests as Standard and adds nine additional tests. This test is the most detailed and takes the longest to complete.

TIP

If you don't know what each of these tests is looking for, I would say that Standard is a good starting point for your tests. Extended will take longer, so if you don't need the extra tests, you may not get any worthwhile information from running them. That said, it won't hurt your server to run either of the three tests.

- **Cache:** Cache sets the cache setting (cache is used to improve the speed of memory access for things that are frequently accessed by the CPU) for each test you're going to run. The cache should be disabled if you're running tests that require direct access to the memory. Your options are as follows:
  - **Default:** In most cases, Default is the appropriate setting. It selects the correct cache setting for the test that is being run.
  - **On:** Forces the cache on for the tests.
  - **Off:** Forces the cache off for the tests.
- **Pass Count (0–15):** Pass count controls how many times the whole test mix you selected will run. If it's set to 5, then the selected test mix will run through its tests five times. The default for this setting is to make two passes.

After you've made your selections, press F10 to apply the settings, and the scan will restart.



```
                 Windows Memory Diagnostics Tool - Options

Test Mix:

    Basic
    Standard
    Extended

Description: The Standard tests include all the Basic tests, plus LRAND,
             Stride6 (cache enabled), CHCKR3, WMATS+, and WINVC.

Cache:

    Default
    On
    Off

Description: Use the default cache setting of each test.

Pass Count (0 - 15):   2

Description: Set the total number of times the entire test mix will
             repeat (Max = 15).

 TAB=Next                         F10=Apply                         ESC=Cancel
```

FIGURE 2-5: Windows Memory Diagnostics Tool options.

Using the Command Prompt

When all else fails, the Command Prompt is always there. I've had to troubleshoot many issues over the years where I was saved because the Command Prompt was available. Corrupted system files? Open the Command Prompt and run `sfc /scannow`. Damaged hard drive perhaps? Open the Command Prompt and type **chkdsk /f /r**.

In Table 2-1, I list some of the most helpful tools that I've used over the years. The majority of these commands need the command window to be running with administrator credentials. To run the Command Prompt as administrator, choose Start ➪ Windows System, right-click Command Prompt, click More, and then select Run as Administrator, or if you can bring up Task Manager, you can choose File ➪ Run New Task and type **cmd.exe**.

TABLE 2-1 Troubleshooting with the Command Prompt

Name	Command	Description
System File Checker	`sfc /scannow`	This utility checks system files to see if they match what's expected by comparing the signature of the system file on the server with the signature of a cached copy of the same file. The cached files are stored in a compressed folder located at `C:\Windows\System32\dllcache`. If a corrupt system file is found, it's replaced.
Check Disk	`chkdsk /f /r`	This utility repairs file system errors and marks bad sectors so that the operating system doesn't use them anymore. The `/f` will tell the utility to fix any issues it finds, and the `/r` will locate the bad areas (sectors) on the disk. This can take a while. Kick it off, and grab a cup of coffee.
Driverquery	`driverquery`	This utility queries the system for all the hardware drivers that are installed on Windows. This can be very helpful if you're running into issues with systems that have similar hardware and you want to know if they have a driver in common.
BCDEdit	`bcdedit`	This utility is covered in depth in Book 1, Chapter 4. For now, just know that it allows you to edit the boot configuration on your Windows server.

Working with Third-Party Boot Utilities

This chapter wouldn't be complete without a brief look at third-party utilities that are designed to help diagnose and resolve boot issues, or to at least assist with recovery. Table 2-2 lists a few of my favorites, along with their cost and a brief description.

TABLE 2-2 **Third-Party Boot Utilities**

Name	Cost	Description
Ultimate Boot CD	Free	This is one of my all-time favorite utilities. It includes multiple diagnostic and recovery tools. To use it, you boot to the disc. It's that easy! Go to www.ultimatebootcd.com for more information.
Trinity Rescue Kit	Free	Trinity Rescue Kit is full of great features, this is also a very useful utility. Go to http://trinityhome.org/Home/index.php?content=TRINITY_RESCUE_KIT____CPR_FOR_YOUR_COMPUTER&front_id=12&lang=en&locale=en for more information.

IN THIS CHAPTER

- » Installing the prerequisites to support a successful installation
- » Doing a clean install of Windows Server 2019
- » Upgrading from a previous version of Windows Server
- » Performing a network install with Windows Deployment Services (WDS)

Chapter 3
Performing the Basic Installation

You've made the decision: You want to install Windows Server 2019. Great! You may be wondering what's next. One of the most important things you can do to ensure a successful installation is make sure that you're meeting all the prerequisites for Windows Server 2019. By ensuring that you have the appropriate hardware to meet the needs of the operating system, you can definitely save yourself some headaches later.

When you've got everything necessary to install Windows Server 2019, you're ready to go. In this chapter, I walk you through how to perform a clean install as well as an upgrade install. I also explain how to do a network install with Windows Deployment Services.

TIP

You should know that you can't change between Server Core and Server with Desktop Experience anymore. This capability was removed in Windows Server 2016, in order to support the newer Windows 10 desktop experience on the server, rather than the older legacy desktop experience you had with Windows Server 2012 R2. If you install Server Core, and then change your mind and decide you actually want Server with Desktop Experience, you need to reinstall it.

Making Sure You Have What It Takes

Microsoft publishes the prerequisites for each of its operating systems. Some of the hardware requirements are independent of which edition of Windows Server you're planning to install; other hardware requirements vary based on whether you're installing Server with Desktop Experience or Server Core.

Windows Server 2019 is available only as a 64-bit operating system; there is no 32-bit version available. When you run the installer, you're presented with options for the Standard edition or Datacenter edition. At the same time, you choose whether you want to install Server Core or Server with Desktop Experience.

WARNING

Where I discuss minimum requirements in this section, it's important to understand that these are the *bare minimums* to successfully install Windows Server 2019. You should *not* expect your server to perform well if you give it the specs listed here. For any real workload, your server should have faster processors, more processor cores, and more memory.

So, what are the absolute bare minimums that you have to meet in order to install Windows Server 2019? Read on.

Central processing unit

The central processing unit (CPU) is the brains of the outfit. It processes instructions made by the program and/or applications. The CPU requirements for Windows Server 2019 are pretty easily met by most modern processors:

- **1.4 GHz 64-bit processor:** Considering that the operating system is an x64 system, it makes sense that the processor must also be an x64 processor. Even a cheap server with a lower-end processor should be able to meet the 1.4 GHz requirement with flying colors.
- **Supports No Execute (NX):** When the NX bit is enabled on certain areas of the memory, the processor will not execute anything in that memory space, which can provide protection against malware. Areas protected by the NX bit usually contain things like processor instructions or data storage.

  TECHNICAL STUFF

  Intel may refer to this technology as XD (short for Execute Disable), while AMD processors refer to it as Enhanced Virus Protection (EVP).
- **Supports Data Execution Prevention (DEP):** DEP provides additional protection against malware that may target memory locations.

VERSION AND EDITION REQUIREMENTS

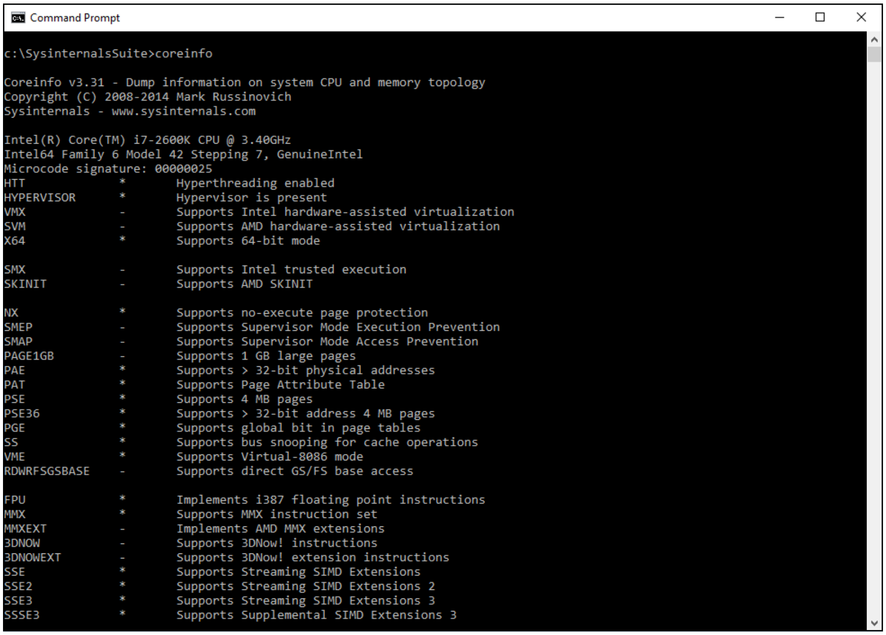
For the most part, there is aren't many differences between the minimum requirements of Server Core and those of Server with Desktop Experience. The one very important exception to that is the amount of random access memory (RAM). The minimum requirement to install Server Core is 512MB of RAM; Server with Desktop Experience needs a minimum of 2GB of RAM.

If you're installing Windows Server 2019 Standard, you should base the hardware specifications on the requirements of the workload you're intending to run. If you choose to run Windows Server 2019 Datacenter, you may want to look at installing better hardware. A great example of a use case for the Datacenter edition is as a Hyper-V host. The Datacenter edition doesn't limit you in terms of how many virtual machines (VMs) you can run. Your hardware will really be the limiting factor. In this use case, you would want multiple cores and a lot of memory.

- **Supports CMPXCHG16b, LAHF/SAHF, and PrefetchW:** These settings are specific to the processor, and there are multiple whitepapers published on the specifics. CMPXCHG16b is an instruction set supported by most modern x86_64 processors. Load AH from Flags (LAHF)/Store AH into Flags (SAHF) is needed to support virtualization. PrefetchW provides improvements to performance when using AMD processors. You don't need to memorize these things — just know that these processor features can speed up execution of tasks and add some additional security features as well.
- **Supports Second Level Address Translation (Extended Page Table [EPT] or Nested Page Table [NPT]):** This feature is especially important if you're planning on running Hyper-V. It improves the performance of the VMs on the system and takes some of the pressure off the hypervisor, which can, in turn, improve hypervisor performance.

TIP

You may be curious how you can tell if your CPU supports these requirements. Microsoft offers a tool that is part of the Sysinternals suite named Coreinfo; this tool tells you what your processor is capable of supporting. You can download Coreinfo for free from the Microsoft website (https://docs.microsoft.com/en-us/sysinternals/downloads/coreinfo). The file you download is a compressed zip file, so you need to extract it first. Then launch a command prompt to run the utility. To run Coreinfo, simply type **coreinfo** into the command window and you get a report of all available and unavailable features. Available features are marked with an asterisk (*), and unavailable features are marked with a hyphen (-), as shown in Figure 3-1.



```
c:\SysinternalsSuite>coreinfo

Coreinfo v3.31 - Dump information on system CPU and memory topology
Copyright (C) 2008-2014 Mark Russinovich
Sysinternals - www.sysinternals.com

Intel(R) Core(TM) i7-2600K CPU @ 3.40GHz
Intel64 Family 6 Model 42 Stepping 7, GenuineIntel
Microcode signature: 00000025
HTT             *       Hyperthreading enabled
HYPERVISOR      *       Hypervisor is present
VMX             -       Supports Intel hardware-assisted virtualization
SVM             -       Supports AMD hardware-assisted virtualization
X64             *       Supports 64-bit mode

SMX             -       Supports Intel trusted execution
SKINIT          -       Supports AMD SKINIT

NX              *       Supports no-execute page protection
SMEP            -       Supports Supervisor Mode Execution Prevention
SMAP            -       Supports Supervisor Mode Access Prevention
PAGE1GB         -       Supports 1 GB large pages
PAE             *       Supports > 32-bit physical addresses
PAT             *       Supports Page Attribute Table
PSE             *       Supports 4 MB pages
PSE36           *       Supports > 32-bit address 4 MB pages
PGE             *       Supports global bit in page tables
SS              *       Supports bus snooping for cache operations
VME             *       Supports Virtual-8086 mode
RDWRFSGSBASE    -       Supports direct GS/FS base access

FPU             *       Implements i387 floating point instructions
MMX             *       Supports MMX instruction set
MMXEXT          -       Implements AMD MMX extensions
3DNOW           -       Supports 3DNow! instructions
3DNOWEXT        -       Supports 3DNow! extension instructions
SSE             *       Supports Streaming SIMD Extensions
SSE2            *       Supports Streaming SIMD Extensions 2
SSE3            *       Supports Streaming SIMD Extensions 3
SSSE3           *       Supports Supplemental SIMD Extensions 3
```

FIGURE 3-1: Running the Coreinfo utility on a Windows system.

Random access memory

Random access memory (RAM) is used by the server to store things that you need to access right now and things that you may need to access in the near future. RAM is much faster than persistent storage, so a server that has lots of RAM will perform far better than a system with very little RAM. As I mention in the "Version and edition requirements" sidebar, earlier in this chapter, Server Core requires a minimum of 512MB of RAM, while Server with Desktop Experience requires a minimum of 2GB of RAM. The RAM must also be Error Correcting Code (ECC)–type memory. ECC-type memory is able to correct single-bit errors (for example, if electrical interference flips a bit in error, using the parity bit can ensure that the data in memory is corrected).

Storage

There's no fancy formula or calculation here. If you want to install Windows Server 2019, you need a minimum of 32GB of hard drive space. Remember that this is the absolute bare minimum to install the operating system. If all you have is 32GB, you won't have room to install anything else. If you're limited on storage space, according to Microsoft, Windows Server Core is approximately 4GB smaller than Windows Server with Desktop Experience.

Network adapter

A server does you no good if you can't access it. The network adapter, also referred to as the network interface card (NIC), gives your server a way to talk on your network. For Windows Server 2019, your network adapter will have to support at least gigabit ethernet. Your network adapters may be *onboard*, meaning that they're a part of the motherboard, or they may be on a NIC, which plugs into a PCI Express slot.

Your network adapter should support the Pre-boot Execution Environment (PXE). This is what the majority of organizations use today to image systems from a central imaging server like Windows Deployment Services or System Center Configuration Manager.

DVD drive

Not all servers come with DVD drives anymore. There are so many more options for installing operating systems like booting from flash drives or booting from the network that many system administrators don't bother with DVDs. That said, if you want to install from a DVD, you need to ensure that you have a DVD drive. The drive can be internal or external.

UEFI-based firmware

Unified Extensible Firmware Interface (UEFI) has replaced the traditional legacy Basic Input/Output System (BIOS) at this point. I highly recommend that you choose UEFI rather than BIOS. It'll be required if you want to use some of the advanced features like secure boot.

Trusted Platform Module

The majority of motherboards come with a Trusted Platform Module (TPM) chip nowadays. If you plan on doing disk encryption with BitLocker, this is a must-have item.

Monitor

It goes without saying that you need to be able to see what's going on with your server when you're installing your operating system. Windows Server 2019 requires a Super Video Graphics Array (SVGA) connection with a minimum of 1024 x 768 screen resolution. You can accomplish this by attaching a physical monitor to the server or by viewing the video stream through a KVM.

TECHNICAL STUFF

KVMs allow you to use one keyboard, monitor (video, in the acronym), and mouse to administer multiple servers. The older KVMs required you to be physically on site to use the keyboard, monitor, and mouse. Modern KVMs allow you to administer your servers remotely through a web service, and they provide similar functionality to what you would get if you physically plugged in a keyboard, monitor, and mouse to your server.

Keyboard and mouse

You can connect a keyboard and mouse directly to the server during imaging or you can present them to the system via a KVM. Either way, you need a keyboard and a mouse of some kind to interact with the system.

Performing a Clean Install

Clean installs are my preferred way to go. By performing a clean install, you're far less likely to run into issues caused by bad drivers, corrupted system files, or misconfigurations. In this section, I walk you through how to do a clean install of Windows Server 2019.

In this section, I assume that you've already booted to whatever media you're going to use for the installation (DVD, flash drive, and so on), and you're on the starting installation screen for Windows Server 2019. If you've done this, you should see a screen that looks like Figure 3-2. From this screen, follow these steps:

1. **Select the appropriate settings for your locality and click Next.**

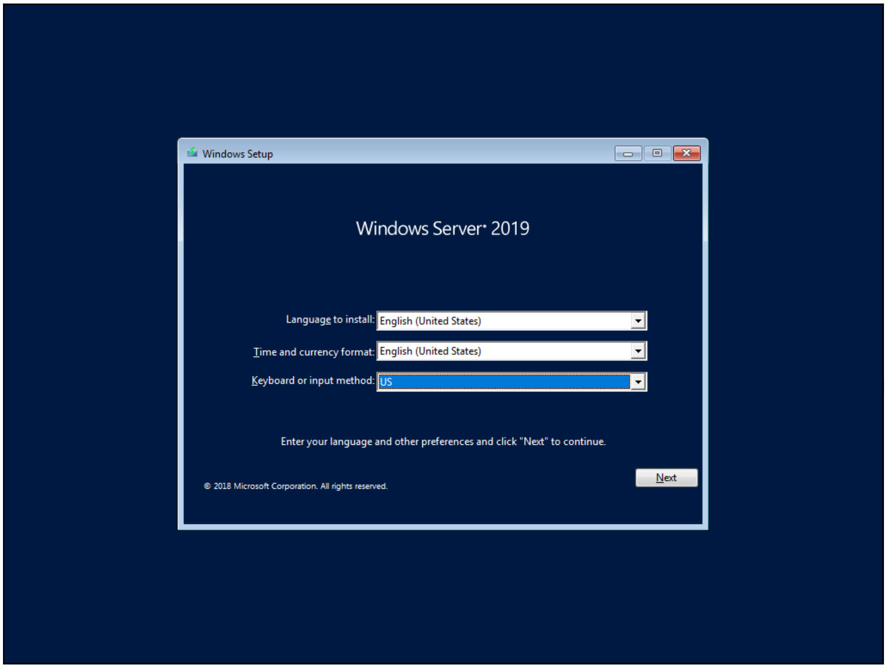
   In my example, I've chosen the following:

   - **Language to Install:** English (United States)
   - **Time and Currency Format:** English (United States)
   - **Keyboard or Input Method:** US

   After you click Next, the screen shown in Figure 3-3 appears.

2. **Click Install Now.**
3. **On the next screen, enter the product key and click Next.**

   If you don't have a license key, click the I Don't Have a Product Key link.



Windows Setup

Windows Server® 2019

Language to install: English (United States)

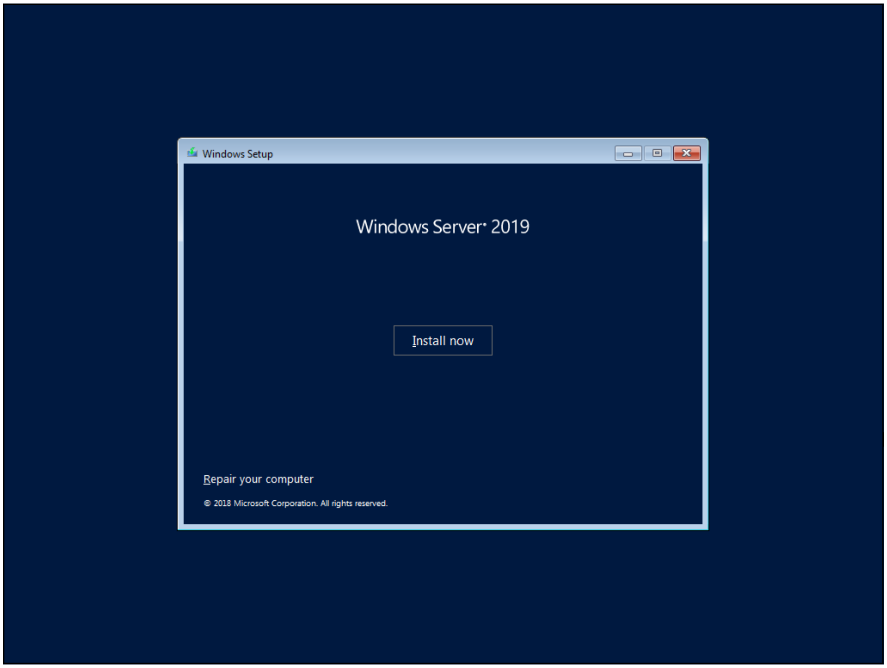
Time and currency format: English (United States)

Keyboard or input method: US

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

© 2018 Microsoft Corporation. All rights reserved.

FIGURE 3-2: The first installation screen for Windows Server 2019.



Windows Setup

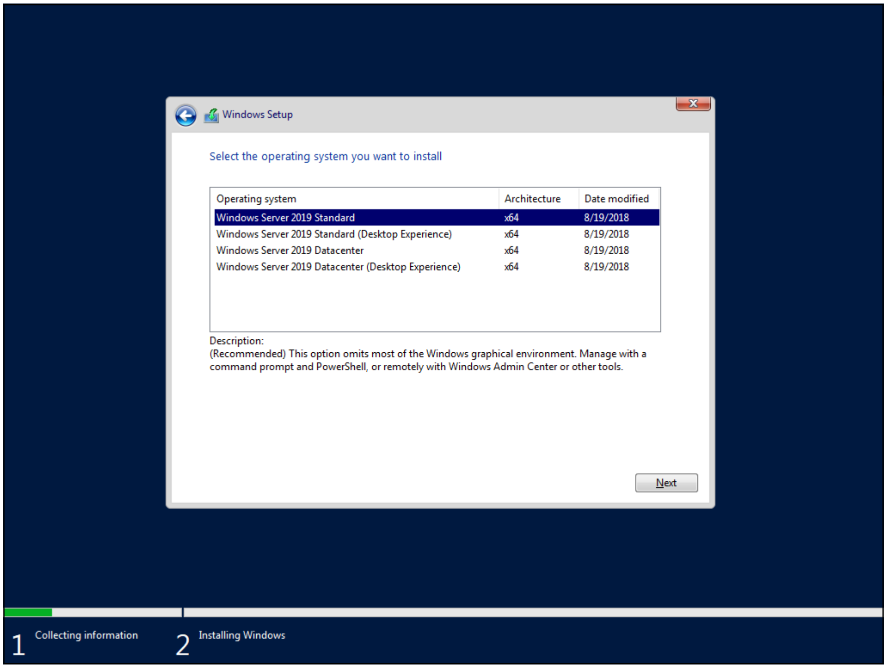
Windows Server® 2019

© 2018 Microsoft Corporation. All rights reserved.

FIGURE 3-3: The Windows Server 2019 Install now button.

4. **On the next screen, choose which version of the operating system you want to install and click Next.**

   The default selection is for Windows Server 2019 Standard (shown in Figure 3-4). If you prefer, you can select Windows Server 2019 Standard (Desktop Experience), Windows Server 2019 Datacenter, or Windows Server 2019 Datacenter (Desktop Experience).



Select the operating system you want to install

Operating system	Architecture	Date modified
Windows Server 2019 Standard	x64	8/19/2018
Windows Server 2019 Standard (Desktop Experience)	x64	8/19/2018
Windows Server 2019 Datacenter	x64	8/19/2018
Windows Server 2019 Datacenter (Desktop Experience)	x64	8/19/2018

Description:
(Recommended) This option omits most of the Windows graphical environment. Manage with a command prompt and PowerShell, or remotely with Windows Admin Center or other tools.

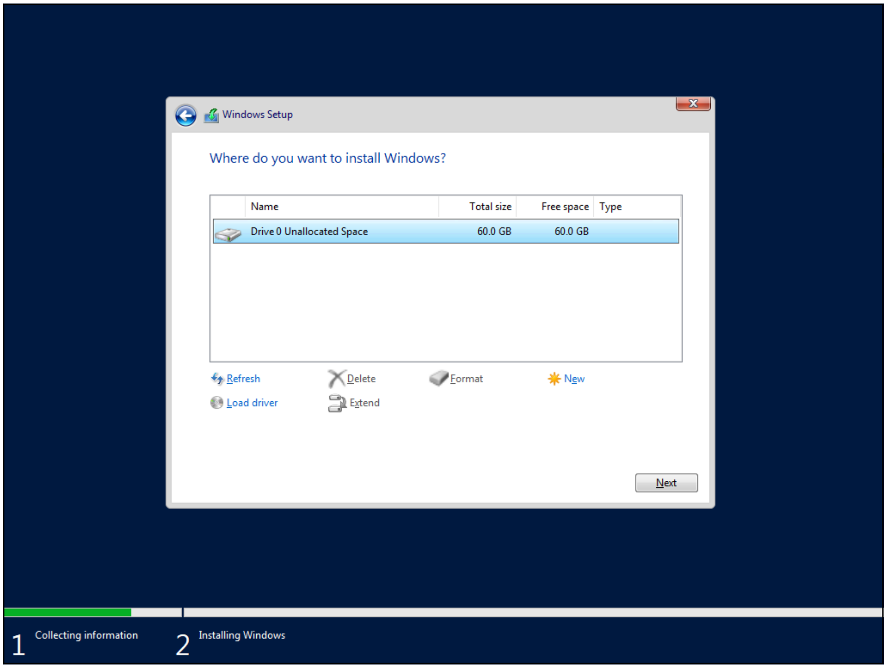
FIGURE 3-4: Choosing your desired edition and experience of Windows Server 2019.

5. **On the next screen, check the I Accept the License Terms box and click Next.**
6. **On the next screen, choose Custom.**

   The other option is for upgrade installations.
7. **On the next screen, select the partition on which you want to install Windows and click Next.**

   In Figure 3-5, you can see that this is Drive 0.

   Windows Server 2019 begins installation and restarts after it's finished. That's when the real fun begins!



Where do you want to install Windows?

	Name	Total size	Free space	Type
	Drive 0 Unallocated Space	60.0 GB	60.0 GB	

FIGURE 3-5: Choose where to install Windows.

Upgrading Windows

When considering an upgrade install, you need to ensure that the version of the operating system you're starting with is able to be upgraded to Windows Server 2019. Table 3-1 tells you which operating systems you can upgrade from, and which edition of Windows Server 2019 you can upgrade to. You also need to check with your application vendors to ensure that the applications on the server are compatible with Windows Server 2019. If they aren't, then you may need to upgrade your applications before you upgrade the server operating system.

TABLE 3-1 Windows Server 2019 Upgrade Compatibility Matrix

If you're running this edition . . .	You can upgrade to these editions . . .
Windows Server 2016 Standard	Windows Server 2019 Standard or Datacenter
Windows Server 2016 Datacenter	Windows Server 2019 Datacenter
Windows Server 2012 R2 Standard	Windows Server 2019 Standard or Datacenter
Windows Server 2012 R2 Datacenter	Windows Server 2019 Datacenter
Windows Server 2012 R2 Essentials	Windows Server 2019 Essentials

TIP

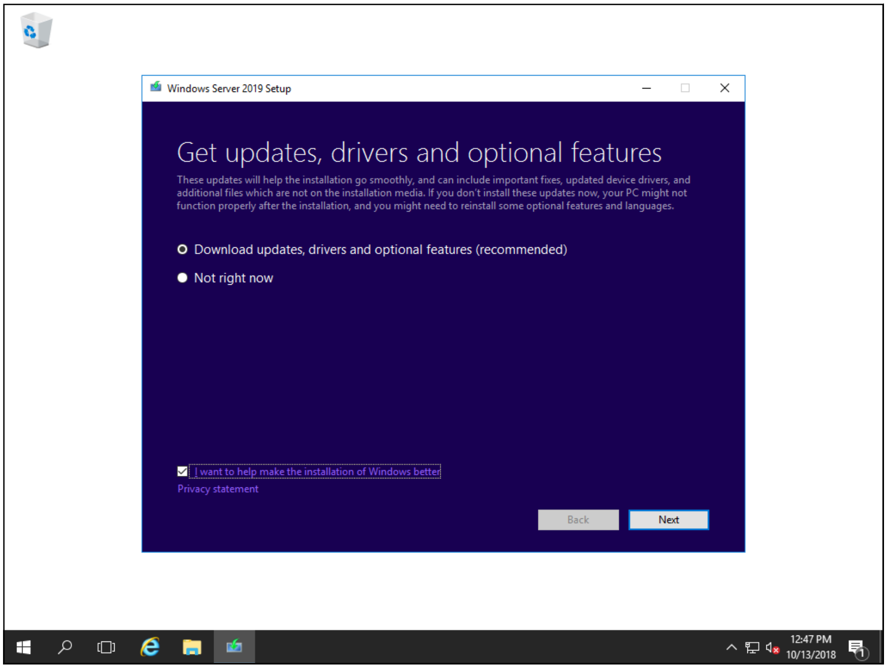
There is no direct upgrade path from Windows Server operating systems that are older than Windows Server 2012 R2. If you're migrating from an older server, start with a clean installation. If you can't use a clean installation, you'll need to upgrade to either Windows Server 2012 R2 or Windows Server 2016 to be able to then upgrade to Windows Server 2019.

After you've verified that you're on a compatible version, you can begin the upgrade install. For this example, I'll start with a Windows Server 2016 Datacenter installation and upgrade it to Windows Server 2019 Datacenter. Follow these steps:

1. **Log in as the administrator on the system that you want to upgrade.**
2. **Insert the disc or other installation media into the system that you're wanting to upgrade, and run** `setup.exe`**.**

   The next screen asks if you want to download updates and drivers ahead of time (see Figure 3-6).
3. **Select the Download Updates, Drivers, and Optional Features radio button and then click Next.**

   The next screen asks you which image you want to install.



Get updates, drivers and optional features

These updates will help the installation go smoothly, and can include important fixes, updated device drivers, and additional files which are not on the installation media. If you don't install these updates now, your PC might not function properly after the installation, and you might need to reinstall some optional features and languages.

◉ Download updates, drivers and optional features (recommended)

○ Not right now

☑ I want to help make the installation of Windows better

FIGURE 3-6: The Get Updates, Drivers, and Optional Features option can simplify your upgrade.

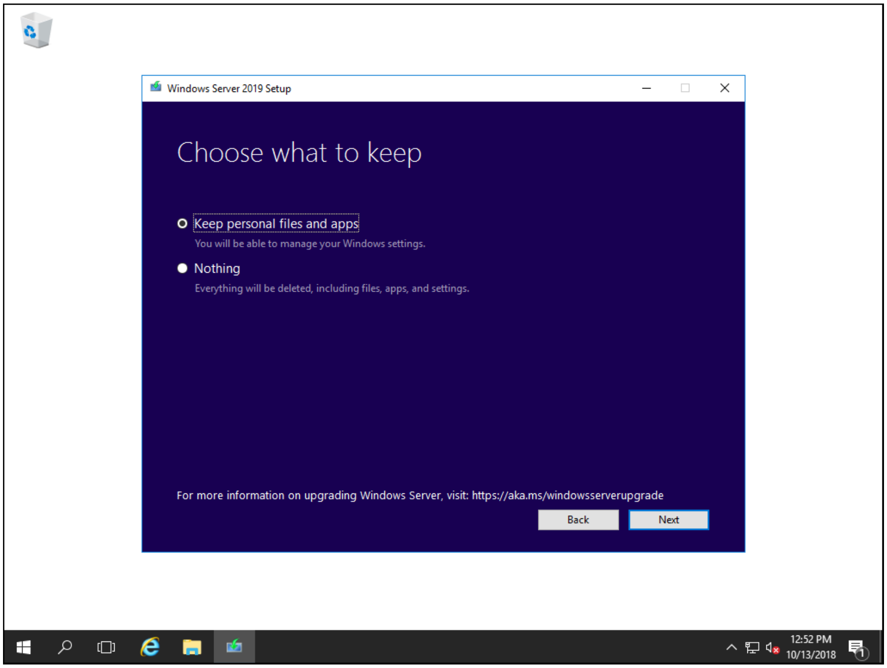
4. **Select Windows Server 2019 Datacenter with Desktop Experience (or whichever version you want) and click Next.**

5. **Read through the license terms if you have time on your hands, and then click Accept.**

   On the next screen, you choose whether to keep your personal files and apps or keep nothing. If you're sticking with the same experience (Core or Desktop), you'll see both options. If you're changing the experience, the only option you'll have will be to keep nothing.

6. **If you have the option, select the Keep Personal Files and Apps radio button, as shown in Figure 3-7, and click Next.**

   The installer fetches any applicable updates and presents you with a summary screen.



Windows Server 2019 Setup

Choose what to keep

◉ Keep personal files and apps

You will be able to manage your Windows settings.

○ Nothing

Everything will be deleted, including files, apps, and settings.

For more information on upgrading Windows Server, visit: https://aka.ms/windowsserverupgrade

FIGURE 3-7: Upgrade options in Windows Server 2019.

7. **If everything looks correct, click Install.**

   The installer begins the upgrade install to Windows Server 2019. It may restart several times during this process.

   That's it — you're done!

Performing a Network Install with Windows Deployment Services

Windows Deployment Services (WDS) is a role that can be installed on a Windows Server operating system. It serves as a combination of a Preboot Execution Environment (PXE) server and a Trivial File Transfer Protocol (TFTP) server and enables you to install Windows over a network connection by choosing the network interface card as the boot device.

Installing WDS is fairly straightforward. You can choose to install it as a standalone server or integrate it with Active Directory. You tell it what the boot file is that you want to use. The easiest one to start with is the `boot.wim` file on the Windows Server installation media, which contains the Windows Preinstallation Environment (WinPE).

From there, you need to create the installation files. The simplest way to do this is to copy `install.wim` from the Windows Server 2019 installation media. It gives you the same edition and experience options that you would've gotten from the installation wizard on disc. After WDS is fully configured, it serves images over the network. All you need to do is tell your new server to boot from the network.

TECHNICAL STUFF

If you're doing a network install, and the server isn't in the same subnet as the WDS server, you need to set Dynamic Host Configuration Protocol (DHCP) options 66 and 67. Option 66 specifies the hostname or IP address of the WDS server, and Option 67 is the bootfile name. You may also need to create a firewall rule to allow UDP ports 67 and 68 if there is a firewall between the two networks.

IN THIS CHAPTER

- **Understanding the default settings in Windows Server 2019**
- **Getting an overview of the configuration process**
- **Providing the information your server needs to be set up properly**
- **Updating Windows Server 2019 with the latest patches, hotfixes, and everything in between**
- **Customizing Windows Server 2019 to your preferences**
- **Configuring your server startup options with BCDEdit**

Chapter 4

Performing Initial Configuration Tasks

Now that you've installed Windows Server 2019, it's time for the fun to begin! As an administrator, your next task after installing the server operating system is to configure it to do what you want it to do.

Microsoft introduced the Server Manager feature in Server 2008, and it was updated heavily in Windows Server 2012 to support Remote Management, as well as multi-server management. Server Manager is your starting location for the majority of the configuration tasks that you need to accomplish on your server if you're working on a server that has Desktop Experience.

If you're working on a Server Core system, you won't use Server Manager on the console. Instead, you'll use the sconfig utility to do your initial configuration, assuming that you aren't deploying Server Core images that are already configured for your environment. Of course, you can use Server Manager to administer your Server Core systems remotely, with a little setup initially to get things going. I cover that subject in my overview of the configuration process.

Understanding Default Settings

When Windows Server 2019 is first installed, there are some settings that are created or set by default. Typically, these are things that you'll want to change, such as setting the server's name, setting an IP address, joining the server to a domain, and so on. Table 4-1 covers these default settings and discusses what they're set to out of the box to give you a better idea of what you're starting with.

TABLE 4-1 Windows Server 2019 Default Settings

Setting	Default Value	Description
Computer Name	WIN-<*randomstring*>	This will be a randomly generated name starting with WIN-. You should change the name based on your organization's naming standards. When you change the name, you'll be required to restart the system.
IP Address	Assigned by DHCP	By default, your brand-new server is using DHCP to automatically receive an IP address. If your organization uses DHCP to manage IP addresses, you're good to go. If not, you may need to set a static IP address.
Domain or Workgroup	Workgroup named WORKGROUP	Windows Server 2019 begins life joined to a workgroup named WORKGROUP. If it's going to be a standalone server, then that setting may work well for you. Servers in workgroups are not domain joined. If your server needs to be joined to a domain, you'll want to change this setting. Doing so will require a reboot.
Windows Update	Automatic update download	Updates are downloaded automatically, but they aren't installed until you allow them to be.
Windows Firewall	Public and private profiles: On Core OS functionality: Allowed	In its default state Windows Firewall has a public and a private profile. Core functionality needed for the operating system to function is allowed automatically. The domain profile will appear if the server becomes domain joined.
Windows Defender Antivirus	Real-time protection: On	Provides real-time virus/malware scanning. It prevents malware from installing and/or running on your server. Automatic sample submission is also enabled by default. This sends sample files to Microsoft for analysis.

Setting	Default Value	Description
Roles and Features	Some roles/features are installed	Some roles and features are enabled out of the box to allow the server basic functionality. It's important to note that just because a role or feature is selected, that doesn't mean that the role as a whole is installed.
Remote Management	Enabled	Allows the server to be managed by PowerShell remotely. Also allows applications or commands that require Windows Management Instrumentation (WMI) to manage the server.
Remote Desktop	Disabled	Allows users to connect to the desktop of the server remotely. Allowed users can be configured individually or by security groups.

Getting an Overview of the Configuration Process

When you start with a freshly installed server, it isn't configured to do much of anything. You'll need to take some basic configuration steps. Some of these steps are the basics like setting the day and time; others are tasks that will allow you to manage your systems remotely.

Here's the basic process:

- Activate Windows Server 2019.
- Set the date, time, and time zone.
- Change the computer name.
- Add to the domain (if there is one to join).
- Configure the networking.
- Configure the server to receive Windows updates.
- Add roles and features.
- Setup the Windows Server OS for remote administration.
- Configure the Windows Server firewall.

You can find the specifics on how to do each of these tasks in the following section.

Providing Computer Information

When you're deploying new servers, you have to perform certain tasks, such as activating the operating system with a valid Microsoft product key, setting the time zone, changing the name, and adding the server to the domain. In this section, I explain how to provide information for the server on both Windows Server 2019 with Desktop Experience and Server 2019 Core.

Windows Server 2019 with Desktop Experience

Many system administrators got their start with the graphical user interface (GUI) of a Windows Server operating system. Windows Server 2019 continues the tradition of the GUI with the Desktop Experience installation. Let's take a look at what is involved with configuring Windows Server 2019 with Desktop Experience.

Activation

One of the first things that you do after installing the Windows Server operating system is activate it with a valid product key. You can do this through the desktop interface or through the command line.

In this section, I cover activating through the desktop interface. I cover activation through the command line in the later section on activation for Server Core.

1. **Log into the server.**

   Server Manager opens automatically.

2. **In Server Manager, click Local Server in the navigation pane.**
3. **To start the activation process, click the Not Activated hyperlink next to Product ID.**

   A dialog box launches automatically asking for the product key.

4. **Enter your product key and click Next.**

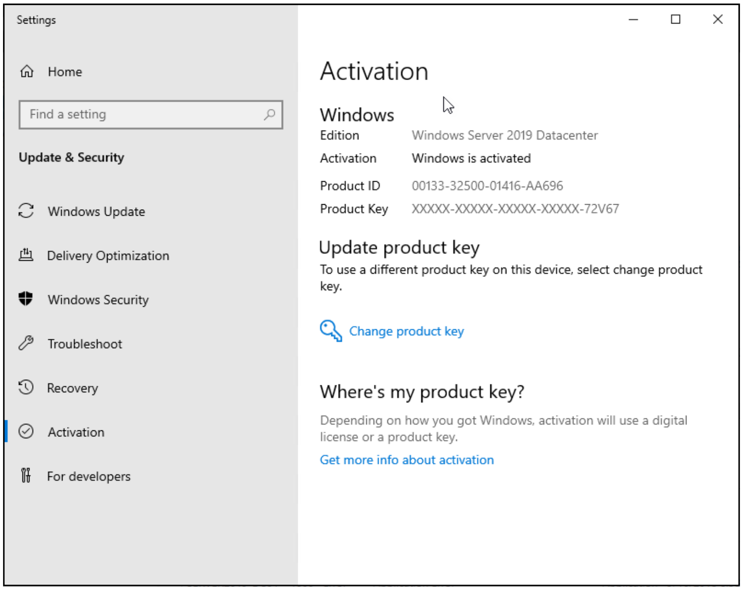
   You're prompted to activate Windows.

5. **Click Activate.**

   You get a confirmation that Windows has been activated.

6. **Click Close.**

   You're left on the Activation screen shown in Figure 4-1, where you see that your version of Windows is now activated.



Activation

Windows

Edition Windows Server 2019 Datacenter
Activation Windows is activated
Product ID 00133-32500-01416-AA696
Product Key XXXXX-XXXXX-XXXXX-XXXXX-72V67

Update product key

To use a different product key on this device, select change product key.

Change product key

Where's my product key?

Depending on how you got Windows, activation will use a digital license or a product key.

Get more info about activation

FIGURE 4-1: The Activation screen showing that Windows Server 2019 is activated.

Time zone

Setting the time zone is a common task in the server provisioning process. You may want to set the server to the time zone that you are in, or to the same time zone as a corporate office located elsewhere. This is common if your servers are in a co-location and you want them to be on the same time zone as your local systems.

1. **In Server Manager, click Local Server in the left-hand menu.**
2. **Click the hyperlink next to Time Zone.**

   This may already be set to the correct time zone for your area.
3. **Click the Change Time Zone button.**
4. **Select your time zone from the drop-down list.**
5. **If you're in an area that uses Daylight Saving Time, click the check box next to Automatically Adjust Clock for Daylight Saving Time. If you do not use Daylight Saving Time, leave the box unchecked.**
6. **Click OK to exit the Time Zone Settings dialog box, and then click OK again to exit the Date and Time dialog box.**

Computer name and domain

Setting the computer name is a must in an enterprise environment. Most organizations have a naming convention that you need to follow, but the names the organization requires will certainly be easier to remember than the default randomly generated name. Joining to the domain is one of the simpler steps, but also one of the most important steps to enable centralized authentication management and configuration capabilities.

1. **In Server Manager, click Local Server in the left-hand menu.**
2. **Click the hyperlink next to Computer Name.**

   This will be the default name that starts with WIN- and will be followed by a random string of letters and numbers.
3. **Click the Change button.**
4. **In the Computer Name field, enter the name that you want for your server, and then click OK.**

   A dialog box appears telling you that you need to restart the server.
5. **Click OK.**
6. **Click the Close button in the System Properties dialog box.**

   You're prompted to either Restart Now or Restart Later.
7. **Click Restart Now if you want to reboot the server immediately. Click Restart Later if you want to finish other administrative tasks you may have first.**

   If you click Restart Later, you'll need to manually reboot the server when you're ready.
8. **To join a domain, perform Steps 1 through 3.**
9. **In the Computer Name/Domain Changes dialog box, click the Domain radio button, and enter the name of the domain you want to join.**
10. **Click OK.**

    A dialog box appears telling you that you need to restart the server.
11. **Click OK.**
12. **Click the Close button in the System Properties dialog box.**
13. **Click Restart Now or Restart Later.**

    After the restart, the server will be joined to the domain.

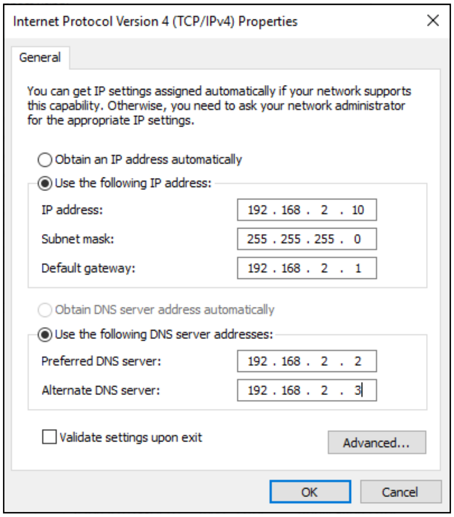
Configure networking

Your server will use a dynamically assigned IP address by default. If this is not desirable, you'll want to set a static IP address so that the server will continue to use the same address.

1. **In Server Manager, click Local Server in the left-hand menu.**
2. **Next to Ethernet, click the hyperlink that says IPv4 Address Assigned by DHCP, IPv6 Enabled.**
3. **Right-click your network adapter (it should be called Ethernet), and click Properties.**
4. **Click Internet Protocol Version 4, and then click the Properties button.**

   By default, the server is set to obtain an IP address automatically and obtain DNS server address automatically. If this is what is desired, then no changes are necessary.
5. **If you need to make changes, select Use the Following IP Address.**
6. **Fill in the IP address, subnet mask, and default gateway.**
7. **Manually enter the addresses for the preferred DNS servers.**

   See Figure 4-2 for an example.
8. **Click OK to close the dialog box.**
9. **Click OK one more time to exit out of Ethernet Properties.**



Internet Protocol Version 4 (TCP/IPv4) Properties

General

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

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 2 . 10

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 2 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 2 . 2

Alternate DNS server: 192 . 168 . 2 . 3

□ Validate settings upon exit

FIGURE 4-2: The Internet Protocol Version 4 Properties dialog box.

Windows Server 2019 Core

Many system administrators have configured a Windows Server with a GUI, but not many have used Windows Server Core. As you see in this section, Windows Server Core has a simple interface, and when you learn how to navigate it, you may find it simpler to work with than Windows Server with Desktop Experience.

Activation

Windows Server Core gives you a few different options for activating your copy of Windows Server 2019. In this section, I cover activating via sconfig, as well as activating via the command line.

ACTIVATING WITH SCONFIG

Sconfig is the built-in configuration utility in Windows Server Core. It's a text-based menu that allows you to do the majority of your initial configuration tasks all from one central location.

1. **At the Command Prompt, type** sconfig **to launch the configuration utility.**
2. **Type** 11 **for Windows Activation and press Enter.**
3. **Type** 3 **to install your product key.**
4. **Enter your 25-character product key in the dialog box that pops up, and then click OK.**

   A Command Prompt window appears using the slmgr.vbs script to set the key. This script is covered in "Activating from the command line," later in this chapter.

   After the key is installed, you see a message saying the key was installed successfully.
5. **Close the window by clicking the red X, or by typing** exit **and then pressing Enter.**
6. **When you're back on the sconfig screen, type** 2 **to Activate Windows, and then press Enter.**

   A Command Prompt window launches again with the slmgr.vbs script to perform the activation. Assuming there are no errors, this will complete with no message.
7. **Close out of the window by clicking the red X or by typing** exit **and then pressing Enter.**

ACTIVATING FROM THE COMMAND LINE

After you've logged into Windows Server Core, you're presented with the Command Prompt. From there, you can activate your copy of Windows. First, you have to set the key. You do this with the Windows Server License Manager script, slmgr.vbs.

TECHNICAL STUFF

The slmgr.vbs script allows you to work with your Windows Server product keys in different ways depending on the parameter that you use along with it. In the example in this book, I use both `-ipk` and `-ato`. The `-ipk` parameter is used when installing product keys, and the `-ato` parameter is used to specify online activation.

To install the product key that will be needed for your version of Windows Server 2019, use the following command with the parameter `-ipk`. Just replace *<productkey>* with your 25-character license key, including the dashes.

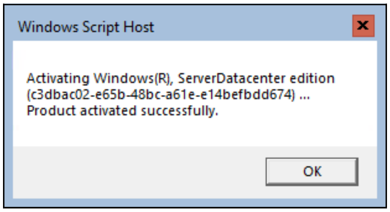
```
slmgr.vbs -ipk <productkey>
```

You get a dialog box that tells you the product key installed successfully. Click OK.

After the license key is installed, you use the same script with the `-ato` parameter to do an online activation of your copy of Windows. You do that with the following command:

```
slmgr.vbs -ato
```

If the activation was successful, you get a dialog box that says the product was activated successfully (see Figure 4-3).



Activating Windows(R), ServerDatacenter edition
(c3dbac02-e65b-48bc-a61e-e14befbdd674) ...
Product activated successfully.

FIGURE 4-3: Using slmgr.vbs to activate Windows Server.

Time zone

Much like activation in Windows Server Core, you can set the time zone via sconfig or the command line. In this section, I cover both methods. The great thing about the command line version is that it will work on Windows Server with Desktop Experience as well.

SETTING THE TIME ZONE WITH SCONFIG

Sconfig is the built-in configuration utility in Windows Server Core. Because it's a simple text-based menu, it provides a simple way for administrators to configure the time zone without needing scripting knowledge to do so.

1. **At the Command Prompt, type** sconfig **to launch the configuration utility.**
2. **Enter** 9 **to go into the settings for Date and Time.**

   The Date and Time dialog box appears.
3. **Click the Change Time Zone button.**
4. **Select your time zone from the drop-down list.**
5. **If you're in an area that uses Daylight Saving Time, click the check box next to Automatically Adjust Clock for Daylight Saving Time. If you do not use Daylight Saving Time, leave the box unchecked.**
6. **Click OK to exit out of the Time Zone Settings dialog box, and click OK once more to exit out of the Date and Time dialog box.**

SETTING THE TIME ZONE FROM THE COMMAND LINE

If you prefer to work on the command line, you can also set the time zone from there. This utilizes the control command to call the Control Panel's Date and Time screen.

1. **At the Command Prompt, type the following:**

   ```
   control timedate.cpl
   ```

   The Date and Time dialog box appears.
2. **Click the Change Time Zone button.**
3. **Select your time zone from the drop-down list.**
4. **If you're in an area that uses Daylight Saving Time, click the check box next to Automatically Adjust Clock for Daylight Saving Time. If you do not use Daylight Saving Time, leave the box unchecked.**
5. **Click OK to exit out of the Time Zone Settings dialog box, and click OK once more to exit out of the Date and Time dialog box.**

Computer name and domain

Setting the name and adding a server to a Windows domain are some of the most common activities that system administrators do with new servers. With Windows

Server Core, there are two methods that you should know to complete this task: sconfig (the configuration utility in Windows Server Core) and the command line.

SETTING THE COMPUTER NAME WITH SCONFIG

The sconfig utility in Windows Server Core makes it simple to change the name of your server with its text-driven menus. Follow these steps:

1. **At the Command Prompt, type** sconfig **to launch the configuration utility.**
2. **Type** 2 **to change the computer name.**

   You're prompted to enter a new name.
3. **Enter the new name, and press Enter.**

   You need to restart your computer to apply the change.
4. **Type** yes **to reboot now or** no **to reboot later.**

ADDING TO A DOMAIN WITH SCONFIG

When the server has the correct name, you may want to add it to a Windows domain. You can do this with the sconfig utility as well.

1. **At the Command Prompt, type** sconfig **to launch the configuration utility.**
2. **Type** 1 **to change the domain.**
3. **Type** D **to join a domain and press Enter.**
4. **Give it the name of the domain you want to join and then press Enter.**
5. **Enter the name of an authorized user and press Enter.**
6. **Enter the password of the user and press Enter.**

   You need to restart your computer to apply the change.
7. **Click** yes **to reboot now or** no **to reboot later.**

SETTING COMPUTER NAME FROM THE COMMAND LINE

Although sconfig is a nice utility, you may want to be able to script the changes that you want to make. Whenever this is the case, the command line can be very helpful. From running batch scripts in the Command Prompt, to running PowerShell scripts in PowerShell, both methods work regardless of whether you're on Windows Server Core or Windows Server with Desktop Experience.

1. **From the Command Prompt, type** powershell**.**

   The PowerShell window opens on your Server Core box.

2. **Use the** `Rename-Computer` **command to change the name of your server:**

   ```
   Rename-Computer -NewName <new-name>
   ```

   You get a message stating that the NetBIOS name will be truncated if your name is longer than 15 characters.

3. **If you receive this message, type** Y **and then press Enter to accept.**

ADDING TO A DOMAIN FROM THE COMMAND LINE

The ability to script the joining of the domain is a useful skill if you're going to be deploying any quantity of servers. Not only does adding a domain via the command line make it simpler to do, but it also helps to ensure that there are no mistakes in the process of joining the domain.

1. **From the Command Prompt, type** powershell.exe**.**

   The PowerShell window opens on your Server Core box.

2. **Use the** `Add-Computer` **command to add the server to the domain.**

   Here's an example:

   ```
   Add-Computer -DomainName "your_domain_name" -Restart
   ```

   A dialog box appears asking for a username and password.

3. **Enter a username that is authorized to add systems to your Active Directory domain and enter the corresponding password.**

4. **Click OK.**

   The server restarts.

Configure networking

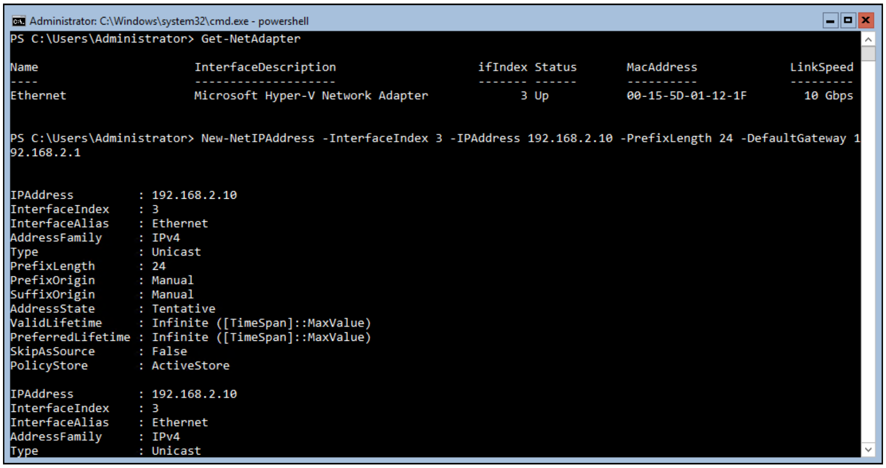
Before you can set the IP address for the adapter with PowerShell, you need to find out what the index of your interface is. You can do this by typing the following:

```
Get-NetAdapter
```

The output lists all network adapters. In this case, you want the one that says Ethernet. After you have the index number, you can set the IP address and the DNS servers. On my server, the index is 3.

Use the following command to set the static IP address. `InterfaceIndex` is the index number for my network card, `IPAddress` is the IP address I want to assign, `PrefixLength` is the subnet mask that I want to use, and `DefaultGateway` is the gateway address for the local network (see Figure 4-4).

```
New-NetIPAddress -InterfaceIndex 3 -IPAddress 192.168.2.10
  -PrefixLength 24 -DefaultGateway 192.168.2.1
```



```
PS C:\Users\Administrator> Get-NetAdapter

Name                      InterfaceDescription                    ifIndex Status       MacAddress             LinkSpeed
----                      --------------------                    ------- ------       ----------             ---------
Ethernet                  Microsoft Hyper-V Network Adapter             3 Up           00-15-5D-01-12-1F        10 Gbps


PS C:\Users\Administrator> New-NetIPAddress -InterfaceIndex 3 -IPAddress 192.168.2.10 -PrefixLength 24 -DefaultGateway 1
92.168.2.1


IPAddress         : 192.168.2.10
InterfaceIndex    : 3
InterfaceAlias    : Ethernet
AddressFamily     : IPv4
Type              : Unicast
PrefixLength      : 24
PrefixOrigin      : Manual
SuffixOrigin      : Manual
AddressState      : Tentative
ValidLifetime     : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipAsSource      : False
PolicyStore       : ActiveStore

IPAddress         : 192.168.2.10
InterfaceIndex    : 3
InterfaceAlias    : Ethernet
AddressFamily     : IPv4
Type              : Unicast
```

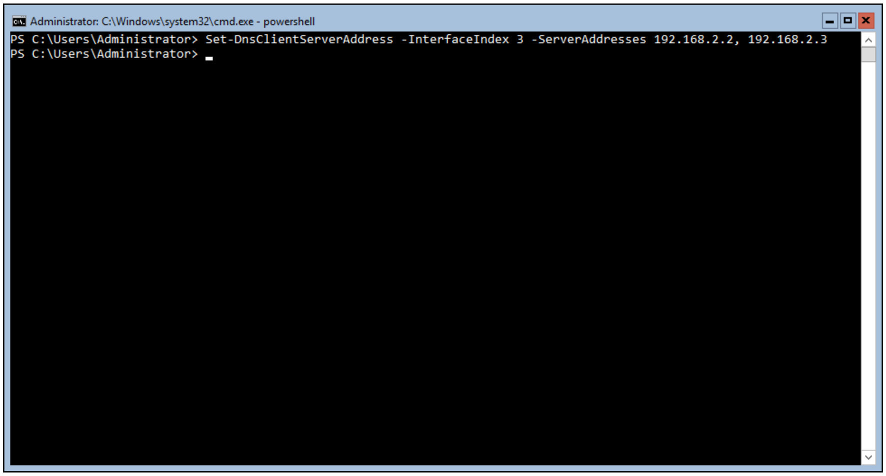
FIGURE 4-4: Setting the IP address with PowerShell.

TECHNICAL STUFF

I haven't discussed PowerShell much at this point, and this is a more complex bit of PowerShell. The `New-NetIPAddress` is a cmdlet that allows you to work with IP addresses on Windows Server systems. The parameters that come afterward, like `-InterfaceIndex`, help to identify the object you want to work with (the network adapter, in this case) or to make changes to the settings, like the `-IPAddress` parameter where you specify the IP address you want to set on the network adapter.

To set the DNS Server after that, the command uses the same index number for my network card. `ServerAddresses` is used to identify the DNS servers that the system should use (see Figure 4-5). If you have more than one, you can separate them with a comma.

```
Set-DNSClientServerAddress -InterfaceIndex 3 -ServerAddresses
  192.168.2.2, 192.168.2.3
```



Administrator: C:\Windows\system32\cmd.exe - powershell

```
PS C:\Users\Administrator> Set-DnsClientServerAddress -InterfaceIndex 3 -ServerAddresses 192.168.2.2, 192.168.2.3
PS C:\Users\Administrator> _
```

FIGURE 4-5: Setting the DNS servers with PowerShell.

Updating Windows Server 2019

After you have installed your brand-new Windows Server, and maybe even done some of the basic configuration work like changing the name and joining the domain, you'll want to update the server. Updates contain fixes for security vulnerabilities and new features, and should always be installed before turning a server over to the team that requested it.

Windows Server 2019 with Desktop Experience

Considering how important it is to stay up to date on Windows Server updates, most organizations are going to set up automatic updates. You may have a server that can't be set to receive updates automatically, or there may be an emergency patch that was issued and you want to apply it right away. In this section, I explain how to do automatic updates and manual updates.

Automatic updates

Most organization use automatic updates. The following directions walk you through setting up your server to reach out to Microsoft's update servers (the default behavior).

TECHNICAL STUFF

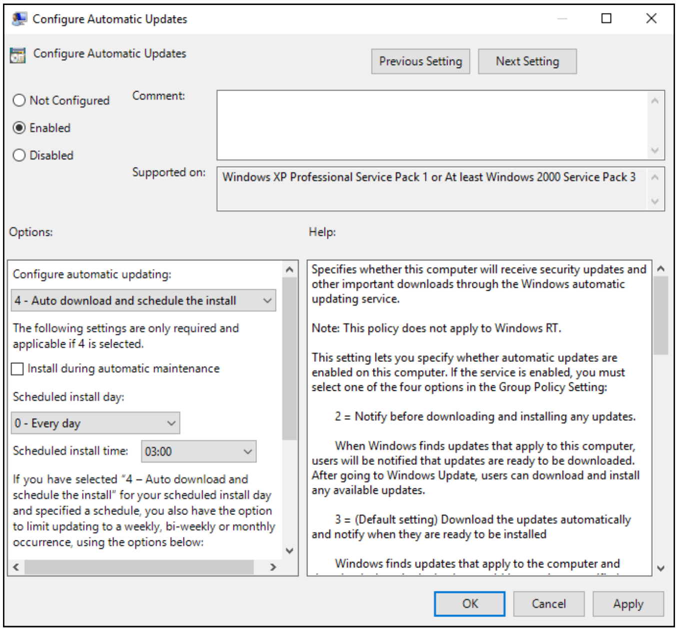
Many organizations have patching solutions that handle the scheduling of updates, and could still be considered an automatic update because the tool will schedule the deployment of approved patches.

1. **Click the Start menu and type** gpedit.msc**.**
2. **Navigate to the Windows Update section by clicking on Computer Configuration, then Administrative Templates, then Windows Components, and finally Windows Update.**
3. **Double-click Configure Automatic Updates.**
4. **Select Enabled.**

   You're given configuration options.

   Under Configure Automatic Updating, you can see that it's set to Auto Download and Notify to Install. This is the default setting.
5. **Click the drop-down box and select the setting that works best for your environment.**

   In my case, I've chosen Auto Download and Schedule the Install. See Figure 4-6 for an example.
6. **Click OK to save the change.**



Configure Automatic Updates

Configure Automatic Updates

Previous Setting | Next Setting

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: Windows XP Professional Service Pack 1 or At least Windows 2000 Service Pack 3

Options:

Configure automatic updating:

4 - Auto download and schedule the install

The following settings are only required and applicable if 4 is selected.

□ Install during automatic maintenance

Scheduled install day:

0 - Every day

Scheduled install time: 03:00

If you have selected "4 – Auto download and schedule the install" for your scheduled install day and specified a schedule, you also have the option to limit updating to a weekly, bi-weekly or monthly occurrence, using the options below:

Help:

Specifies whether this computer will receive security updates and other important downloads through the Windows automatic updating service.

Note: This policy does not apply to Windows RT.

This setting lets you specify whether automatic updates are enabled on this computer. If the service is enabled, you must select one of the four options in the Group Policy Setting:

2 = Notify before downloading and installing any updates.

When Windows finds updates that apply to this computer, users will be notified that updates are ready to be downloaded. After going to Windows Update, users can download and install any available updates.

3 = (Default setting) Download the updates automatically and notify when they are ready to be installed

Windows finds updates that apply to the computer and

OK | Cancel | Apply

FIGURE 4-6: Using the Local Group Policy Editor to change the automatic updates setting in Windows Server 2019.

Downloading and installing updates

You hear about the next big security vulnerability on the news media, and vendors release patches to the vulnerability very quickly after that. When a security vulnerability impacts your Windows Server systems, you may want to start a manual update — that way, your systems are protected outside of your normal patching windows. If your organization uses a patching solution, the patch may be pushed from that system, but there are always a few systems that don't take the patch for whatever reason. You may have to manually update when that occurs.

1. **With Server Manager open, click Local Server in the left-hand menu.**
2. **Click the hyperlink next to Last Checked for Updates.**

   This may say Never if it hasn't been run yet.
3. **Click the Check for Updates button.**

   The server will check to see if there are any updates available.

Windows Server 2019 Core

Windows Server Core has the same needs when it comes to receiving updates from Microsoft that Windows Server with Desktop Experience does. In this section, I show you how to set up automatic updates and how to perform manual updates from the command line.

Automatic updates

There are two ways you can enable automatic updates on Server Core: using the sconfig utility and using the command line.

SETTING UPDATES TO AUTOMATIC VIA SCONFIG

The text-driven menu provided by the sconfig utility makes enabling automatic updates very simple. You can set up automatic updates in just four quick steps:

1. **At the Command Prompt, type** sconfig**.**
2. **Type** 5 **to configure Windows Update settings, and then press Enter.**

   You're given the choice of selecting A for automatic download and install, D for download only (which is the default), or M for manual updates.
3. **Type A for automatic download and installation of Windows updates.**

   You get a dialog box confirming the change was successful.
4. **Click OK.**

SETTING UPDATES TO AUTOMATIC VIA COMMAND LINE

To set updates to automatic via the command line, you need to navigate to `C:\Windows\system32` and stop the Windows Update service. It may already be stopped. Then you can use the script program to execute scregedit.wsf. Adding the switch `/AU 4` enables automatic updates, `/AU 1` would disable automatic updates. The following example enables Windows updates:

1. **Stop the Windows Update Server service.**

   ```
   net stop wuauserv
   ```

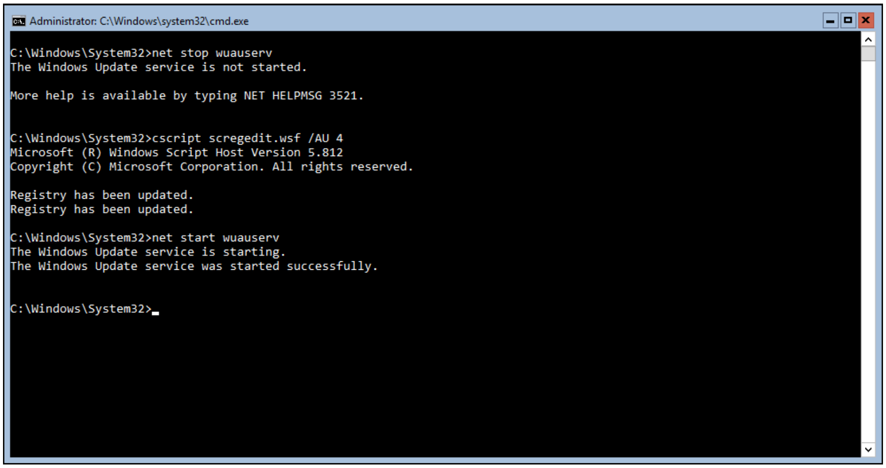
2. **Set automatic updates to 4 which is enabled.**

   ```
   cscript scregedit.wsf /AU 4
   ```

3. **Start the Windows Updates Server service.**

   ```
   net start wuauserv
   ```

If you would like to see an example of what this looks like and what the responses should be, please see Figure 4-7.



```
C:\Windows\System32>net stop wuauserv
The Windows Update service is not started.

More help is available by typing NET HELPMSG 3521.


C:\Windows\System32>cscript scregedit.wsf /AU 4
Microsoft (R) Windows Script Host Version 5.812
Copyright (C) Microsoft Corporation. All rights reserved.

Registry has been updated.
Registry has been updated.

C:\Windows\System32>net start wuauserv
The Windows Update service is starting.
The Windows Update service was started successfully.


C:\Windows\System32>_
```

FIGURE 4-7: Setting automatic updates in the Command Prompt.

Downloading and installing updates

To force Server Core to then detect and install any available updates, simply type the following command and press Enter.

```
wuauclt /detectnow
```

Customizing Windows Server 2019

After your Windows Server operating system is installed, the next step is to customize it and make it your own! This involves things like installing roles and features, setting up remote administration, and configuring the firewall.

Windows Server 2019 with Desktop Experience

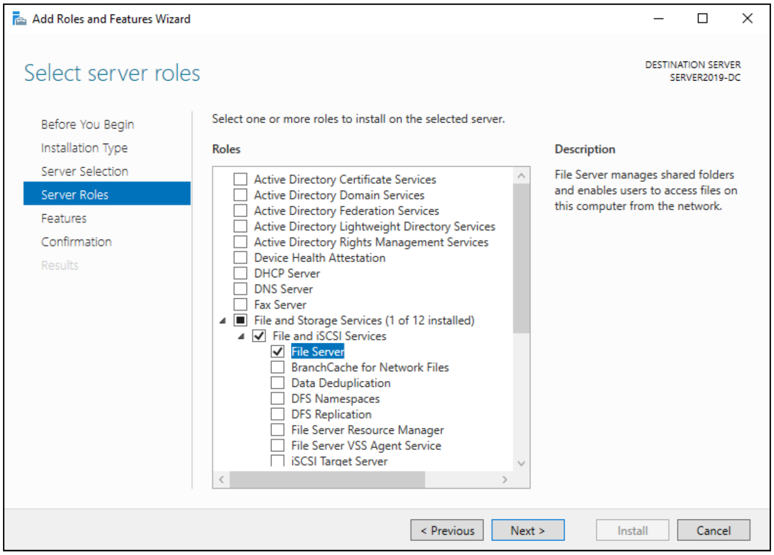
I'll start the customization discussion with the Desktop Experience. When you log into a server with Desktop Experience enabled, by default Server Manager will launch. A lot of the configuration and customization tasks you may have can be accomplished from Server Manager.

Adding roles and features

Roles and features are added in Windows Server 2019 with Desktop Experience through Server Manager.

1. **Open Server Manager**
2. **Choose Manage➪Add Roles and Features.**
3. **On the Before You Begin page, click Next.**
4. **On the Select Installation Type page, click Next.**
5. **On the Select Destination Server page, click Next.**
6. **Check the check box next to the role that you want to install and click Next.**

   For this demonstration, I've chosen File Server under File and Storage Services (see Figure 4-8).
7. **On the next screen, select any features you may want to install and then click Next.**
8. **If you want the server to restart automatically if needed for the role you installed, you can select the Restart the Destination Server Automatically if Required check box. If a restart is not needed, or you don't want it to restart, leave the check box unchecked.**
9. **Click Install to install the roles and/or features you selected.**



Select server roles

DESTINATION SERVER
SERVER2019-DC

Select one or more roles to install on the selected server.

Roles

- ☐ Active Directory Certificate Services
- ☐ Active Directory Domain Services
- ☐ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Device Health Attestation
- ☐ DHCP Server
- ☐ DNS Server
- ☐ Fax Server
- ■ File and Storage Services (1 of 12 installed)
  - ☑ File and iSCSI Services
    - ☑ File Server
    - ☐ BranchCache for Network Files
    - ☐ Data Deduplication
    - ☐ DFS Namespaces
    - ☐ DFS Replication
    - ☐ File Server Resource Manager
    - ☐ File Server VSS Agent Service
    - ☐ iSCSI Target Server

Description

File Server manages shared folders and enables users to access files on this computer from the network.

FIGURE 4-8: The select Server Roles Screen with File Server selected.

Enabling remote administration

REMEMBER

Remote Management is enabled by default and allows for remote administration through PowerShell. Remote Desktop is a separate setting that allows you to connect to the server and work with it directly.

When a server has Desktop Experience, administrators often prefer to work with the server over Remote Desktop. This is disabled by default; you enable it to use it. If the firewall on the server is enabled and does not have Remote Desktop enabled, you won't be able to connect to it. You need to enable the Remote Desktop – User Mode (TCP-In) rule listed in the Inbound Rules of your server's firewall.

1. **With Server Manager open, click Local Server in the left-hand menu.**
2. **Click the hyperlink next to Remote Desktop that says Disabled.**
3. **In the dialog box that appears, select Allow Remote Connections to This Computer.**

   A dialog box appears telling you that a firewall exception will be made for Remote Desktop.
4. **Click OK.**
5. **If you want to set remote access for specific people or groups, click the Select Users button.**

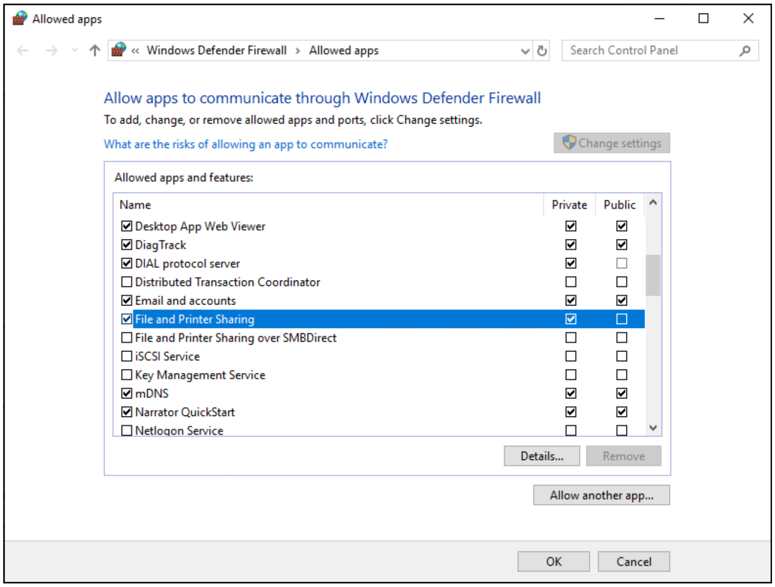
6. **Click Add, choose your person or group, and click OK.**
7. **Click OK again on Remote Desktop Users to close out of it.**
8. **Click OK one more time on the System Properties screen to enable Remote Desktop.**

Configure Windows Firewall

Assuming that you're going to use the Windows Firewall on your server, you need to know how to enable applications through the firewall. By allowing inbound traffic, you enable the server to do the job you plan on using it for.

1. **From Server Manager, select Local Server on the left-hand side.**
2. **Click the hyperlink that says Public:On next to Windows Defender Firewall.**

   The Firewall & Network Protection app opens.
3. **Click Allow an App through Firewall.**
4. **Select File and Print Sharing and enable it for the Private profile by selecting the check box under Private (see Figure 4-9).**
5. **Click OK to save your changes.**



Allow apps to communicate through Windows Defender Firewall

To add, change, or remove allowed apps and ports, click Change settings.

What are the risks of allowing an app to communicate?

Allowed apps and features:

Name	Private	Public
☑ Desktop App Web Viewer	☑	☑
☑ DiagTrack	☑	☑
☑ DIAL protocol server	☑	□
□ Distributed Transaction Coordinator	□	□
☑ Email and accounts	☑	☑
☑ File and Printer Sharing	☑	□
□ File and Printer Sharing over SMBDirect	□	□
□ iSCSI Service	□	□
□ Key Management Service	□	□
☑ mDNS	☑	☑
☑ Narrator QuickStart	☑	☑
□ Netlogon Service	□	□

FIGURE 4-9: Allowing an app through Windows Defender Firewall.

Windows Server 2019 Core

Whether you're running PowerShell commands against your Windows Server Core system while connected to the console or through remote PowerShell, you can do much of your configuration work with just a few PowerShell commands.

Adding roles and features

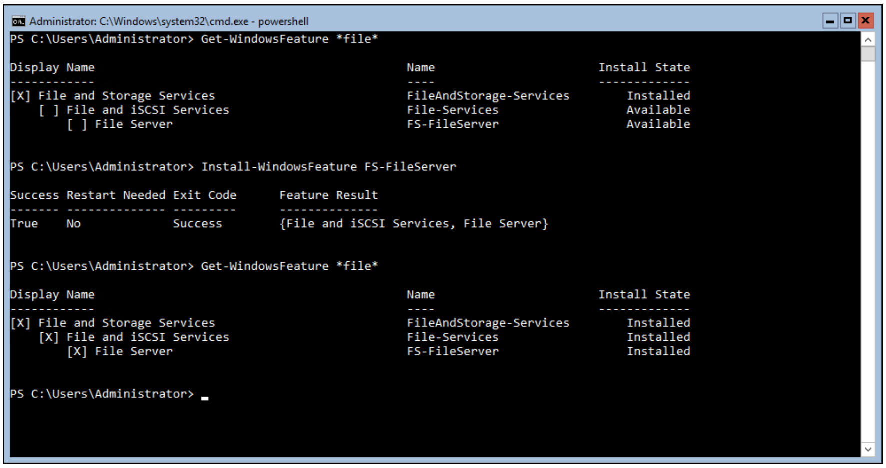
To get really good working with Server Core, half of the battle you face is learning how to find the things you want. In Server with Desktop Experience, you have the GUI to guide you. Not so with Server Core.

Let's look at the example I used with the Desktop Experience server. You want to install the File Server role. Before you can install the role, you need to find out what to call it. By using `Get-WindowsFeature`, you can find the names of the roles and features you're interested in. If you have an idea of what the name is, you can do a wildcard search. In the following example, I've used `*file*` to indicate that I want the `Get-WindowsFeature` cmdlet to return results that have the word *file* in them.

```
Get-WindowsFeature *file*
```

When you type the preceding command, you get three results of items that have *file* in their names. You can see File Server under Display Name. For the installation command, you need the name under the Name column. In this case, it's FS-FileServer. Now you're ready to install it! Use the following command to install the File Server (see Figure 4-10):

```
Install-WindowsFeature FS-FileServer
```



Administrator: C:\Windows\system32\cmd.exe - powershell

```
PS C:\Users\Administrator> Get-WindowsFeature *file*

Display Name                                            Name                       Install State
------------                                            ----                       -------------
[X] File and Storage Services                           FileAndStorage-Services        Installed
    [ ] File and iSCSI Services                         File-Services                  Available
        [ ] File Server                                 FS-FileServer                  Available


PS C:\Users\Administrator> Install-WindowsFeature FS-FileServer

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {File and iSCSI Services, File Server}


PS C:\Users\Administrator> Get-WindowsFeature *file*

Display Name                                            Name                       Install State
------------                                            ----                       -------------
[X] File and Storage Services                           FileAndStorage-Services        Installed
    [X] File and iSCSI Services                         File-Services                  Installed
        [X] File Server                                 FS-FileServer                  Installed


PS C:\Users\Administrator> _
```

FIGURE 4-10: Using PowerShell to install roles and features.

You see a progress bar as the feature is installed. After it's installed, if you run the first command again, you see that all three results are now installed. File and iSCSI Services was installed because File Server relies on it.

Enabling remote administration

Remote Management is enabled by default in Windows Server 2019. If it was disabled in your environment, you can enable it by running the Configure-SMRemoting command. This allows you remotely administer your server with Server Manager.

```
Configure-SMRemoting.exe -Enable
```

To be able to administer the server remotely with PowerShell, you need two additional commands. Enable-PSRemoting configures PowerShell to receive remote commands that are sent to your system. Winrm quickconfig will analyze and automatically configure the WinRM service for you. This is very helpful when you just want it to work and don't need to customize it. The command starts the WinRM service if it isn't already started, and ensures that WinRM is set to automatically start. It also configures listeners for HTTP and HTTPS, and ensures that the Windows firewall is allowing HTTP and HTTPS traffic inbound.

The Enable-PSRemoting command will not give you any output if it succeeds. You'll simply be presented with the PowerShell prompt again.

```
Enable-PSRemoting -force
```

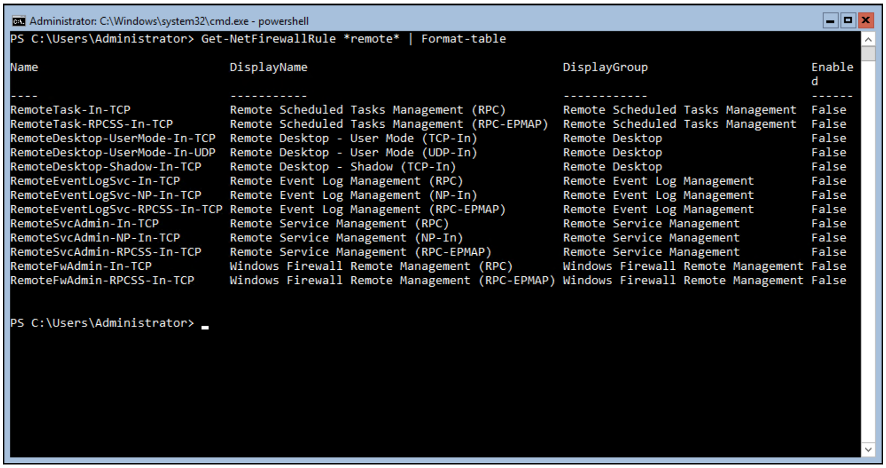
Running winrm quickconfig is a little different. After it runs its analysis, it tells you what needs to be changed and asks for a yes or no as to whether it can make the necessary changes. Select Y and press Enter. If everything looked good during the analysis, you'll be told that WinRM is already running and is already set up for Remote Management instead of the yes/no question.

```
winrm quickconfig
```

Configure Windows Firewall

Working with the Windows Defender Firewall on Server Core is pretty simple. You need to find the name of the rule you want to work with first. You can do that with the Get-NetFirewallRule command (see Figure 4-11). Using the Format-table command at the end makes the output more easily readable. Try the command without it — you'll see what I mean!

```
Get-NetFirewallRule *remote* | Format-table
```



```
PS C:\Users\Administrator> Get-NetFirewallRule *remote* | Format-table

Name                           DisplayName                                    DisplayGroup                       Enable
                                                                                                                 d
----                           -----------                                    ------------                       ------
RemoteTask-In-TCP              Remote Scheduled Tasks Management (RPC)        Remote Scheduled Tasks Management  False
RemoteTask-RPCSS-In-TCP        Remote Scheduled Tasks Management (RPC-EPMAP)  Remote Scheduled Tasks Management  False
RemoteDesktop-UserMode-In-TCP  Remote Desktop - User Mode (TCP-In)            Remote Desktop                     False
RemoteDesktop-UserMode-In-UDP  Remote Desktop - User Mode (UDP-In)            Remote Desktop                     False
RemoteDesktop-Shadow-In-TCP    Remote Desktop - Shadow (TCP-In)               Remote Desktop                     False
RemoteEventLogSvc-In-TCP       Remote Event Log Management (RPC)              Remote Event Log Management        False
RemoteEventLogSvc-NP-In-TCP    Remote Event Log Management (NP-In)            Remote Event Log Management        False
RemoteEventLogSvc-RPCSS-In-TCP Remote Event Log Management (RPC-EPMAP)        Remote Event Log Management        False
RemoteSvcAdmin-In-TCP          Remote Service Management (RPC)                Remote Service Management          False
RemoteSvcAdmin-NP-In-TCP       Remote Service Management (NP-In)              Remote Service Management          False
RemoteSvcAdmin-RPCSS-In-TCP    Remote Service Management (RPC-EPMAP)          Remote Service Management          False
RemoteFwAdmin-In-TCP           Windows Firewall Remote Management (RPC)       Windows Firewall Remote Management False
RemoteFwAdmin-RPCSS-In-TCP     Windows Firewall Remote Management (RPC-EPMAP) Windows Firewall Remote Management False


PS C:\Users\Administrator> _
```

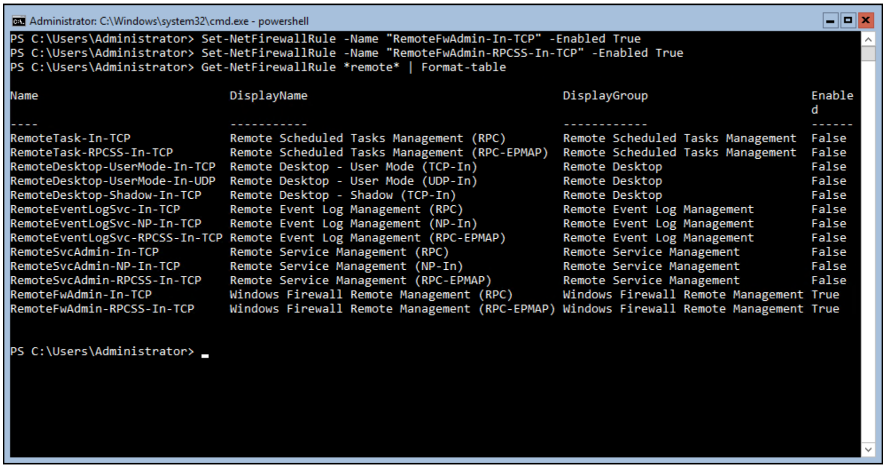
FIGURE 4-11: Using Get-NetFirewallRule to find rules.

The preceding command looks for any rules that have remote in the name. You can see each rule and whether it's enabled.

Let's enable the Remote Firewall Management rules. These would allow you to administer this server's firewall from another system. The rules you're interested in are RemoteFwAdmin-In-TCP and RemoteFWAdmin-RPCSS-In-TCP.

Here are the commands you'll use to enable these (see Figure 4-12):

```
Set-NetFirewallRule -Name "RemoteFwAdmin-In-TCP" -Enabled True
Set-NetFirewallRule -Name "RemoteFwAdmin-RPCSS-In-TCP" -
  Enabled True
```



```
PS C:\Users\Administrator> Set-NetFirewallRule -Name "RemoteFwAdmin-In-TCP" -Enabled True
PS C:\Users\Administrator> Set-NetFirewallRule -Name "RemoteFwAdmin-RPCSS-In-TCP" -Enabled True
PS C:\Users\Administrator> Get-NetFirewallRule *remote* | Format-table

Name                           DisplayName                                    DisplayGroup                       Enable
                                                                                                                 d
----                           -----------                                    ------------                       ------
RemoteTask-In-TCP              Remote Scheduled Tasks Management (RPC)        Remote Scheduled Tasks Management  False
RemoteTask-RPCSS-In-TCP        Remote Scheduled Tasks Management (RPC-EPMAP)  Remote Scheduled Tasks Management  False
RemoteDesktop-UserMode-In-TCP  Remote Desktop - User Mode (TCP-In)            Remote Desktop                     False
RemoteDesktop-UserMode-In-UDP  Remote Desktop - User Mode (UDP-In)            Remote Desktop                     False
RemoteDesktop-Shadow-In-TCP    Remote Desktop - Shadow (TCP-In)               Remote Desktop                     False
RemoteEventLogSvc-In-TCP       Remote Event Log Management (RPC)              Remote Event Log Management        False
RemoteEventLogSvc-NP-In-TCP    Remote Event Log Management (NP-In)            Remote Event Log Management        False
RemoteEventLogSvc-RPCSS-In-TCP Remote Event Log Management (RPC-EPMAP)        Remote Event Log Management        False
RemoteSvcAdmin-In-TCP          Remote Service Management (RPC)                Remote Service Management          False
RemoteSvcAdmin-NP-In-TCP       Remote Service Management (NP-In)              Remote Service Management          False
RemoteSvcAdmin-RPCSS-In-TCP    Remote Service Management (RPC-EPMAP)          Remote Service Management          False
RemoteFwAdmin-In-TCP           Windows Firewall Remote Management (RPC)       Windows Firewall Remote Management True
RemoteFwAdmin-RPCSS-In-TCP     Windows Firewall Remote Management (RPC-EPMAP) Windows Firewall Remote Management True


PS C:\Users\Administrator> _
```

FIGURE 4-12: Using PowerShell to set firewall rules and validate that they're enabled.

If the commands complete successfully, you'll get no response. You'll be returned to the PowerShell prompt. If you run your search again, you'll see that these rules are now enabled.

Configuring Startup Options with BCDEdit

With Windows Server 2008, Microsoft introduced a utility called BCDEdit, which allows you to manipulate the Windows boot configuration data (BCD) store. The BCD is used to tell the operating system how it should boot; it contains all the boot configuration parameters needed to support that function. This replaced the older `bootcfg.exe` utility that was used to edit the `boot.ini` file pre–Windows Vista. You must be a member of the local Administrator's group on a system to use BCDEdit. This is an advanced utility that is useful in troubleshooting issues that are preventing a server from booting properly.

REMEMBER

You may need to disable or suspend both BitLocker and Secure Boot on a system before you can use BCDEdit.

WARNING

Mistakes made using the BCDEdit utility could leave your system unable to boot at all. Always make sure that you either have a good backup of the system, or if you don't have a good backup, export the current settings from BCDEdit so that you can restore them if needed. You can export the current boot configuration database by typing **BCDEdit /Export <*export_path*>**. If you need to restore from that export, the command is very similar. You need only type **BCDEdit /Import <*path_to_export*>**.

Table 4-2 lists some of the more common options available for BCDEdit.

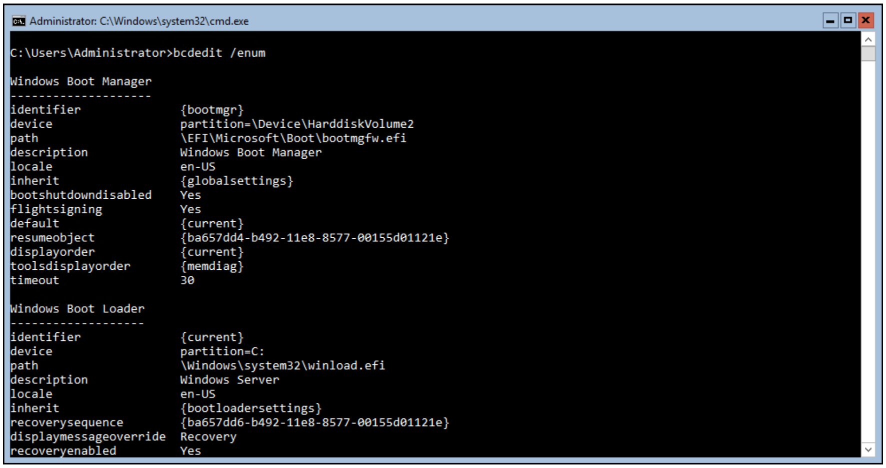
Most often, you'll use `bcdedit /set` to make changes to your boot configuration datastore. Before you make any changes, you need to know what your BCD looks like currently. You can use the `/enum` option to do that. In Figure 4-13, you can see the current settings for the Windows Boot Manager and the Windows Boot Loader.

You may notice that the description in the Windows Boot Loader just says Windows Server. Maybe you want it to be more descriptive than that. You can change it with `bcdedit /set`. You need the ID of the object that you're wanting to work on. In this case, you're wanting to edit the Windows Boot Loader; the identifier that you can see in Figure 4-13 is `{current}`. The full command you type will look something like this:

```
bcdedit /set {current} description "Windows Server 2019
  Datacenter"
```

TABLE 4-2 BCDEdit Common Options

Option	Description
`/bootdebug`	Enables or disables boot debugging.
`/dbgsettings`	Configures the type of debugging connection.
`/debug`	Enables or disables kernel debugging.
`/delete`	Deletes boot entries from the datastore — use with caution!
`/deletevalue`	Deletes or removes a boot entry option — use with caution!
`/displayorder`	Sets the order used by the boot manager when displaying the multiboot menu.
`/enum`	Lists all the entries in the boot configuration datastore.
`/export`	Exports the contents of the BCD; can be used as a backup to restore the BCD.
`/import`	Imports the contents of an exported file; can be used as a restore option if needed.
`/set`	Sets a value in a boot option.

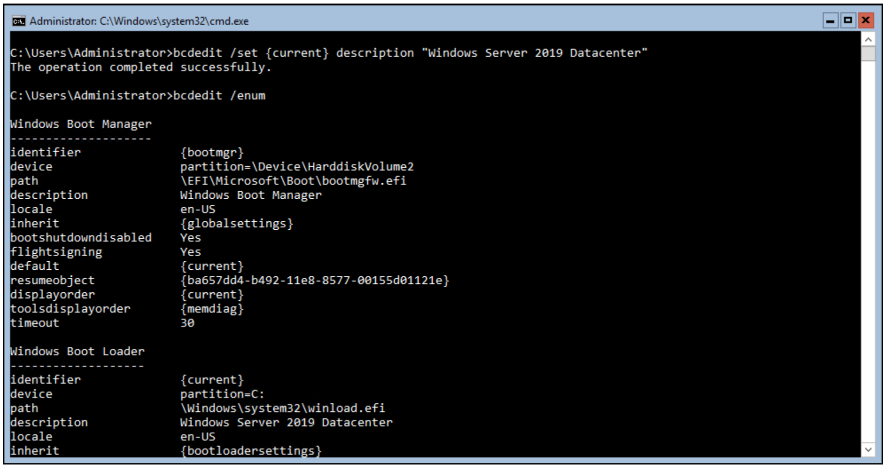


```
C:\Users\Administrator>bcdedit /enum

Windows Boot Manager
--------------------
identifier              {bootmgr}
device                  partition=\Device\HarddiskVolume2
path                    \EFI\Microsoft\Boot\bootmgfw.efi
description             Windows Boot Manager
locale                  en-US
inherit                 {globalsettings}
bootshutdowndisabled    Yes
flightsigning           Yes
default                 {current}
resumeobject            {ba657dd4-b492-11e8-8577-00155d01121e}
displayorder            {current}
toolsdisplayorder       {memdiag}
timeout                 30

Windows Boot Loader
-------------------
identifier              {current}
device                  partition=C:
path                    \Windows\system32\winload.efi
description             Windows Server
locale                  en-US
inherit                 {bootloadersettings}
recoverysequence        {ba657dd6-b492-11e8-8577-00155d01121e}
displaymessageoverride  Recovery
recoveryenabled         Yes
```

FIGURE 4-13: Using `bcdedit /enum` to see the current settings of the boot configuration datastore.

When you get the message `The operation completed successfully`, use `bcdedit /enum` again. You'll see your new description. See Figure 4-14 for my example.

Why would you want to change the name on the Windows Boot Loader? Consider the example of a multiple boot system that has the same operating system on both disks. The disks are used for very different purposes, so you want to ensure that you remember which is which. Being able to change the descriptions will simplify choosing the appropriate disk in the boot menu. BCDEdit can also be used to change the order of the boot menu. This is useful if you want to set one of your disks to be first in the list and the default disk to boot to after a certain amount of time.



```
C:\Users\Administrator>bcdedit /set {current} description "Windows Server 2019 Datacenter"
The operation completed successfully.

C:\Users\Administrator>bcdedit /enum

Windows Boot Manager
--------------------
identifier              {bootmgr}
device                  partition=\Device\HarddiskVolume2
path                    \EFI\Microsoft\Boot\bootmgfw.efi
description             Windows Boot Manager
locale                  en-US
inherit                 {globalsettings}
bootshutdowndisabled    Yes
flightsigning           Yes
default                 {current}
resumeobject            {ba657dd4-b492-11e8-8577-00155d01121e}
displayorder            {current}
toolsdisplayorder       {memdiag}
timeout                 30

Windows Boot Loader
-------------------
identifier              {current}
device                  partition=C:
path                    \Windows\system32\winload.efi
description             Windows Server 2019 Datacenter
locale                  en-US
inherit                 {bootloadersettings}
```

FIGURE 4-14: Using `bcdedit /set` to alter the description of the Windows Boot Loader entry.