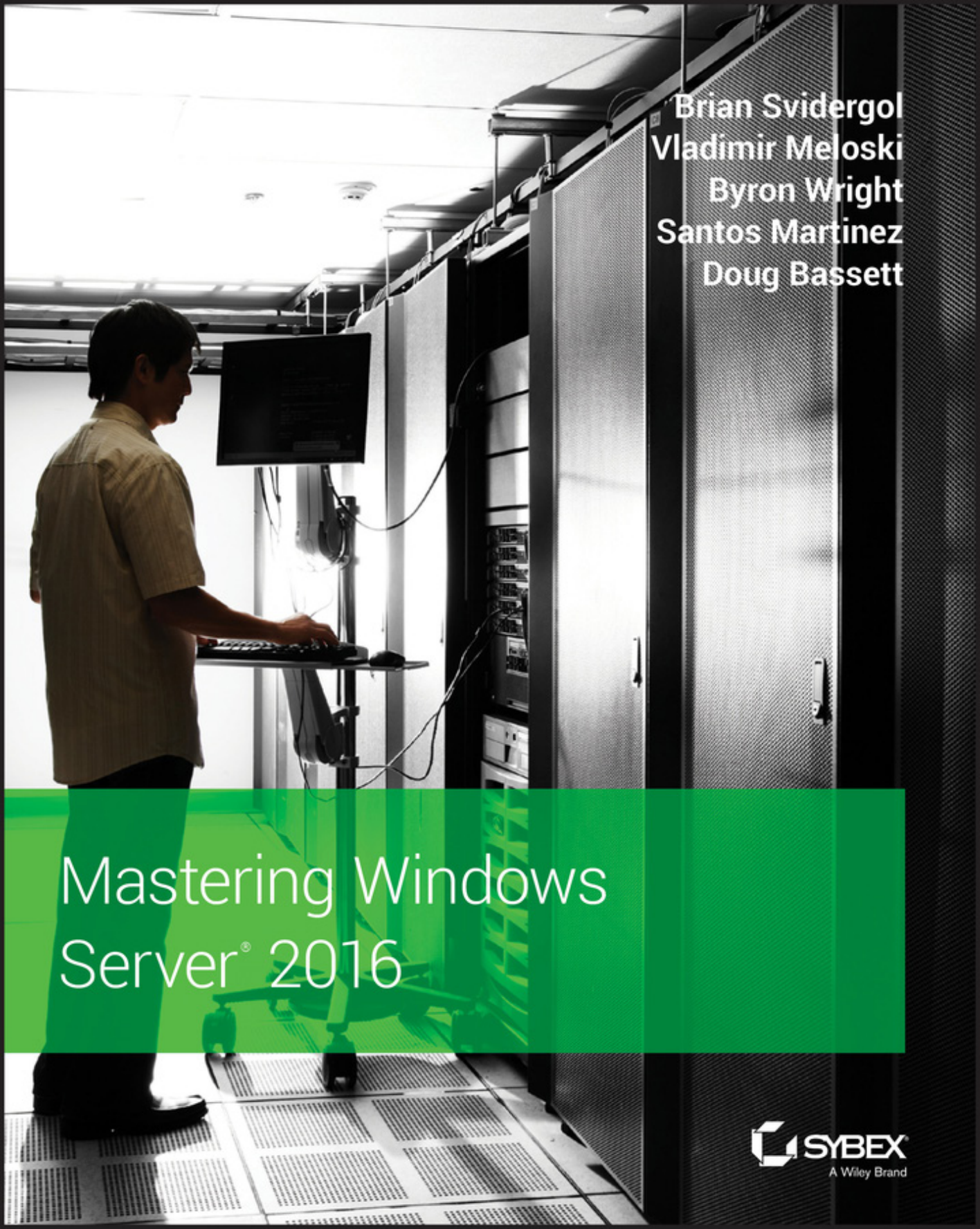
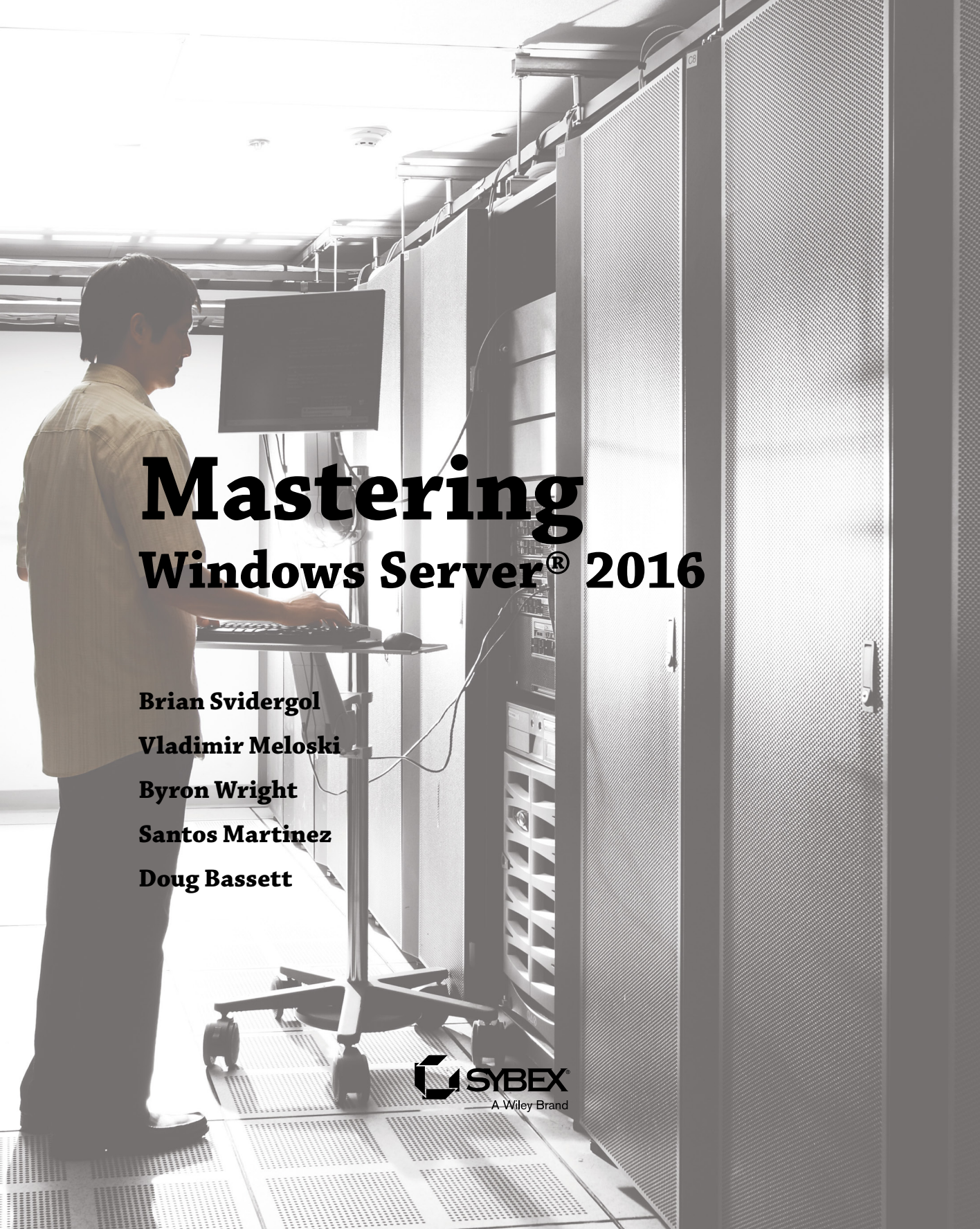


Brian Svidergol
Vladimir Meloski
Byron Wright
Santos Martinez
Doug Bassett

Mastering Windows Server® 2016

SYBEX
A Wiley Brand

Mastering
Windows Server® 2016



Mastering
Windows Server® 2016

Brian Svidergol

Vladimir Meloski

Byron Wright

Santos Martinez

Doug Bassett

SYBEX

A Wiley Brand

Senior Acquisitions Editor: Kenyon Brown
Development Editor: Kim Wimpsett
Technical Editor: Rodney R. Fournier
Production Editor: Barath Kumar Rajasekaran
Copy Editor: Kathy Carlyle
Editorial Manager: Pete Gaughan
Production Manager: Kathleen Wisor
Proofreader: Nancy Bell
Indexer: Johnna VanHoose Dinse
Project Coordinator, Cover: Brent Savage
Cover Designer: Wiley
Cover Image: © Thomas Northcut/Getty Images, Inc.

ISBN: 978-1-119-40497-2
ISBN: 978-1-119-40507-8 (ebk.)
ISBN: 978-1-119-40506-1 (ebk.)

Manufactured in the United States of America

Library of Congress Control Number: 2018935413

10 9 8 7 6 5 4 3 2 1

Acknowledgments

Many talented and hardworking people gave their best efforts to produce *Mastering Windows Server 2016.* We offer our sincerest gratitude to those individuals who helped bring this book to you.

Many thanks go out to the editorial and production teams at Wiley for their efforts. Kenyon Brown managed the project (which took much more effort than he signed up for!) and helped recruit the right resources to make this project happen. Kim Wimpsett, the developmental editor, did a great job turning around the chapters, communicating with the team, and tracking down late chapters. Thanks! We also want to thank the technical editor, Rodney Fournier, for his work reviewing all of the work and ensuring that we have things right. Finally, we want to thank the production editor, Barath Kumar Rajasekaran; the copy editor, Kathy Carlyle; and the proofreader, Nancy Bell. All of them contributed to making this book a high-quality production.

I'd like to thank my wife, Lindsay; my son, Jack; and my daughter, Leah, for their continued support and for the joy they bring me regularly.

–Brian Svidergol

To my loving family who always supports me.

–Vladimir Meloski

I'd like to thank Tracey, Sammi, and Michelle for consistently being the best part of my day.

–Byron Wright

I want to dedicate this book to the following: my wife, Karla; you are my soulmate, and I want to grow old with you. To my kids, Bryan and Naomy, I hope this gives you some inspiration one day of what you can possibly achieve; and finally thank you to all my family and friends for their support in my craziness. Also to my martial arts students, peers, and masters, thank you for allowing me to be who I am as a professional and a martial arts master.

I want to thank my colleagues across Microsoft for their support on this book. Thank you to the contributing authors for their great work and especially to Jose Rodas for his commitment and dedication to the OMS and Operations Manager Technology and for his contributions to making the content of this book better.

To my peer author, Brian Svidergol, thanks for the opportunity and making this happen for us. To my friend Elias Mereb, as he continues to evolve and assist us in many ways, thanks

Brother for all your feedback and commitment to Windows technology. Finally, I want to thank all the Configuration Manager and the Enterprise Mobility + Security community, who have always been so passionate about the technology and willing to help us improve our writing. Let's keep it up as we evolve together.

–Santos Martinez

I dedicate this book to my grandmother, Helen Wells, who bought me my first computer, and to my grandfather, Lyle Wells, for not killing her.

–Doug Bassett

About the Authors

Brian Svidergol designs and builds infrastructure, cloud, and hybrid solutions. He holds many industry certifications including the Microsoft Certified Trainer (MCT) and Microsoft Certified Solutions Expert (MCSE) – Cloud Platform and Infrastructure. Brian is the author of several books covering everything from on-premises infrastructure technologies to hybrid cloud environments. He has worked with startup organizations and large Fortune 500 companies on design, implementation, and migration projects.

Vladimir Meloski is a Microsoft Most Valuable Professional on Office Server and Services, Microsoft Certified Trainer and consultant, providing unified communications and infrastructure solutions based on Microsoft Exchange Server, Skype for Business, Office 365, and Windows Server. With a bachelor's degree in computer sciences, Vladimir has devoted more than 20 years of professional experience in information technology. Vladimir has been involved in Microsoft conferences in Europe and in the United States as a speaker, moderator, proctor for hands-on labs, and technical expert. He has been also involved as an author and technical reviewer for Microsoft official courses, including Exchange Server 2016, 2013, 2010, 2007, Office 365, and Windows Server 2016, 2012; and he is one of the book authors of *Mastering Microsoft Exchange Server 2016*. As a skilled IT professional and trainer, Vladimir shares his best practices, real-world experiences, and knowledge with his students and colleagues, and he is devoted to IT community development by collaborating with IT Pro and developer user groups worldwide. He enjoys his spare time in country with his son and wife.

Byron Wright is the owner of BTW Technology Solutions where he designs and implements solutions using Microsoft technologies. He has been a consultant, author, and instructor for 20 years, specializing in Windows Server, Active Directory, Office 365, and Exchange Server. Byron was a Microsoft MVP for Exchange Server/Office 365 from 2012–2015.

Santos Martinez was born in Caguas, Puerto Rico, in 1982, and grew up in Caguas. Santos has more than 18 years of experience in the IT industry. He has worked on major implementations and in support of Configuration Manager and Enteprise Mobility + Security for many customers in the United States and Puerto Rico. Santos was a Configuration Manager engineer for a Fortune 500 financial institution and an IT consultant before joining Microsoft. For the Fortune 500 companies, he helped with the implementation and support of more than 200+ Configuration Manager Site Server and support of more than 300,000 Configuration Manager and Intune clients worldwide.

Santos was a SQL Server MVP from 2006 to 2009 and then a ConfigMgr MVP from 2009 to 2011. He is well known in the Microsoft communities as a mentor for other MVPs, Microsoft FTEs, and for helping other IT community members. He has also participated in Microsoft TechEd, MMS, and Ignite as a technical expert for Configuration Manager, Database, and Microsoft Intune. Santos is also a former Puerto Rican martial arts champion and currently holds a Six Degree black belt in TaiFu-Shoi Karate-Do where he earned the title of Shihan Sensei.

Santos and Karla, a pastry chef, have been married for 16 years and have two kids, Bryan Emir and Naomy Arwen. Santos currently is a senior program manager for Microsoft in the Enterprise Management and Mobility Product Group. You can follow him on Twitter (`@ConfigNinja`) or at his blog (`http://aka.ms/ConfigNinja`).

Doug Bassett has been involved in the computer industry since the early 1980s when he taught a high school computer science class, while still a high school student. Doug has many certifications from Microsoft, Cisco, CompTIA, and others, and has been MCSE certified since the old Windows NT days. Doug has also been a Microsoft Certified Trainer (MCT) for over 20 years. He was one of the first 100 people in the world to certify on Windows 2008. Doug has lectured at both Apple and Microsoft corporate headquarters and was invited by Microsoft to present at the Microsoft world conference in Barcelona, Spain, on virtual classroom and online learning. Doug is currently teaching live classes over the Internet and enjoys not having to shovel snow while living in Arizona.

About the Contributing Author

Jose Rodas is an IT professional certified as A +, CCEA, MCSA + M, MCSE, MCTS, MCITP EA, and MCT, and he has more than 20 years of industry experience. He started working at Microsoft in the System Center Team in October 2007 supporting System Center Operations Manager and System Center Service Manager. Currently, he is a Microsoft Premier Field Engineer dedicated to customers while traveling to customer sites to provide proactive/reactive assistance in System Center and Azure Log Analytics projects.

Contents at a Glance

Contents

Introduction

Welcome to *Mastering Windows Server 2016*. This book covers Windows Server 2016 and the core technologies built into the operating system. It has a mix of content ranging from networking, identity and access, storage, and much more. We don't cover every single feature or option but focus on providing a deep understanding of the key topics that we cover throughout the chapters. This book is best read from front to back and can later used as a reference.

Major Changes in Windows Server 2016

Most of the major components of Windows Server 2016 have new features, enhancements, and changes for Windows Server 2016. With that said, most of the changes involve improvements to existing services and the introduction of new features. Throughout the chapters, we will look at some of these new features in detail. The following major changes represent the changes that we feel stand out from the rest:

Nested Virtualization With nested virtualization, a brand new feature for Windows Server 2016, you can deploy a Hyper-V host inside of a VM. This simplifies the process for testing failover clustering and for testing a variety of virtualization-related features and configurations. Note that nested virtualization is best suited for nonproduction environments, such as a lab environment. See Chapter 3 for more information.

Shielded Virtual Machines This new feature enhances the security of Hyper-V hosts and VMs. It protects against scenarios such as malicious administrators trying to view the console or trying to view the data on the virtual hard disks. See Chapter 3 for more information.

Device Guard and Credential Guard These new features protect Generation 2 VMs against exploits. See Chapter 8 for more information.

Privileged Access Management (PAM) PAM enhances the security of Active Directory Domain Services environments by completely changing the way many administrators manage their environments. See Chapter 9 for more information.

Storage Spaces Direct This new feature provides a highly available and highly scalable storage solution using local server storage. See Chapter 4 for more information.

Software Defined Networking (SDN) There are many new enhancements to networking in Windows Server 2016. SDN enables you to configure your on-premises environment like Azure and manage it using System Center Virtual Machine Manager. See Chapter 5 for more information.

Containers Containers are a feature that offers a way for app teams to have a prepackaged way to deploy app environments quickly (for example, IIS with ASP.NET). The container contains everything an app team needs—and the container is portable; it can run on-premises or in the public cloud. See Chapter 7 for more details.

Nano Server When Microsoft introduced the Server Core installation of Windows Server, it was lauded for the small size, small requirements, high performance, and enhanced security. Nano Server went a step further (albeit with more limitations). Initially, it was just a smaller footprint deployment, without a GUI, that could run some core roles such as Hyper-V and Scale-Out File Server. However, recently Microsoft announced some big changes for Windows Server 2016 (release 1709). With 1709, Nano Server will no longer support the core roles such as Hyper-V. Instead, it will be dedicated for containers and be geared for the cloud. Nano Server is introduced in Chapter 1.

The Mastering Series

The *Mastering* series from Sybex provides outstanding instruction for readers with intermediate and advanced skills in the form of top-notch training and development for those already working in their field, and clear, serious education for those aspiring to become pros. Every *Mastering* book includes the following:

- Skill-based instruction with chapters organized around real tasks rather than abstract concepts or subjects
- End of chapter "Master It" scenarios to test your knowledge of the information in the chapter

How to Use This Book

How you use this book will depend on your goals and your level of experience across the Windows Server technologies. For example, if you have limited experience with Windows Server, then reading the book from front to back might provide the best experience. If you are an experienced server administrator but want to learn more about the networking components of Windows Server 2016, then you might want to go straight to the networking-related chapters. If you are studying for a certification exam, you might want to read specific topics from various chapters to strengthen your knowledge in very specific areas. While the book is ordered so that it is easiest to read it front to back, take the path that best suits your experience and goals.

In several parts of the book, we will perform step-by-step installations and configurations. We highly recommend that you perform those same steps in your lab or nonproduction environment (whether at home or at work). Reading about a technology is good for learning. Deploying, troubleshooting, and maintaining a technology is good for learning. Doing both is great for learning!

Windows Server is a huge product. There is a plethora of technologies in it—and the technologies are complex, much more so than in previous versions (especially older and legacy versions) of Windows Server. Therefore, as authors, we must pick and choose exactly what we cover while still trying to keep the book manageable in size. In general, for this book, we have opted to cover the most used parts of Windows Server, and we try to go into detail in specific parts of

every chapter. Lastly, we avoid the introductory information unless it is imperative to the topic. Our readers have historically been experienced administrators who are looking to enhance their knowledge of the newest version of Windows Server. Therefore, we try to avoid material that is "too basic" for our typical reader.

How This Book Is Organized

Each *Mastering Windows Server 2016* chapter represents a milestone in your progress toward becoming an expert Windows Server 2016 user. We start off by walking you through the installation, Server Manager, and PowerShell. It is a good way to start and enables you to have a Windows Server 2016 computer to reference while working through the step-by-step sections of chapters. It is also good to know the tools that we are going to reference throughout the book (especially PowerShell) before we dive into them!

- Chapter 1, "Windows Server 2016 Installation and Management," shows you how to install Windows Server 2016 and how to work with Server Manager for server administration.
- Chapter 2, "PowerShell," details how to work with PowerShell. It covers a huge amount of information in a single chapter and will be especially beneficial to readers who aren't well-versed in PowerShell yet.

After you have an installation and know your way around the management of Windows Server, you are ready to dive deeper into the foundational technologies.

- Chapter 3, "Compute," is all about the compute portions of Windows Server, such as Hyper-V and failover clustering.
- Chapter 4, "Storage," details file systems, data deduplication, Storage Spaces, Storage Replica, and Storage Quality of Service.
- Chapter 5, "Networking," dives into remote access, DNS, DHCP, and a host of new networking technologies in Windows Server 2016.

At this point, you'll have a pretty good grasp of the basics of Windows Server 2016 and understand some of the new technologies. The next chapters are designed to help you branch out into smaller (but still important) technologies in Windows Server.

- Chapter 6, "File Services," tells you how to implement and manage file services—not just shared folders but the advanced aspects of managing file services.
- Chapter 7, "Windows Server Containers," explains what containers are, how they work, and how to create and manage them. This technology is new and rapidly evolving.
- Chapter 8, "Security Mechanisms," is where you'll learn about Just Enough Administration (JEA), Just In Time (JIT) administration, Credential Guard, and other new security features in Windows Server 2016.

Several Active Directory technologies are built into Windows Server 2016. In this book, we cover the three most deployed. We exclude AD LDS and AD RMS.

- Chapter 9, "Active Directory Domain Services," covers AD DS, including information about design and architecture, deployment, and day-to-day administration.
- Chapter 10, "Active Directory Certificate Services," covers AD CS and public key infrastructure technologies. It also walks through a step-by-step two-tier hierarchy.
- Chapter 11, "Active Directory Federation Services," takes you through AD FS and design considerations. Then, it walks you through a step-by-step implementation of AD FS and Web Application Proxy.

Earlier in the book, we cover managing servers one at a time with Server Manager and PowerShell. In this part of the book, we look at managing servers at the enterprise level where automation and self-service are keys to successful management.

- Chapter 12, "Management with System Center," introduces you to the entire suite of Microsoft System Center. It walks through deployment and configuration, as well as introduces the concepts around enterprise management.
- Chapter 13, "Management with OMS," shows you how to use Microsoft Operations Management Suite OMS), an Azure service, to manage your on-premises and cloud-based Windows servers.

Getting More Information

In each chapter, you will see links to external sources for additional information. Whenever you have an interest in a particular topic and we link to an external resource, you should opt to spend a few minutes exploring that content. We specifically tried to link to value-adding material that complements and sometimes expands upon the information in the book.

Errata

We hope that *Mastering Windows Server 2016* will be of benefit to you and that, after you've read the book, you'll continue to use the book as a reference. Please note that while we have made every effort toward accuracy, sometimes software updates will cause a screenshot to look slightly different than the interface you see on your screen. You should still be able to follow along with the instructions given. However, if you find errors, please let our publisher know by emailing to `errata@wiley.com`.

Thanks for choosing *Mastering Windows Server 2016*!

Chapter 1

Windows Server 2016 Installation and Management

Windows Server 2016 builds on the installation and management processes of earlier Windows Server versions. To install Windows Server 2016, you need to understand the editions of Windows Server 2016 and how they are licensed. This will enable you to select the edition of Windows Server 2016 that best meets your needs. You also need to select an appropriate installation method such as automation with Windows Deployment Services.

After installing Windows Server 2016, Server Manager is the main interface that you'll use for management. From Server Manager, you can launch tools that you can use to manage and monitor Windows Server 2016.

IN THIS CHAPTER, YOU WILL LEARN TO:

- Define a deployment process
- Select an edition of Windows Server 2016
- Select an activation method
- Monitor Windows Server 2016

Windows Server 2016 Editions and Licensing

Microsoft has had various editions of Windows Server with each generation. Depending on the generation of Windows Server, varying editions came with different features or different licensing. You can obtain Windows Server 2016 Standard or Windows Server 2016 Datacenter. The vast majority of features are the same between the two editions, but there are some significant differences worth noting and they are listed in Table 1.1.

Table 1.1: Windows Server 2016 Edition Differences

Feature	Description
Virtualization Licensing	One Windows Server 2016 Standard license can be used for two virtual machines on a single virtualization host. One Windows Server 2016 Datacenter license can be used for an unlimited number of virtual machines on a single virtualization host.

Table 1.1: Windows Server 2016 Edition Differences *(continued)*

Feature	Description
Software Defined Networking	This feature that applies policies to control network configuration and security is not included in Standard edition.
Shielded Virtual Machines	To configure Shielded virtual machines, the Hyper-V host must be running Windows Server 2016 Datacenter edition.
Hyper-V Containers	Windows Server 2016 Standard has a limit of two Hyper-V Containers per Hyper-V host. Windows Server 2016 can have an unlimited number of Hyper-V Containers. Both editions of Windows Server 2016 can have an unlimited number of standard containers.
Storage Replica	This feature that synchronizes data between two servers is available only in Windows Server 2016 Datacenter edition.
Storage Spaces Direct	This feature that provides high availability for file shares is available only in Windows Server 2016 Datacenter edition.

As you can see from Table 1.1, there are only a few feature differences between Windows Server 2016 Standard and Windows Server 2016 Datacenter. If those features are not required, then the primary driver for selecting an edition of Windows Server 2016 is usually virtualization licensing.

Most organizations deploy new servers as virtual machines. With a single Windows Server 2016 Standard license, you can install Windows Server 2016 Standard with Hyper-V for a virtualization host and configure two virtual machines with Windows Server 2016 Standard. By purchasing a second Windows Server 2016 Standard license, you can add two more virtual machines running Windows Server 2016 Standard. In smaller organizations with only a few virtual machines per virtualization host, it is often cost-effective to use Windows Server 2016 Standard.

In larger organizations with many virtual machines, it is often more cost-effective and easier to manage if you use Windows Server 2016 Datacenter. With a single Windows Server 2016 Datacenter license, you can install Windows Server 2016 Datacenter with Hyper-V for a virtualization host and configure an unlimited number of virtual machines on that host.

Virtualization Licensing without Hyper-V

Hyper-V is an excellent hypervisor that is widely used to implement server and desktop virtualization. However, there are other hypervisors such as VMware, XenServer, and others. When you use a hypervisor other than Hyper-V, the licensing for the virtual servers works exactly the same as if you were using Hyper-V. A Windows Server 2016 Standard license allows you to implement two virtual machines running Windows Server 2016 Standard on any hypervisor. A Windows Server 2016 Datacenter license allows you to implement an unlimited number of virtual machines running Windows Server 2016 Datacenter on any hypervisor.

Processor Core-Based Licensing

At one time, before virtualization became common, Windows Server was licensed based on a ratio of one-to-one with physical machines. Older editions of Windows Server were limited based on the number of physical processors and the amount of memory they could address. When virtualization became common, a number of virtual machines were included per license. Now, physical hardware has become so powerful that limitations have been introduced based on the number of processor cores in the physical server.

Windows Server 2016 Standard and Windows Server 2016 Datacenter use the same core-based licensing structure. The base operating system license provides licensing for two eight-core processors (a total of 16 cores). If there are more than eight physical cores per processor (hyperthreading does not count as additional cores), then you need to purchase additional core licenses in minimum increments of two cores.

Each processor in a server must be licensed for a minimum of eight cores. So, if you have four processors in a server, then you need to be licensed for a minimum of 32 cores. You can meet this requirement by purchasing two Windows Server licenses. In the case of Windows Server 2016 Standard, this would give you rights to install two virtual machines. To allow four virtual machines, you would need to fully license all processors in the server again.

Client Access Licenses

On a Windows-based network, you need to license your clients in addition to the servers. A Client Access License (CAL) provides users or devices with rights to access services that are running on the servers. For example, if a computer is joined to the domain and a user signs in to the network, then a CAL is required. That CAL can be a user CAL for the person who is connecting to the network. The CAL can also be a device CAL for the computer that is being used to connect to the network. Only one CAL is required, either a user CAL or a device CAL.

When you purchase CALs, you need to determine whether user or device CALs are most cost-effective for your organization. If a single user has multiple devices that access network services, such as a desktop computer and laptop computer, then a user CAL is most cost-effective. If a single device is used by multiple users, such as a call center with multiple shifts, then a device CAL is most cost-effective. You can combine user and device CALs as you deem appropriate.

CALs are paper-based licensing. This means that you need to track your users and devices accurately, but Windows Server 2016 does not monitor licenses in use. You also do not need to specifically assign your licenses to user accounts or computers.

Licensing Programs

Microsoft has a variety of different licensing programs with different benefits, restrictions, and costs. You can obtain Windows Server 2016 licenses and CALs through a number of these programs. As these programs change over time, you'll need to talk with an expert about how you should purchase your licenses. However, here is a high-level overview of a few licensing methods:

- Original Equipment Manufacturer (OEM). This type of licensing can be purchased when you buy a new physical server. It is generally the least expensive option but cannot be moved to other hardware.
- Volume license. This type of license is more flexible than OEM licensing because it is not restricted to a specific physical server. The frequency that you can move this license

between servers is restricted. This is an important consideration for high-availability scenarios where virtual machines can move between virtualization hosts.

- Software assurance. This type of license is added on to volume licensing to include software upgrades. Software assurance also offers additional benefits such as the ability to move licenses between physical servers as often as you like.
- Enterprise agreement. This type of licensing is user-based rather than server-based. For a set fee per user in the organization, you can run the number of server instances necessary to meet your needs. This type of license also includes CALs and may include other products such as SQL Server and Exchange Server.

Other Editions of Windows Server 2016

Windows Server 2016 Essentials is an edition of Windows Server 2016 that is targeted at small businesses. Licensing for this edition of Windows Server 2016 is simpler than Standard or Datacenter editions because it does not require CALs. Instead, Windows Server 2016 Essentials has a limit of 25 users and 50 devices. There are also no virtualization rights for multiple instances, a 64 GB limit on memory, and a limit of two physical CPUs. To simplify deployment some server roles and features are automatically installed and configured.

Windows Storage Server 2016 is available only through hardware vendors for storage appliances. There are a limited number of server roles because this edition is designed to be a general-purpose operating system. For example, you can't configure Windows Storage Server 2016 as a domain controller.

For more information about Windows Server 2016 licensing, see Windows Server 2016 Licensing & Pricing at `https://www.microsoft.com/en-us/cloud-platform/windows-server-pricing`.

Installing Windows Server 2016

Physical servers are specialized hardware that often require drivers that are not included as part of Windows Server 2016. Before you begin installing, you should obtain all the necessary drivers for your server. Some manufacturers have a specialized process for installing Windows Server 2016 that injects the drivers during the installation process.

The firmware for a modern server is Unified Extensible Firmware Interface (UEFI) rather than the older Basic Input Output System (BIOS). Although you can set UEFI firmware to legacy mode to emulate BIOS, there is no need to do that. Windows Server 2016 can be booted using UEFI firmware. Additionally, using UEFI provides advantages such as booting from larger disks and a more secure boot process.

Real World Scenario

Installing in Virtual Machines

It's likely that you'll be deploying most servers as virtual machines. Virtual machines provide a lot of flexibility for deployment and management. To work properly in a virtual environment, Windows Server 2016 needs to have the correct drivers for that virtual environment, just as Windows Server 2016 needs to have the correct drivers to work properly on physical hardware.

When you install Windows Server 2016 in a virtual machine on a Hyper-V host, the installation files include all the necessary drivers. If you create a Generation 1 virtual machine, it emulates BIOS firmware. If you create a Generation 2 virtual machine, it uses UEFI firmware. Windows Server 2016 works properly with either type of firmware.

If you install Windows Server 2016 in a virtual machine using another type of hypervisor, such as VMware, then you generally need to install additional drivers. For example, you would install VMware Tools for virtual machines running on VMware.

Before installing, you should also plan the disk partitioning for your server. A key consideration is the size of the C: drive that is used for the operating system. The C: drive needs to be large enough to support not only the initial installation of Window Server 2016, but also any updates that are installed over time. Additionally, most organizations keep applications and data on separate partitions from the operating system whenever possible. Separating applications and data from the operating system helps to prevent the operating system drive from running out of space and can simplify backup and restore.

Installation Steps

To begin installing Windows Server 2016, ensure that your server is configured to boot from DVD. This will be a configuration option in the firmware. Place the installation DVD in the DVD drive and complete the following process.

1. Start the server and press a key, when prompted, to start installing from DVD.
2. Select a language, time and currency format, and a keyboard layout that are appropriate for your location, as shown in Figure 1.1, and click Next.
3. Click Install Now.
4. In the Activate Windows window, enter your product key and click Next. If you select I Don't Have a Product Key, you can enter the product key later.
5. In the Select the Operating System You Want to Install window, select the operating system version you want to install, as shown in Figure 1.2, and then click Next.

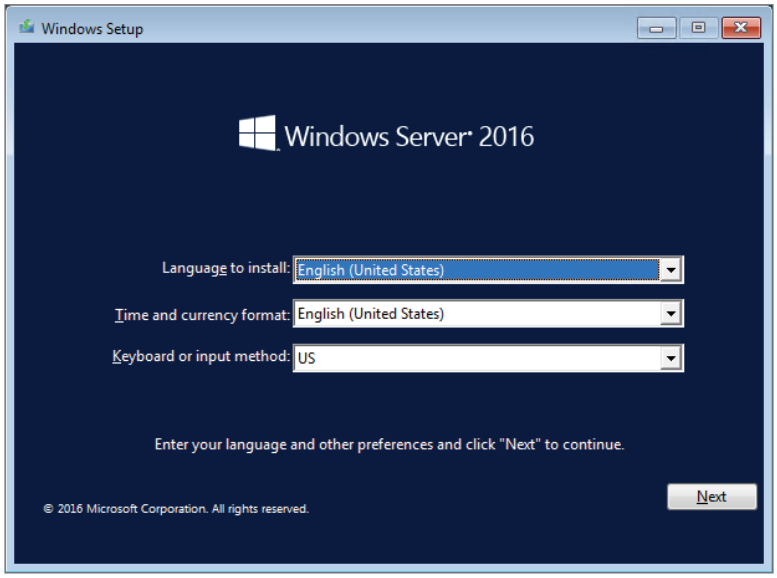


FIGURE 1.1
Select localization settings

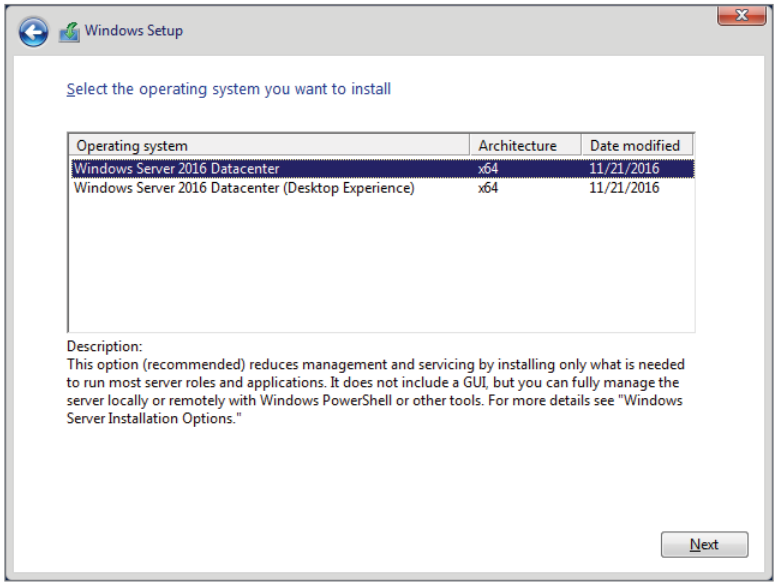


FIGURE 1.2
Select an operating system.

6. In the Applicable Notices and License Terms Window, select the I Accept the License Terms check box and click Next.

Server Core and Desktop Experience

When you install Windows Server 2016 Standard or Datacenter edition, you have the option of installing Server Core or Desktop Experience. The Desktop Experience is the full server installation that includes the graphical interface. This installation type can run all the management tools at the server console. In Windows Server 2012 R2, you could add or remove the graphical interface. This is not possible in Windows Server 2016.

Server Core is a stripped-down version of Windows Server 2016 that does not include the graphical interface. To manage Server Core, you can use a command prompt or Windows PowerShell locally. To use graphical tools, you can use the Remote Server Administration Tools (RSAT) in Windows 10.

A subset of server roles is available in Server Core. These roles include most of the network services such as DNS, DHCP, Active Directory Domain Services (AD DS), Active Directory Certificate Services, File Services, and Windows Server Update Services. If you are running applications on the server, you need to verify that the applications are compatible with Server Core.

The limited functionality in Server Core, reduces the attack surface of the operating system. It also reduces the need to update and consequently increases uptime. Disk utilization is also reduced, which allows more efficient disk utilization in large-scale virtualization.

7. In the Which Type of Installation Do You Want window, shown in Figure 1.3, click Custom: Install Windows Only (Advanced). Performing an in-place upgrade from one server operating system version to another is rare. It is more common to install a new server and migrate services and applications to the new server.

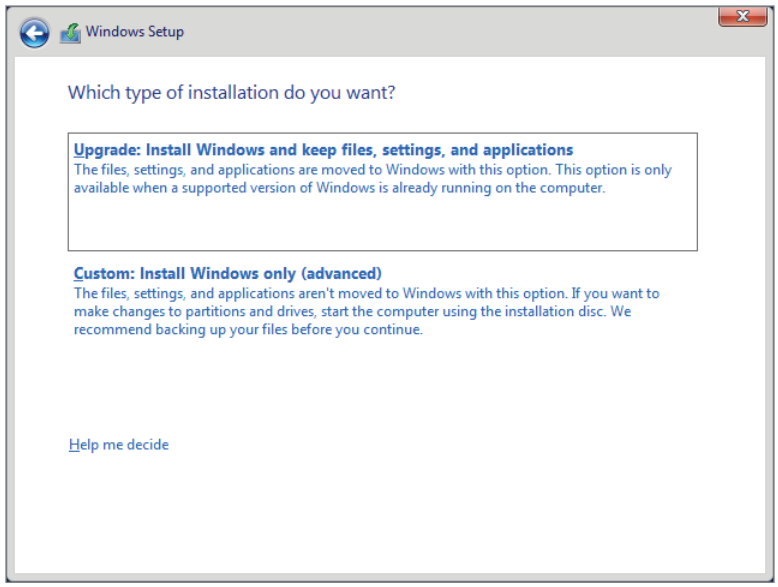


Figure 1.3
Select an installation type.

8. In the Where Do You Want to Install Windows window, shown in Figure 1.4, select the correct drive for the operating system installation and click Next. If your disk is not displaying in this window, then you can use the Load Driver option to install the missing storage driver. You also have the option manually create and delete partitions.

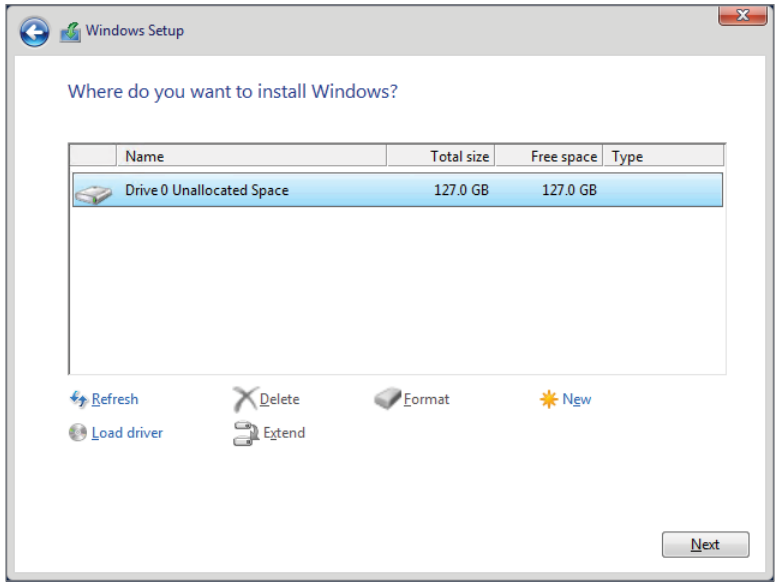


FIGURE 1.4
Select the installation location.

Boot and System Partitions

When the server is using UEFI firmware and you allow the Windows Server 2016 installation process to create partitions on the disk, it will create three partitions:

- Recovery partition. This partition is 450 MB and contains the recovery tools for Windows Server 2016. If Windows Server 2016 can't start, then the server boots from this partition and you can use these tools to attempt recovery.
- EFI system partition. This partition is 100 MB and stores the operating system files that are required to begin the Windows Server 2016 boot process.
- Boot partition. This partition uses the remainder of the disk and stores the Windows Server 2016 operating system files. This partition is also used to store the paging file.

If the server is using legacy BIOS firmware, only two partitions are created:

- System partition. This 500 MB partition contains files used to start the Windows Server 2016 boot process and files used for recovery.
- Boot partition. The partition uses the remainder of the disk and stores the Windows Server 2016 operating system files. This partition is also used to store the paging file.

9. Wait while files are copied and the installation finishes. This can take up to 30 minutes if your server or disks are slow.
10. After the server reboots, on the Customize Settings screen, in the Password and Reenter Password boxes, type a password for the local Administrator account and click Finish.

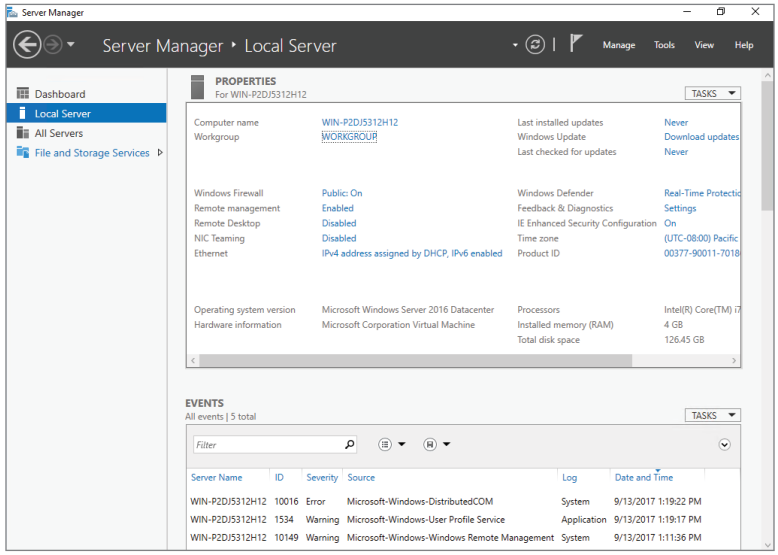
Post-Installation Configuration

To simplify the installation process for Windows Server 2016, many settings have a default value. However, you'll probably want to change these four items right away:

- Computer name. During installation, a computer name is generated automatically in the format of WIN-*RandomString*. You'll want to change that computer name to match the naming standard used by your organization.
- Workgroup. Each computer is automatically a member of a workgroup named WORKGROUP. In most cases, you'll want to join the domain.
- IPv4 address. IPv4 is configured to obtain an IP address automatically from DHCP after installation. Most organizations set a static IPv4 address rather than using DHCP.
- Time zone. The default time zone (UTC-08:00) Pacific Time (US & Canada). Change the time zone to match where the server is located.

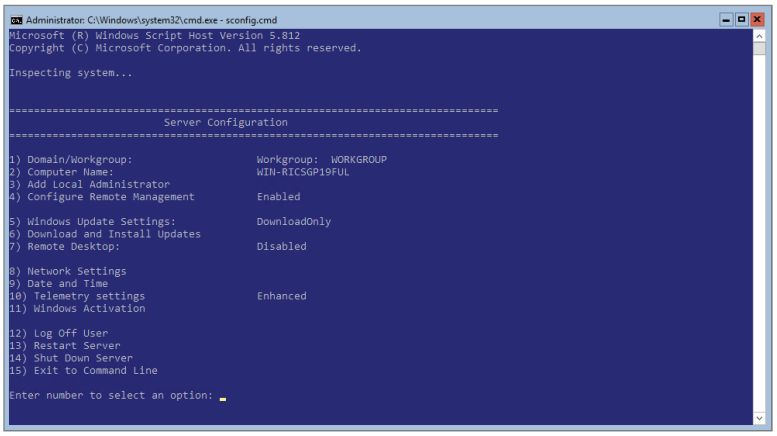
If the Desktop Experience is installed, you can use Server Manager, shown in Figure 1.5, to configure these items. You can also use Server Manager to review and configure other common settings.

FIGURE 1.5
Server Manager



If Server Core is installed, you need to use either command-line tools or Windows PowerShell to configure these items. To simplify configuration of Server Core, you can use `sconfig.cmd`, shown in Figure 1.6. This script is included with Server Core and provides a menu-driven interface for configuring common items.

FIGURE 1.6
`Sconfig.cmd`



Activation

All editions of Windows Server 2016 need to be activated. Activation is what proves that your license key is valid. If you do not activate a copy of Windows Server 2016, it will enter notification mode after 180 days. In notification mode, you will receive reminders to activate and some features such as personalization will be disabled.

Smaller organizations might purchase Windows Server 2016 with the physical servers. The original equipment manufacturer (OEM) licenses are less expensive than volume licensing but cannot moved to another physical server. So, if a physical server is retired, the license is retired with it.

OEM licenses are activated by contacting Microsoft. Typically, you activate the server over the Internet, but you can also do it by phone.

Larger organizations typically purchase volume licenses that are more flexible. Volume licenses can be moved among physical servers. Volume licenses also have more options for activation.

A Multiple Activation Key (MAK) can be activated more than once. The number of activations is tracked by Microsoft, but you are responsible for ensuring that the correct number of licenses is being used. Activation for a MAK key can be done over the Internet or by phone.

A Key Management Service (KMS) key allows new servers to activate automatically within your organization and does not require the new servers to communicate over the Internet. This is important because most organizations do not allow servers to communicate with the Internet. Table 1.2 describes the activation methods for using KMS keys.

Table 1.2: Activation Methods for Using KMS Keys

Method	Description
KMS host	You can configure Windows Server 2016 to be a KMS host. Then you can add the KMS key to the KMS host. When you add the KMS key to the KMS host, it is activated with Microsoft. However, new servers activate by contacting the KMS host. A KMS host has minimum activation thresholds. For server operating systems, the activation threshold is five. If you have fewer than five servers using a KMS host for activation, then activation never occurs. This makes a KMS host difficult to use for smaller organizations or remote sites.
Active Directory-Based Activation	When you implement Active Directory-Based Activation, the activation information is stored in Active Directory instead of on a KMS host. Because the new server communicates with Active Directory, there is no single point of failure for activation. Also, there are no minimum activation thresholds for Active Directory-Based Activation. This is the preferred activation method for software that supports it.

To configure a KMS host or Active Directory-Based Activation, install the Volume Activation Services server role in Windows Server 2016. After installing this server role, you run Volume Activation Tools, which allows you to select to enable either KMS or Active Directory-Based Activation and manage keys.

Generic Volume License Keys

When you use KMS or Active Directory-Based Activation, you do not manually install a license key in Windows Server 2016. By default, Windows Server 2016 includes a generic volume license key (GVLK) that activates against KMS or Active Directory-Based Activation.

In rare cases, volume activation fails because someone accidentally changes the key. You can change the key back to the correct GVLK.

For a list of GVLKs, see Appendix A: KMS Client Setup Keys at `https://technet.microsoft.com/en-us/library/jj612867(v=ws.11).aspx`.

For detailed information about volume activation, see Planning for Volume Activation at `https://technet.microsoft.com/en-us/library/dd996589.aspx`.

Automating the Installation of Windows Server 2016

To simplify the installation of Windows Server 2016 in larger organizations, you should automate the process. An automated deployment process reduces the administrative effort required to deploy new servers. So, instead of taking 30 to 60 minutes to perform an installation, you can start the automated process and walk away until it's done.

Automated deployment also provides consistent results. You can define specific sets of features to be installed. For example, you can automatically enable BitLocker to encrypt the local hard disk. With a manual installation, you would need to enable BitLocker as a separate process after the server is deployed.

Windows Server 2016 deployment can be automated a few different ways. Some options have no additional cost, while others use tools you'll need to buy. If your environment is virtualized, you'll have additional options.

Sysprep and Imaging

Imaging is the process of taking a prepared computer and copying its configuration. The image that you take of the prepared computer is stored in a file, and that image can be applied to other physical computers or virtual machines.

When you install Windows Server 2016, it configures system-specific information such as the computer name, hardware information, and a local machine internal security identifier (SID). Those system-specific configuration items need to be removed as part of the imaging process. When those items are removed, the image can be applied to a computer running different hardware.

The Sysprep (System Preparation) utility is included in Windows Server 2016 to prepare the operating system for imaging. Sysprep removes the computer name, hardware information, and SID. Then when the image is applied to a new computer, those items are re-created.

Sysprep Options

`Sysprep.exe` is stored in `C:\Windows\System32\Sysprep`. When you run Sysprep with the graphical interface, you need to select a system cleanup action, as shown in Figure 1.7. The system cleanup action controls what happens after Sysprep runs and the operating system is restarted.

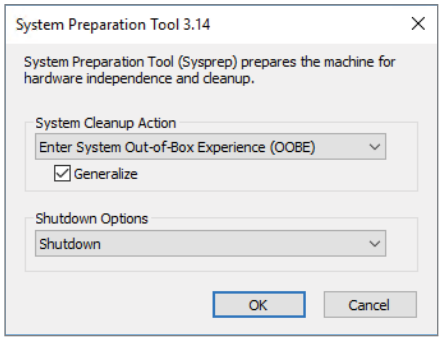


Figure 1.7
Sysprep graphical interface

The two system cleanup actions are

- Enter System Out-of-Box Experience (OOBE). This option causes Windows to run the OOBE process that occurs during the installation of Windows. During the OOBE process, a new computer name is generated and you are prompted for a new administrator password.

- Enter System Audit Mode. This option is used for maintenance of the image. Instead of running OOBE, the operating system starts and you can perform tasks such as adding drivers and updates. After modifying the image, you can put it into audit mode again or OOBE to ready it for deployment.

When preparing an image for deployment, you should select the Generalize option. This option removes computer-specific information such as the computer name, SID, and hardware drivers.

The three shutdown options are

- Quit. Sysprep will quit and the operating system will remain running. You will need to shut down the operating system to capture the image.
- Reboot. The computer will restart and enter the mode defined by the system cleanup action. This is not appropriate if you want to capture the image.
- Shutdown. The computer will shut down after Sysprep completes. This is the option you should use before capturing the image.

Real World Scenario

Running Sysprep for Virtualization

You are creating a new Windows Server 2016 image for deployment. One of the complaints you had in previous deployments after using Sysprep was that it took a long time for new images to detect the hardware. When many servers were being deployed, it significantly slowed down the deployment process.

To speed up the initial configuration of each VM, you can use the `/mode:vm` option when you run Sysprep. This will prevent generalization from removing the hardware drivers. Leaving the hardware drivers in place significantly speeds up the deployment process for new virtual machines.

When you use `/mode:vm`, the image will be specific to a hypervisor. So, an image you create from a Hyper-V virtual machine would not be appropriate to use on VMware hypervisor.

DISM

Many tools are available to perform imaging. Some of those tools allow you to capture all the partitions on a disk, and some only do one partition at a time. The Deployment Image Servicing and Management (DISM) tool included with Windows Server 2016 images the contents of one partition at a time and stores the image in a `.wim` file. It is a file-based imaging tool.

The `.wim` format used by DISM can store multiple images in a single file. When multiple images are stored in the `.wim` file, deduplication is used. If there are multiple copies of the same file, only one copy is stored in the `.wim`, but that copy is available to each image contained in the file.

When multiple images are stored in a single `.wim` file, you need to reference either the index number or name of the image inside the file. The index number is based on the order in which the images were added to the file. The names are assigned as each image is added to the file.

To use DISM to capture an operating system image, the operating system must be shut down to ensure that there are no open files. To run DISM, you need to boot the computer using an alternative operating system. Microsoft provides Windows PE as part of the Windows Assessment and Deployment Kit (ADK). You can configure Windows PE to boot from a USB drive or other boot media.

For more information about Windows ADK and creating Windows PE boot media, see Download WinPE (Windows PE) at `https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/download-winpe--windows-pe`.

When you boot from the Windows PE media, you can run DISM to capture or apply images. Typically, the images are stored on network drives, but they can also be stored on local media such as a USB drive.

If you were capturing the local C: drive to a `.wim` file on a network drive Z:, you would use the following syntax:

```
Dism /Capture-Image /ImageFile:Z:\Win2016.wim /CaptureDir:C: /Name:Win2016Image
```

To apply an image to the local C: drive, you would use the following syntax:

```
Dism /Apply-Image /ImageFile:Z:\Win2016.wim /Name:Win2016Image /ApplyDir:C:\
```

In addition to capturing and deploying images, DISM can also be used to mount and modify images stored in `.wim` files. You can make simple modifications such as adding, removing, or editing files. You can also apply Windows Updates or install new drivers to the image.

Windows System Image Manager

One way to automate the installation of Windows Server 2016 is by using answer files. An answer file provides information to the Windows Server 2016 setup process that modifies the default installation options. For example, you could create an answer file that defines the disk partitions to be created during installation, the install language, and the local Administrator password to avoid the need to interact with Setup during deployment.

The tool that you use to create answer files is Windows System Image Manager (SIM), which is included as part of Windows ADT.

Beyond creating a simple answer file, Windows SIM also creates a distribution share that you can use for deployment (Figure 1.8). In the distribution share, you can store the `.wim` file being used for installation (copied from installation media or customized), drivers to be added during deployment, and updates to be added during deployment. Note that adding drivers and updates during deployment avoids the need to update the image in the `.wim` file.

The installation process for Windows Server 2016 has multiple configuration phases. Settings for unattended installations are applied during specific stages of the installation process. When you add a setting, you might be offered multiple configuration-phase options to which you can add it. You need to ensure that you add the setting to a configuration pass that is being used in your scenario. The configuration passes are listed in Table 1.3.

FIGURE 1.8
Windows SIM

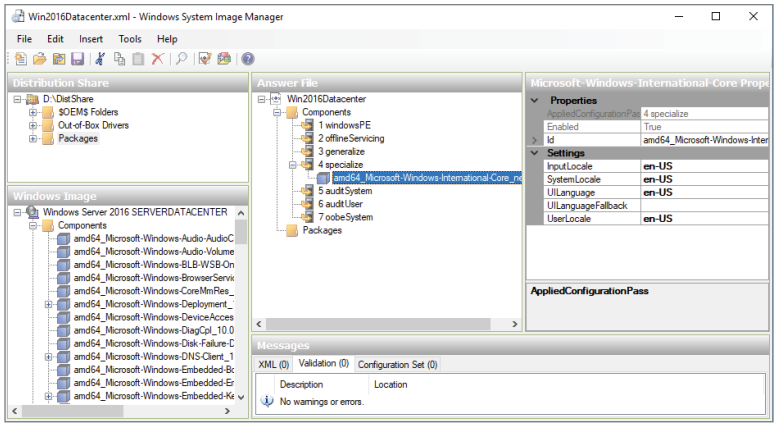


TABLE 1.3: Configuration Passes

Configuration Pass	Description
windowsPE	These settings are implemented when you run `setup.exe` and before the Windows operating is installed. You can include settings required by `setup.exe`, such as the language and keyboard settings. You can also include disk-partitioning information. These settings are not used after an image has been prepared with Sysprep.
offlineServicing	This configuration pass copies and applies drivers and Windows updates. Adding drivers may be required for specialized hardware such as storage drivers that are not included with Windows Server 2016. These settings are not used after an image has been prepared with Sysprep.
Generalize	These settings are applied when you select the Generalize option in Sysprep. These settings are not used when you run `setup.exe`.
Specialize	These settings are applied after Windows detects new hardware and generates the SID.
AuditSystem	These settings are applied only when you enter audit mode after running Sysprep.
AuditUser	These settings are applied only when you enter audit mode after running Sysprep.
oobeSystem	This is the final configuration pass before the user is prompted to sign in.

For detailed information about Windows Configuration passes and using answer files, see Windows Setup Configuration Passes at `https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/windows-setup-configuration-passes`.

Windows Deployment Services

Windows Deployment Services (WDS) is a server role included with Windows Server 2016 as a method for deploying operating system images over the network. You can use WDS to install Windows Server 2016 on new servers or new virtual machines. Some other deployment methods also use WDS as a base set of features on which to build.

Preboot Execution Environment (PXE) is a system that allows all new computers to boot directly from the network. A PXE boot downloads the operating system over the network. WDS uses PXE to download a small operating-system image and either apply or capture images. Table 1.4 lists the image types used by WDS.

Table 1.4: WDS Image Types

Image type	Description
Boot	A boot image is based on Windows PE and is delivered to computers via PXE boot to apply an image containing the desired operating system. The `boot.wim` file included on the Windows Server 2016 installation media displays a menu that allows you to select which image you want to install from the WDS server. If necessary, you can customize the `boot.wim` file with network or storage drivers required for your hardware.
Capture	A capture image is based on Windows PE and is delivered to computers via PXE boot to capture an image containing the operating system of the computer. You need to run Sysprep before the image is captured.
Install	An install image contains the operating system that you want to deploy. A boot image is used to deploy an install image. A capture image is used to collect an install image and store it on the WDS server.
Discover	A discover image is a bootable ISO that contains Windows PE. This ISO can be used with removable media on computers that do not support PXE boot. It is very uncommon to require discover images because almost all computers support using PXE to boot.

Installing WDS

A typical deployment of WDS requires Active Directory, DNS, and DHCP. Active Directory is used for authentication, and the WDS server is a domain member. Client computers to which you are deploying use DNS and DHCP during the deployment process.

When you install the Windows Deployment Services server role, you are prompted to select the Deployment Server and Transport Server role services. You should select both role services to have a fully functional WDS server. The Transport Server role service can be used alone in a lab environment for multicasting images, but this is not typical.

After installation is complete, you must configure WDS. To configure WDS:

1. Open the Windows Deployment Services tool in Server Manager.
2. In Windows Deployment Services, click Servers, right-click the server to be configured, and click Configure Server.
3. In the Windows Deployment Services Configuration Wizard, on the Before You Begin page, click Next.
4. On the Install Options page, click Integrated with Active Directory and click Next.
5. On the Remote Installation Folder Location page, enter a path to store all the images and click Next. Because this directory can become very large, it should not be stored on the C: drive.
6. On the PXE Server Initial Settings page, shown in Figure 1.9, select the option for computers that the server will respond to and click Next. As a best practice, you should select Do Not Respond to Any Client Computers. After you have configured images, you can configure the server to Respond Only to Known Client Computers or Respond to All Client Computers (Known and Unknown). When you respond to unknown devices, you have the option to require administrator approval.

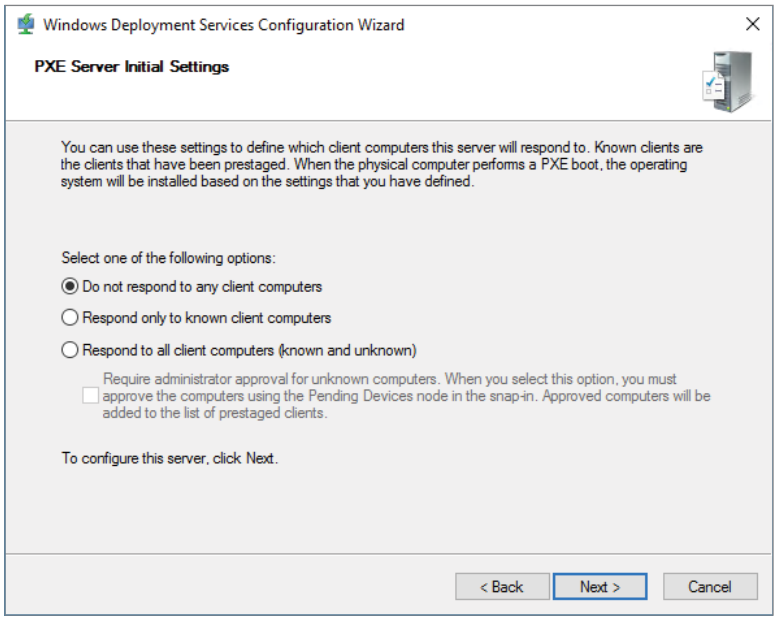


FIGURE 1.9
PXE Server Initial Settings page

7. On the Operation Complete page, click Finish.

The Configuration Wizard configures some of the basic options for the server, but you can view the properties of the server to access additional configuration options such as:

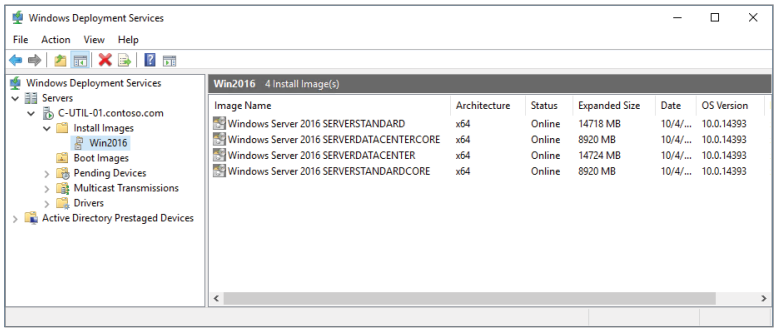
- PXE Response settings. These settings define how PXE responds to clients. If you selected to not respond to any clients during initial configuration, then you need to allow responses here before deploying images.
- AD DS settings. These settings define the format for computer names and which organizational unit in AD DS should store the computer objects.
- Boot settings. These settings define options for the PXE boot process, such as whether pressing F12 is required to boot from PXE.
- Client settings. These settings allow you to provide an answer file that clients will use and whether the client should be joined to the domain.
- DHCP settings. If WDS is deployed on the same server as DHCP, these options need to be enabled to avoid conflicts.
- Multicast settings. These settings define which multicast addresses should be used and whether clients should be split into separate groups based on speed.

Deploying an Image

Before you can deploy images to computers, you need to add at least one boot image and one install image to the WDS server. For the boot image, you can use `boot.wim` from Sources folder of the Windows Server 2016 installation media. For an install image, you can:

- Use the `install.wim` file from the Sources folder on the Windows Server 2016 installation media. This will import one image for each edition of Windows Server 2016 that is on the installation media, as shown in Figure 1.10.
- Use a customized WIM file that you have already created. This will import one image for each image in the WIM file.
- Capture the install image from preconfigured server.

Figure 1.10
Install images.



When you deploy the image, you can deploy by using unicast or multicast. *Unicast* is typical for servers and allows you to deploy to one server at a time. *Multicast* is more useful for client computers because it allows a single image to be sent to multiple computers at the same time.

The process for deploying an image is as follows:

1. Perform a PXE boot on the computer.
2. PXE downloads the boot image to the computer.
3. The boot image starts on the computer and presents a menu.
4. From the menu, you select the install image that you want to deploy.
5. The install image you select is copied to the computer.
6. The computer restarts and you complete the configuration.

Microsoft Deployment Toolkit

To help automate the deployment of Windows Server 2016, you can use the Microsoft Deployment Toolkit (MDT). MDT is primarily a tool for automating the deployment of desktop operating systems, such as Windows 10, but it also works for Windows Server 2016.

One of the difficult parts of automating the installation of Windows Server 2016 is building an answer file. There are many settings that need to be configured to completely automate an installation and require no user input. MDT creates the answer file for you. You can also use MDT to inject drivers as part of the deployment process.

MDT uses task sequences to define operations that need to be performed. Within the task sequence, you can configure detailed information such as how disks should be partitioned. The task sequence also defines where addition drivers are located. You can also define how the computer name is generated. For example, you could configure the computer name based on the computer serial number.

You have the option to create a Lite Touch ISO for the task sequence. If you add this ISO to WDS as a boot image, you can automate the deployment of the operating system to a new computer or virtual machine. The Lite Touch ISO automatically deploys the image defined in the task sequence.

If you have System Center Configuration Manager in your organization, you can implement Zero Touch deployment. A Zero Touch deployment can be pushed out from Configuration Manager and won't require you to be at the console of the server or virtual machine to which it is being deployed.

For detailed information about MDT, see the Microsoft Deployment Toolkit at `https://technet.microsoft.com/en-us/windows/dn475741.aspx`.

Deployment Solutions for Virtualization

Most data centers are now virtualized, and this provides you with additional options for automatically creating and configuring virtual machines. Rather than having to go through an imaging process, a virtual hard disk with a prepared operating system can be copied instead. The operating system must be prepared by using Sysprep, just as when imaging is performed.

You can copy the virtual hard disks of a virtual machine after running Sysprep instead of performing an imaging process. Then you can create a new virtual machine using the copied virtual hard disk. You can do more advanced deployment of virtual machines that includes virtual hardware configuration by using more advanced tools.

If you are using Hyper-V, System Center Virtual Machine Manager (VMM) can be used to manage the Hyper-V hosts and virtual machines. In VMM, you can create virtual machine templates and store them in a library. Then when you need to deploy a new server, you can use the virtual machine template.

For more information about VMM, see the Virtual Machine Manager Documentation at `https://docs.microsoft.com/en-us/system-center/vmm/`.

Real World Scenario

Activation for Hyper-V Virtual Machines

You are creating a new image for Windows Server 2016 virtual machines and want activation for the new image to be as easy as possible. You don't ever want to manually enter a product key during deployment. You also want to ensure that activation can occur without other infrastructure in test environments where network connectivity is limited.

If you are using Windows Server 2016 Datacenter for your hypervisor, you have the option to use Automatic Virtual Machine Activation (AVMA) to activate virtual machines running Windows Server 2016 or Windows Server 2012 R2. Effectively, the activation of the Hyper-V host is being used to allow the activation of the virtual machines.

When a virtual machine uses an AVMA key, it activates directly with the Hyper-V host. This works even if the virtual machine has no network connectivity. You need to enter the AVMA key in the virtual machine. There are no minimum activation thresholds for AVMA.

To obtain a list of AVMA keys, see Automatic Virtual Machine Activation at `https://technet.microsoft.com/en-us/library/dn303421(v=ws.11).aspx`.

If you are using VMware ESXi as your virtualization host, you can use VMware vSphere client and vCenter Server to manage the deployment of new servers by using templates. The vSphere client is used to initiate and manage the process, but the vCenter Server stores the template.

For more information about vSphere client and vCenter Server, see the VMware website at `http://www.vmware.com`.

Common Management Tools

You can use Windows PowerShell to manage almost any aspect of Windows Server 2016, but there are still graphical tools that many administrators prefer to use. Server Manager is the main graphical administration tool that you can use to configure Windows Server 2016 and start other administration tools. Computer Management, Device Manager, and Task Scheduler are also commonly used graphical tools for server administration.

Overview of Server Manager

Server Manager is the starting point for graphical administration tools in Windows Server 2016. It provides an interface to perform some of the common post-installation tasks and links to start other graphical administration tools. You can also use Server Manager to add or remove server roles and features.

A single Server Manager console can be used to manage multiple computers running Windows Server 2016. This allows you to configure a single central instance of Server Manager for centralized administration of multiple servers. For example, you could install the Remote Server Administration Tools on a computer running Windows 10 and centrally manage all your computers running Windows Server 2016.

On a Server Core installation of Windows Server 2016, there is no graphical interface for administration. However, you can use Server Manager to remotely manage Server Core.

To manage a server remotely by using Server Manager, Windows PowerShell remoting needs to be enabled on the remote server. This is enabled by default on Windows Server 2016.

To add a server to Server Manager, follow these steps:

1. In Server Manager, click Manage and click Add Servers.
2. In the Add Servers window, on the Active Directory tab, type the name of the server and click Find Now.
3. Double-click the server name and click OK.
4. Verify that the server is listed in the All Servers view.

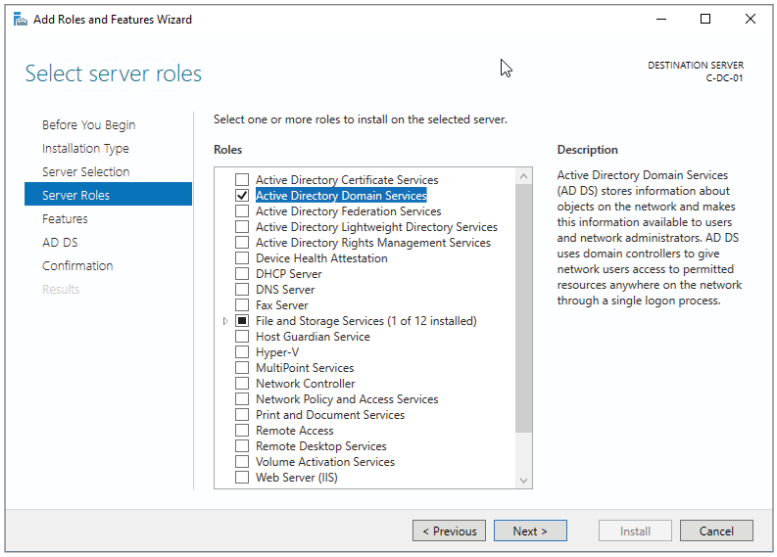
Role and Features

The functionality of Windows Server 2016 is divided into roles and features. *Roles* perform a specific service for clients such as Active Directory Domain Service, DNS server, DHCP server, or web server. *Features* are generally software that support those roles but don't provide services to clients. When you install a server role, you are often prompted to install additional features that are required. Some examples of features are .NET Framework 4.6 Features, BitLocker Drive Encryption, Failover Clustering, and Windows Server Backup.

To install roles and features, follow these steps:

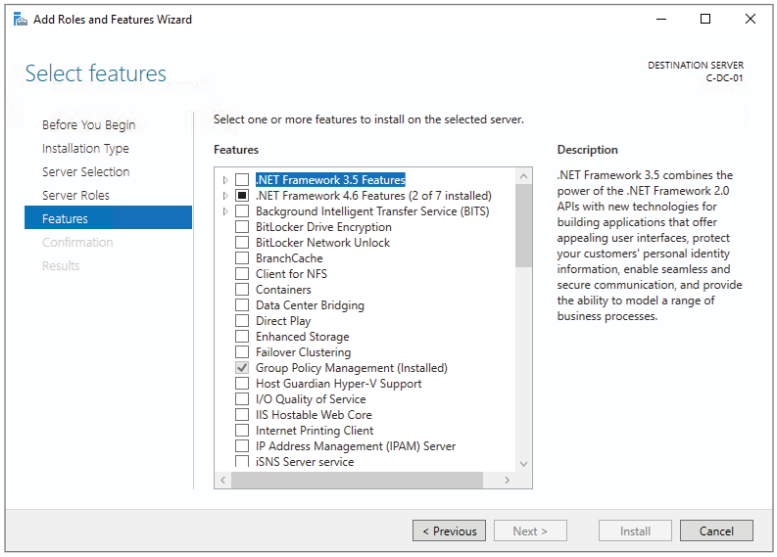
1. In Server Manager, click Manage and click Add Roles and Features.
2. In the Add Roles and Features Wizard, on the Before You Begin Page, click Next.
3. On the Select Installation Type page, select Role-Based or Feature-Based Installation and click Next. The Remote Desktop Services Installation option is used to configure one or more servers to provide access to session-based desktops or virtual desktops.
4. On the Select Destination Server page, select the server you want to install roles and features on and click Next.
5. On the Select Server Roles page, shown in Figure 1.11, select any server roles you want to install and click Next. If prompted to add required features, click Add Features.

FIGURE 1.11
Server roles



6. On the Select Features page, shown in Figure 1.12, select any features you want to install and click Next.

FIGURE 1.12
Features



7. Complete any additional pages required by the server roles you are adding. Some server roles add pages to the wizard to gather additional configuration information.
8. On the Confirmation page, click Install.
9. On the Installation Progress page, click Close. If you close the wizard before installation is complete, the installation continues in the background.

After the server roles and features are installed, you might be prompted to restart the server. Some server roles required additional configuration after installation. In most cases, if a server role requires additional configuration, you will be notified in Server Manager and provided with a link to begin that additional configuration.

For some server roles, administrative and monitoring functionality is added to Server Manager. This is accessible in the far-left navigation menu.

Monitoring

Server Manager provides high-level monitoring functionality that you can use to quickly identify if there are problems that need to be addressed. The Dashboard view, shown in Figure 1.13, provides an overview of servers and server roles. If there are problems that need to be investigated, the role or server appears in red. You can drill down into the identified areas by clicking on them.

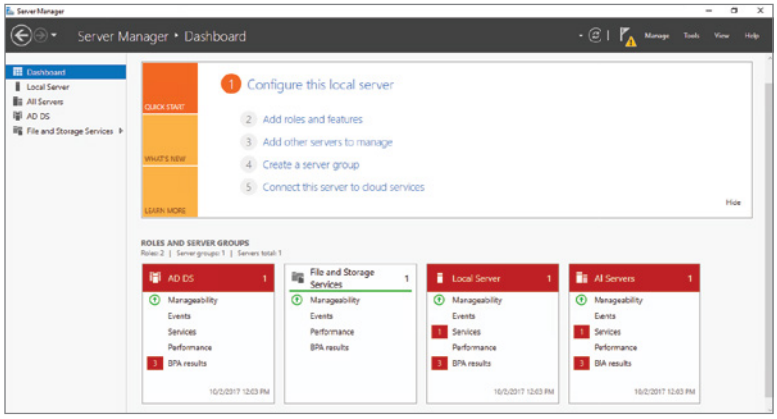


Figure 1.13
Dashboard view

The Local Server view provides an overview of server configuration and some monitoring information. The monitoring information available includes:

- Events. This section lists warning and error events from the event logs.
- Services. This area shows the status of services and allows you to stop and start services.
- Best Practices Analyzer (BPA). This area shows the results of BPA scans. Unlike most other monitoring, this shows potential configuration problems rather than just functional problems such as a failing service. You need to trigger a BPA scan to collect results.

- Performance. This area shows performance alerts for CPU usage and memory based on thresholds that you can configure. The functionality is not enabled by default.
- Role and Features. This area shows the server roles and features that are installed on the server.

The All Servers view displays the same information types as the Local Server view, but aggregates the information for all servers being monitored by this instance of Server Manager.

Computer Management

Computer Management, shown in Figure 1.14, contains many useful tools for managing and monitoring Windows Server 2016. These tools include: Task Scheduler, Event Viewer, Shared Folders, Performance, Device Manager, Disk Management, and Services. Each of these tools can be run separately from the Tools menu in Server Manager or by adding a snap-in to a Microsoft Management Console (MMC), but Computer Management provides one central place to access them.

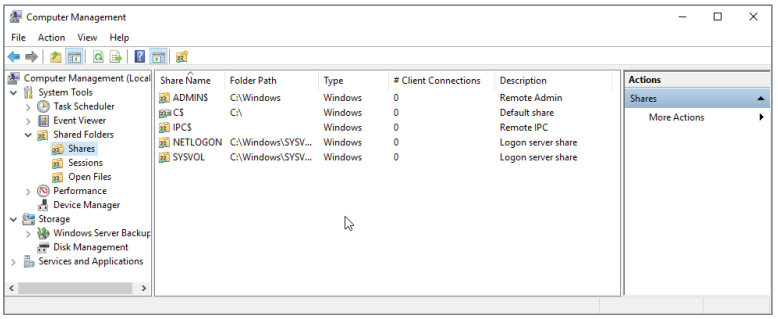


FIGURE 1.14 Computer Management

Device Manager

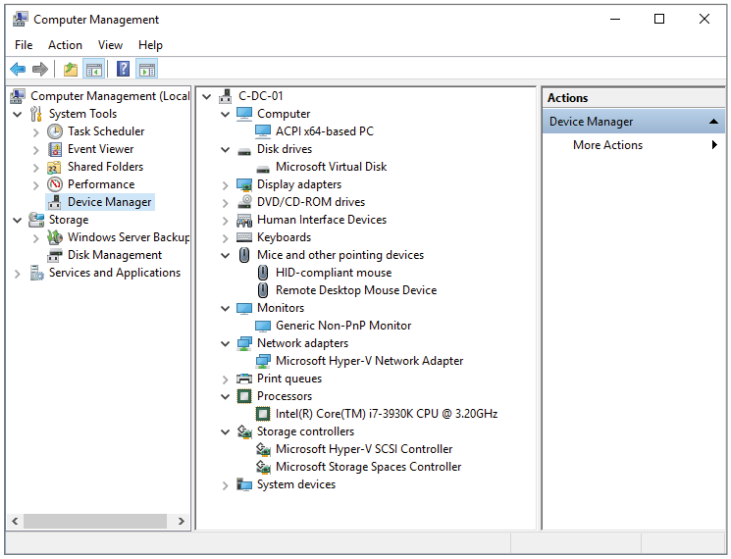
You use Device Manager, shown in Figure 1.15, to view and troubleshoot hardware in Windows Server 2016. If the server is virtualized, there is seldom a need to troubleshoot hardware drivers. This tool is primarily used for physical servers.

Some of the tasks you can perform in Device Manager include:

- View device properties. In the properties of a device, you can view the driver that is loaded and view many device properties such as the hardware IDs that are used by plug-and-play to identify the device and load an appropriate driver.
- Identify unknown devices. If Windows Server 2016 cannot locate a driver for hardware, it will appear as an unknown device. This is common for specialized hardware such as storage controllers. After identifying the unknown device, you can load the driver for it. The necessary driver is typically obtained from the manufacturer.
- Update drivers. If the hardware vendor doesn't distribute device driver updates as an executable file that automatically installs them, you can update drivers from within Device Manager. The device driver installation is based on an `.inf` file that defines the other files that need to be loaded.

- Roll-back drivers. If hardware is not performing properly after a driver update, you can roll back the device driver to the previous version.
- Disable hardware. In rare cases, if hardware is malfunctioning, disabling it in Device Manager can prevent it from interfering with server operation. It can be enabled again for troubleshooting.

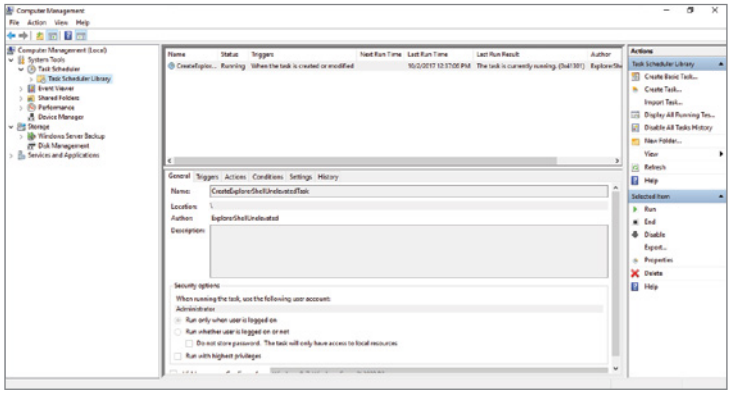
FIGURE 1.15
Device Manager



Task Scheduler

Task Scheduler, shown in Figure 1.16, is used by Windows Server 2016 to perform many background maintenance tasks. In most cases, you do not need to interact with scheduled tasks created by the operating system. If you use Task Scheduler, it is more likely that you will use it to run your own scripts for scheduled maintenance. For example, you can create a scheduled task to delete log files from Internet Information Services when they are more than 30 days old.

FIGURE 1.16
Task Scheduler



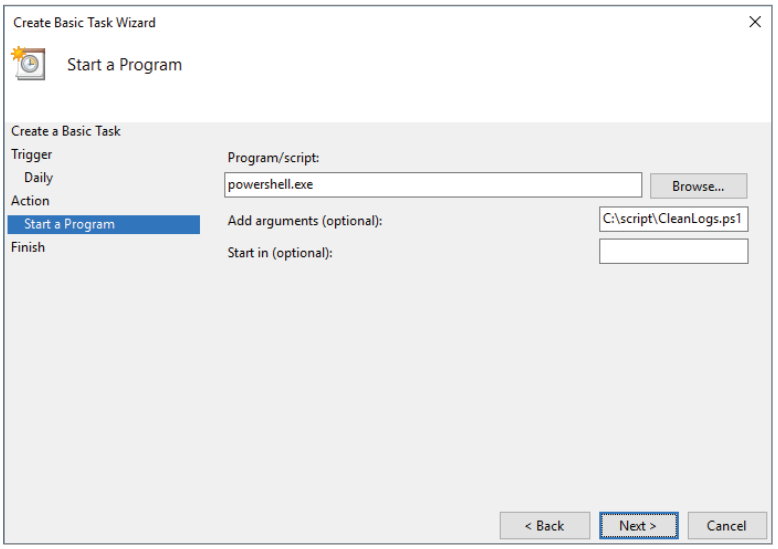
When you create a new task, the critical items to consider are

- Triggers
- Action
- Security

Triggers define when a task is going to run. Most of the time tasks are scheduled based on time of day, day of the week, or day of the month. However, you can also schedule a task to run when the computer starts, when a user signs in, or when a specific event is logged.

The action for a task defines what the task is going to do. There are legacy options to send an email or display a message, but those are deprecated. You should select the option to start a program. You need to identify the executable to be run and any parameters that it required. If you are scheduling a Windows PowerShell script, then you specify `powershell.exe` as the program and provide the path to the script in Add Arguments box, as shown in Figure 1.17.

FIGURE 1.17
Task action



When you create a basic task, the wizard does not prompt you for security information. By default, a basic task is configured to run as the user that created the task and run only when the user is logged on. You saw these settings in Figure 1.16. In most cases, you want the task to run whether the user is logged on or not.

As a best practice, you should not configure scheduled tasks to run as normal user accounts. Instead, you should configure tasks to run as service accounts or as special accounts defined in Windows Server 2016. A service account is a user account you have created with the correct permissions to perform the task. When you configure a service account for a task, you will be prompted to enter a password for the service account. When the password is saved as part of the task, it allows the task to access network resources. If you choose not to store the password, then the service account only has access to local resources. If you need the account to run with administrative permissions, select the Run with Highest Privileges check box.

The special accounts in Windows Server 2016 do not require you to enter a password. The special accounts are listed here:

- SYSTEM. This account has full access to all local resources and the permissions of the computer account on the network. If the server running the task is a domain controller, then SYSTEM has access to modify Active Directory objects.
- SERVICE. This account has limited permissions on the local computer and anonymous permissions on the network.
- NETWORK SERVICE. This account has limited permissions on the local computer and the permissions of the computer account on the network.

For detailed information about the permissions for the special accounts, see Service User Accounts at `https://msdn.microsoft.com/en-us/library/windows/desktop/ms686005(v=vs.85).aspx`.

Monitoring and Troubleshooting Tools

When a server or application is not performing properly, you need to troubleshoot to identify the source of the problem and then resolve it. Application problems can be identified by error messages or just generally slow performance.

If there is an error message, that is your starting point for troubleshooting. Often, you can enter the error message into a search engine to identify possible resolutions. This works well for commonly used software when many people have posted information on the Internet.

The better you understand the process you are trying to troubleshoot, the better you will be at interpreting which web pages have relevant information for you. For example, if you understand that the application server is running on Windows Server 2016 with Internet Information Services (IIS) and the backend is a Microsoft SQL Server database, that will help you identify places where you should look for error messages to aid in your troubleshooting. If you are limited only to error messages directly within the application user interface, you have much less data with which to work.

For more specialized software, you are unlikely to find much troubleshooting information on the Internet. In this case, you should contact the vendor for support. Many vendors include support as part of the product purchase. Even if there is a cost for opening a support case, the cost of the support case is often less than the cost of downtime for the applications.

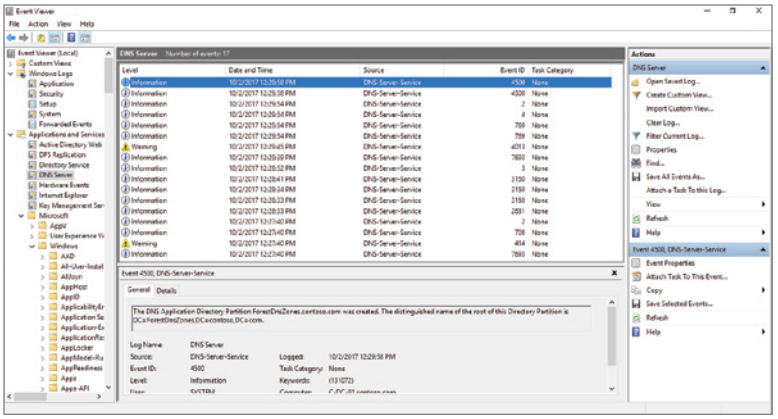
Some of the most difficult problems to troubleshoot are performance issues because there is often no error, just an application running slower than users expect. Performance problems are typically caused by bottlenecks in CPU utilization, memory capacity, network utilization, and disk utilization.

Microsoft has System Center Operations Manager as a full-featured system for monitoring errors and performance. Operations Manager can generate alerts and send notification to specific groups of administrators when errors occur or when system utilization is high. However, Operating Manager is an extra cost that not all organizations choose to implement. There are tools included with Windows Server 2016 that can be used to troubleshoot and monitor performance.

Event Viewer

Most components of Windows Server 2016 record information to the event logs, which are viewed by using Event Viewer, shown in Figure 1.18. The logs are broadly grouped in the Windows Logs and Applications and Services Logs. The Windows Logs are a general set of event logs that have remained the same for many versions of Windows and are probably familiar to you. The Applications and Services Logs are much more detailed about the type of information they contain. Each log contains events for a specific Windows component, such as the DNS server.

FIGURE 1.18
Event Viewer



These Windows Logs are commonly used for troubleshooting:

- Application. This log contains events from Windows services and applications. Applications installed on a server often also write events in this log. For example, Microsoft SQL Server and Microsoft Exchange Server both write events to this log. Errors and warnings in this log should be investigated.
- Security. This log contains events related to auditing resource access and authentication. Some basic auditing is in place by default, but you can configure additional auditing. For example, you can configure auditing of file system access to identify which users are accessing or modifying files.
- System. This log contains operating-system-level events. Information about drivers loading or services starting and stopping are located here.

You should scan the Application and System logs occasionally to identify any errors or warnings. These are items that may indicate a problem. Most of the time, it is not worthwhile to read all of the information events. However, when you review the entire process performed by a piece of software, it can be useful to review the information events from that software along with the error and warning events.

To simplify reading events in a log, you can filter the log to show specific event types and events from specific sources. You can also create custom views that search across multiple event logs and display events matching the criteria that you specify. An Administrative Events custom view exists by default that shows the warnings and errors from all event logs. Some server roles also create a custom view to display events related to that server role.

Each event log has a maximum log size. Most logs have a maximum log size of 20 megabytes (MB) or larger, but this varies among logs. You can modify the maximum log size to a level that you determine is appropriate. Generally, you want the logs to contain enough information to be useful for troubleshooting. So, there should be enough room in the logs to contain at least a few weeks of information. The amount of data collected in logs varies widely, depending on how busy a server is and whether it is experiencing errors. For example, the default size of 128 MB for a security log may contain months of events for a small organization but only an hour of events for a large organization.

By default, when an event log is full, it begins to overwrite older events to maintain the maximum number of events in the log but not skip any newer events. You also have the option to archive event logs that hit the maximum size. However, you will need to monitor the size of the archived event logs over time because they are never removed automatically and could fill up the C: drive on your server. Finally, you have the option to stop collecting events when the event log is full. This option is seldom used because in most scenarios the most recent events are the most important.

If there are events you are watching for across multiple servers, you can configure event log subscriptions. Event log subscriptions allow you to collect specific events from multiple servers into a single log on one server. Centralizing the events on a single server will make it easier to review.

For detailed information about forwarding event logs, see Windows Event Collector at `https://msdn.microsoft.com/en-us/library/bb427443(v=vs.85).aspx`.

Task Manager

In Windows Server 2016, the default view for Task Manager shows only the name of the applications running on the system. It does not show any details about resource utilization or services. Fortunately, if you click More Details, it shows a view with much more information, as shown in Figure 1.19.

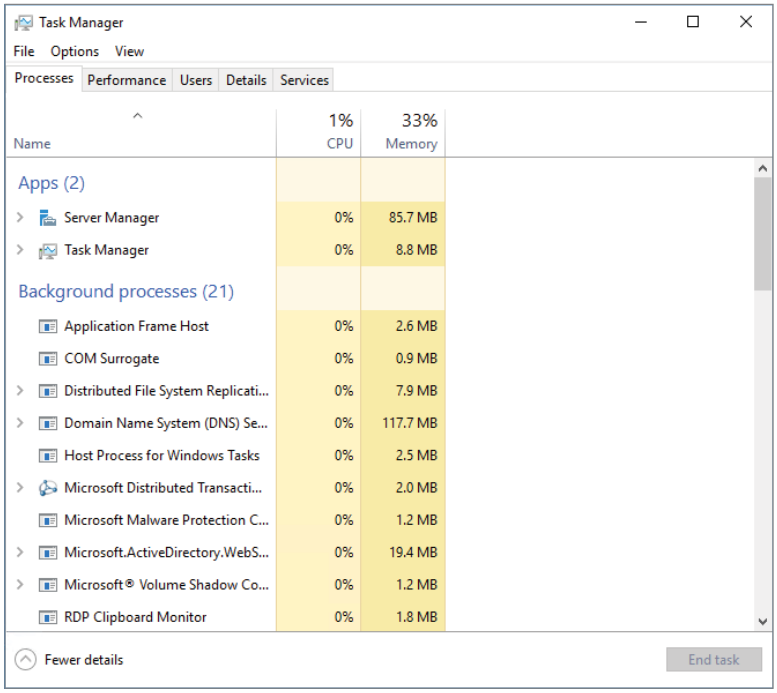
The tabs in Task Manager display the following:

- Processes. The list of processes running on the server are displayed along with the CPU and memory utilization for each. The processes are grouped as apps, background processes, and Windows processes.
- Performance. Information about CPU utilization, memory utilization, and network utilization are displayed. That information can be useful to identify if a specific resource is a bottleneck for performance.

- Users. All users signed in to the server at the console or via Remote Desktop are displayed along with the CPU and memory utilization for processes started by that user. If you expand the user, you can view individual processes.
- Details. For each process, the executable name, process ID, status, user name, CPU utilization, memory utilization, and description are displayed. You can sort the data based on those columns.
- Services. For each service, the service name, process ID, description, and status are displayed. This is a fast way to get a quick overview of service information.

Depending on the tab you are reviewing, you can perform various actions on the items displayed. You can stop, start, and restart services. You can also end specific tasks that are not responding properly. You can also open the file location for a process to identify the location of the executable.

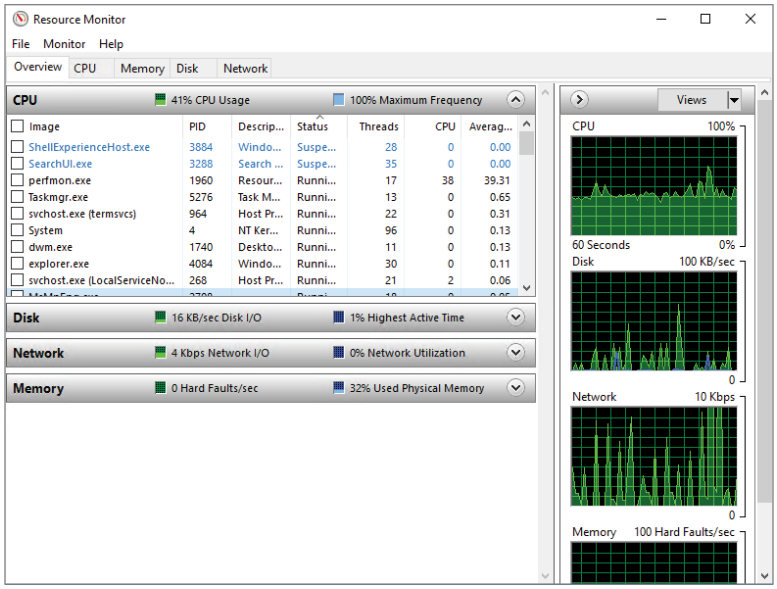
FIGURE 1.19
Task Manager



Resource Monitor

Resource Monitor, shown in Figure 1.20, shows more detailed performance information than what is available in Task Manager. Information is grouped into the four resources that are most likely to be bottlenecks: CPU, memory, disk, and network.

FIGURE 1.20
Resource Monitor



A useful feature in Resource Monitor is the ability to filter the view based on processes. If you select the check boxes for specific processes, the view is filtered to show only information for those processes and that filtering is applied to all the tabs.

The Overview tab shows a summary of the most commonly used information for CPU, memory, disk, and network. You can expand each section to view detailed information for each process.

On the CPU tab, you can see the CPU utilization for each process or service. If you select a specific process, you can also see all of the resources it is accessing in the Associated Handles section. The Associated Modules section shows the Dynamic Link Library (DLL) files that the process uses. This tab also shows the utilization of each CPU core so that you can identify if a process is saturating one core.

The Memory tab identifies the memory used by each process and how it is allocated overall to the operating system. It shows how much memory is in use, how much is being used for cache, and how much is free.

The Disk tab shows how much disk activity is being generated by each process. It also shows how much disk activity is being performed for each file. This can help identify problematic processes when disk utilization is high. The storage section shows the level of activity for each drive, including the disk queue length, which is an indicator of disk utilization. If the disk queue length is above one for extended periods of time, then the disk system is a bottleneck.

The Network tab displays network utilization for each process. It shows overall utilization for the process and breaks it down into individual conversations with other hosts. You can also see a list of all TCP connections and listening ports.

Windows Sysinternals

Windows Sysinternals is a set of advanced troubleshooting tools that are available for download at no charge from Microsoft. These tools can provide very low-level information about how Windows is performing tasks, and they can be useful for troubleshooting difficult problems when standard Windows tools do not provide enough information.

Some of the tools available include:

- TCPView. This utility shows detailed information about TCP and UDP ports on your computer.
- Process Explorer. This tool identifies the files and DLLs that a process has open.
- Process Monitor. This utility allows you to capture the file and Registry activity for a process so that you can understand what it does over a period of time or when an error occurs.

For more information about the Windows Sysinternals tools and to download them, see the Windows Sysinternals page at `https://docs.microsoft.com/en-us/sysinternals/`.

Performance Monitor

Windows Server 2016 includes an extensive set of performance counters that allow you to monitor many detailed aspects of system performance. The data provided by the performance counters is much more detailed than what is available in Task Manager or Resource Monitor but can be harder to interpret. You can use Performance Monitor, shown in Figure 1.21, to record and view these performance counters.

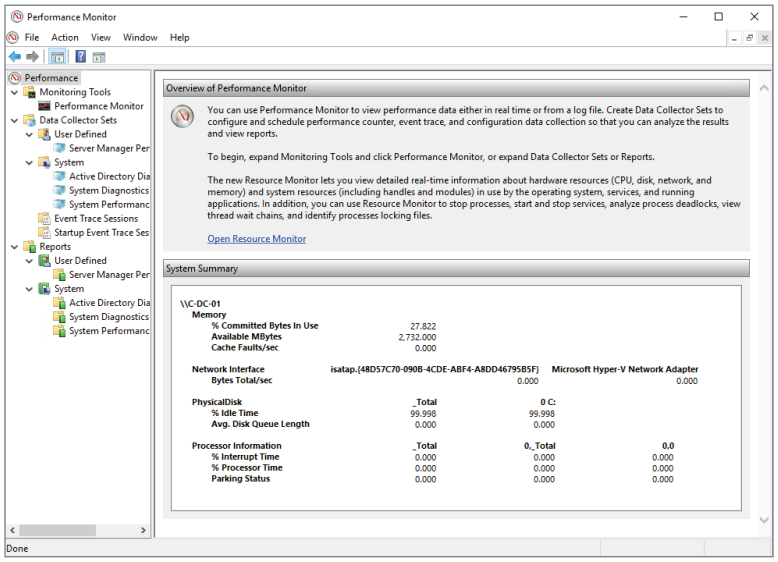


Figure 1.21
Performance Monitor

The Performance node provides an overview of commonly monitored performance counters. The data displayed here is similar to what is available on the Performance tab in Task Manager.

When you want to monitor performance counters in real time, you use the Performance Monitor node. In this node, you can add and remove various performance counters and choose how they are displayed. Performance counters can be displayed as a line graph, a histogram bar chart, or a report displaying numerical values.

To log system activity for later analysis, you need to create a data collector set. The data collector set defines which performance counters to record, when to start, and when to stop. Create your data collector sets in the User Defined node.

The System node in Data Collector Sets contains data collector sets included with Windows Server 2016. When you add server roles, they sometimes include a data collector set for troubleshooting that server role. For example, when you install the AD DS server role an Active Directory Diagnostics data collector set is added.

After a data collector set runs, a report is generated and stored in the Reports node. The report provides a summary of the data that was collected. For performance counters, it displays mean, minimum, and maximum values.

If you are trying to troubleshoot a performance problem that happened at a specific point in time, you need to review the value of performance counters over time. To view the value of performance counters at various points in time, use the Performance Monitor node to open the log files from the data collector set. The line graph view in the Performance Monitor node will allow you to select a specific point in time when viewing performance counter values.

The Bottom Line

Define a deployment process. You can deploy Windows Server 2016 by running `setup.exe` or by using various imaging processes. In general, you should try to automate deployment as much as possible, but you need to define a consistent deployment process that works for your organization. A well-defined deployment process helps to ensure consistency in your server configuration for easier troubleshooting.

> **Master It** Your organization has completely virtualized its infrastructure for deploying servers. To create new servers, your team copies a virtual hard drive with an operating system that has been prepared by using Sysprep. How can you improve this process?
>
> **Solution** If your organization is large enough to justify the cost, you should implement software that manages the deployment of virtual machines. You can use VMM for Hyper-V hosts or vCenter for VMware hosts. By using more advanced deployment software, you can automate processes better.

Select an edition of Windows Server 2016. Windows Server 2016 can be purchased as Standard edition or Datacenter edition. The basic functionality of both editions is the same, but some advanced features are available only in the Datacenter edition. If you need those advanced features, such as Storage Replica or shielded virtual machines, then you should purchase the Datacenter edition.

> **Master It** You are planning the standardized images that you will be using to deploy Windows Server 2016. For previous versions of Windows Server, you have always used