# Chapter

# 1

# Installing Windows Server 2016

## THE FOLLOWING 70-740 EXAM OBJECTIVES ARE COVERED IN THIS CHAPTER:

✓ **Install, upgrade, and migrate servers and workloads**

- This objective may include but is not limited to: Determine Windows Server 2016 installation requirements; determine appropriate Windows Server 2016 editions per workloads; install Windows Server 2016; install Windows Server 2016 features and roles; install and configure Windows Server Core; manage Windows Server Core installations using Windows PowerShell, command line, and remote management capabilities; implement Windows PowerShell Desired State Configuration (DSC) to install and maintain integrity of installed environments; perform upgrades and migrations of servers and core workloads from Windows Server 2008 and Windows Server 2012 to Windows Server 2016; determine the appropriate activation model for server installation, such as Automatic Virtual Machine Activation (AVMA), Key Management Service (KMS), and Active Directory-based Activation.

✓ **Install and configure Nano Server**

- This objective may include but is not limited to: Determine appropriate usage scenarios and requirements for Nano Server; install Nano Server; implement Roles and Features on Nano Server.

So, you have decided to start down the track of Windows Server 2016. The first question you must ask yourself is what's the first step? Well, the first step is to learn about what Windows Server 2016 features and benefits are available and how these features can help improve your organization's network.

So that's where I am going to start. I will talk about the different Windows Server 2016 versions and what version may be best for you. After I show you some of the new and improved Windows Server 2016 features, I will then show you how to install these different versions onto your network.

I will also show you how to use some PowerShell commands in the Windows Server 2016 installation. Let's dive right into the server by talking about some of the new features and advantages of Windows Server 2016.

> **NOTE** The Windows Server 2016 installations will all be done on a virtual server. You can use any virtual software as long as its supports Windows Server 2016 and 64-bit processors.

# Features and Advantages of Windows Server 2016

Before I show how to install and configure Windows Server 2016, let's take a look at some of the new features and the advantages it offers. Microsoft has stated that Windows Server 2016 is "the cloud-ready operating system." This means that many of the features of Windows Server 2016 are built and evolve around cloud based software and networking.

> **NOTE** Since many of you will be upgrading from previous versions of Windows Server, these are the new and/or improved features introduced by Microsoft since then. I will specifically identify any new features or advantages that are new to Windows Server 2016 only.

I will talk about all of these features in greater detail throughout this book. What follows are merely brief descriptions.

**Built-in Security**    Microsoft has always tried to make sure that their operating systems are as secure as possible, but with Windows Server 2016, Microsoft has included built-in breach resistance. This feature helps stop attackers on your system and allows a company to meet any compliance requirements.

**Active Directory Certificate Services**    *Active Directory Certificate Services (AD CS)* provides a customizable set of services that allow you to issue and manage *public key infrastructure (PKI) certificates*. These certificates can be used in software security systems that employ public key technologies.

**Active Directory Domain Services**    *Active Directory Domain Services (AD DS)* includes new features that make deploying domain controllers simpler and that let you implement them faster. AD DS also makes the domain controllers more flexible, both to audit and to authorize for access to files. Moreover, AD DS has been designed to make performing administrative tasks easier through consistent graphical and scripted management experiences.

**Active Directory Rights Management Services**    *Active Directory Rights Management Services (AD RMS)* provides management and development tools that let you work with industry security technologies, including encryption, certificates, and authentication. Using these technologies allows organizations to create reliable information protection solutions.

**BitLocker**    *BitLocker* is a tool that allows you to encrypt the hard drives of your computer. By encrypting the hard drives, you can provide enhanced protection against data theft or unauthorized exposure of your computers or removable drives that are lost or stolen.

**BranchCache**    *BranchCache* allows data from files and web servers on a wide area network (WAN) to be cached on computers at a local branch office. By using BranchCache, you can improve application response times while also reducing WAN traffic. Cached data can be either distributed across peer client computers (distributed cache mode) or centrally hosted on a server (hosted cache mode). BranchCache is included with Windows Server 2016 and Windows 10.

**Containers**    Windows Server 2016 has started focusing on an isolated operating system environment called Dockers. Dockers allow applications to run in isolated environments called Containers. Containers are a separate location where applications can operate without affecting other applications or other operating system resources. To understand Dockers and Containers, think of virtualization.

Virtual machines are operating systems that run in their own space on top of another operating system. Well Dockers and Containers allow an application to run in its own space and because of this, it doesn't affect other applications. There are two different types of containers to focus on.

    **Windows Server Containers**    Windows Server 2016 allows for an isolated application to run by using a technology called process and namespace isolation. Windows Server 2016 containers allow applications to share the system's kernel with their container and all other containers running on the same host.

    **Hyper-V Containers**    Windows Server 2016 Hyper-V Containers add another virtual layer by isolating applications in their own optimized virtual machine. Hyper-V Containers work differently than Windows Server Containers in the fact that the Hyper-V Containers do not share the system's kernel with other Hyper-V Containers.

**Credential Guard**   Credential Guard helps protect a system's credentials and this helps avoid pass the hash attacks. Credential Guard offers better protection against advanced persistent threats by protecting credentials on the system from being stolen by a compromised administrator or malware.

Credential Guard can also be enabled on Remote Desktop Services servers and Virtual Desktop Infrastructure so that the credentials for users connecting to their sessions are protected.

**DHCP**   *Dynamic Host Configuration Protocol (DHCP)* is an Internet standard that allows organizations to reduce the administrative overhead of configuring hosts on a TCP/IP-based network. Some of the features are DHCP failover, policy-based assignment, and the ability to use Windows PowerShell for DHCP Server.

**DNS**   *Domain Name System (DNS)* services are used in TCP/IP networks. DNS will convert a computer name or fully qualified domain name (FQDN) to an IP address. DNS also has the ability to do a reverse lookup and convert an IP address to a computer name. DNS allows you to locate computers and services through user-friendly names.

**Failover Clustering**   *Failover Clustering* gives an organization the ability to provide high availability and scalability to networked servers. Failover clusters can include file share storage for server applications, such as Hyper-V and Microsoft SQL Server, and those that run on physical servers or virtual machines.

**File Server Resource Manager**   *File Server Resource Manager* is a set of tools that allows administrators to manage and control the amount and type of data stored on the organization's servers. By using File Server Resource Manager, administrators have the ability to set up file management tasks, use quota management, get detailed reports, set up a file classification infrastructure, and configure file-screening management.

**Group Policy Objects**   *Group Policy Objects* are a set of rules and management configuration options that you can control through the Group Policy settings. These policy settings can be placed on users' computers throughout the organization.

**Hyper-V**   *Hyper-V* is one of the most changed features in Windows Server 2016. Hyper-V allows an organization to consolidate servers by creating and managing a virtualized computing environment. It does this by using virtualization technology that is built into Windows Server 2016.

Hyper-V allows you to run multiple operating systems simultaneously on one physical computer. Each virtual operating system runs in its own virtual machine environment.

Windows Server 2016 Hyper-V now allows an administrator to protect their corporate virtual machines using the new feature called Shielded Virtual Machine. Shielded Virtual Machines are encrypted using BitLocker and the VMs can only run on approved Hyper-V host systems.

Hyper-V also now includes a new feature called containers. Containers add a new unique additional layer of isolation for a containerized applications.

**IPAM**   *IP Address Management (IPAM)* is one of the features introduced with Windows Server 2012. IPAM allows an administrator to customize and monitor the IP address infrastructure on a corporate network.

**Kerberos Authentication**   Windows Server 2016 uses the *Kerberos authentication* (version 5) protocol and extensions for password-based and public key authentication. The Kerberos client is installed as a *security support provider (SSP)*, and it can be accessed through the *Security Support Provider Interface (SSPI)*.

**Managed Service Accounts (gMSAs)**   Stand-alone *group managed service accounts*, originally created for Windows Server 2008 R2 and Windows 7, are configured domain accounts that allow automatic password management and *service principal names (SPNs)* management, including the ability to delegate management to other administrators. Service accounts are accounts that an administrator creates so that the account can be used to start a service. Managed service accounts are accounts that are created using PowerShell, and then Active Directory manages the account. This includes changing the password on a regular frequency.

**Nano Server**   Windows Server 2016 has introduced a brand-new type of server installation called Nano Server. Nano Server allows an administrator to remotely administer the server operating system. It was primarily designed and optimized for private clouds and datacenters. Nano Server is very similar to Server Core, but the Nano Server operating system uses significantly less hard drive space, has no local logon capability, and only supports 64-bit applications and tools.

**Nested Virtualization**   Windows Server 2016 introduces a new Hyper-V feature called Nested Virtualization. Nested Virtualization allows administrators to create virtual machines within virtual machines. As an instructor, I think this is an awesome new feature. Now I can build a Windows Server 2016 Hyper-V server with a training virtual machine. Then when I get to the part when I need to teach Hyper-V, I can just do that right in the classroom virtual machine. There are numerous possibilities and we will talk more about them throughout this book.

**Networking**   There are many networking technologies and features in Windows Server 2016, including BranchCache, Data Center Bridging (DCB), NIC Teaming, and many more.

**PowerShell Direct**   Windows Server 2016 includes a new simple way to manage Hyper-V virtual machines called PowerShell Direct. PowerShell Direct is a new powerful set of parameters for the PSSession cmdlet called VMName. This will be discussed in greater detail in the Hyper-V chapters.

**Remote Desktop Services**   Before Windows Server 2008, we used to refer to this as Terminal Services. *Remote Desktop Services* allows users to connect to virtual desktops, RemoteApp programs, and session-based desktops. Using Remote Desktop Services allows users to access remote connections from within a corporate network or from the Internet.

**Security Auditing**   *Security auditing* gives an organization the ability to help maintain the security of an enterprise. By using security audits, you can verify authorized or unauthorized access to machines, resources, applications, and services. One of the best advantages of security audits is to verify regulatory compliance.

**Smart Cards**   Using *smart cards* (referred to as *two-factor authentication*) and their associated *personal identification numbers (PINs)* is a popular, reliable, and cost-effective way to provide authentication. When using smart cards, the user not only must have the physical card but also

must know the PIN to be able to gain access to network resources. This is effective because even if the smart card is stolen, thieves can't access the network unless they know the PIN.

**TLS/SSL (Schannel SSP)**   *Schannel* is a security support provider (SSP) that uses the *Secure Sockets Layer (SSL)* and *Transport Layer Security (TLS)* Internet standard authentication protocols together. The Security Support Provider Interface is an API used by Windows systems to allow security-related functionality, including authentication.

**Windows Deployment Services**   *Windows Deployment Services* allows an administrator to install Windows operating systems remotely. Administrators can use Windows Deployment Services to set up new computers by using a network-based installation.

**Windows PowerShell Desired State Configuration**   Windows Server 2016 created a new PowerShell management platform called Windows PowerShell Desired State Configuration (DSC). DSC enables the deploying and managing of configuration data for software services and it also helps manage the environment in which these services run.

DSC allows administrators to use Windows PowerShell language extensions along with new Windows PowerShell cmdlets, and resources. DSC allows you to declaratively specify how a corporation wants their software environment to be configured and maintained.

DSC allows you to automate tasks like enabling or disabling server roles and features, manage Registry settings, manage files and directories, manage groups and users, deploy software, and run PowerShell scripts to just name a few.

**Windows Server Backup Feature**   The *Windows Server Backup* feature gives an organization a way to back up and restore Windows servers. You can use Windows Server Backup to back up the entire server (all volumes), selected volumes, the system state, or specific files or folders.

# Planning the Windows Server 2016 Installation

Before you install Windows Server 2016, you must first ask yourself these important questions: What type of server do I need? Will the server be a domain controller? What roles do I need to install on this server?

Once you have figured out what you need the server to do, you can make a game plan for the installation. So, let's start by looking at some of the server roles and technologies that can be installed on a Windows Server 2016 computer.

## Server Roles in Windows Server 2016

When you install Windows Server 2016, you have to decide which roles and features are going to be installed onto that server. This is an important decision in the computer world. Many administrators not only overuse a server but also underutilize servers in their organization.

For example, many administrators refuse to put any other roles or features on a domain controller. This may not be a good use of a server. Domain controllers help authenticate users onto the network, but after that the domain controllers are really not very busy all day long. Domain controllers have tasks that they must perform all day, but the server on which they reside is not heavily used when compared to a SQL Server machine or an Exchange mail server. This is where monitoring your server can be useful.

If your domain controller is a virtual machine or if you have more than enough servers, then having a domain controller with no other applications on it (except DNS) may be fine. But if servers are limited, then think about putting other services or applications on your server if the server can handle them. Just remember, some applications work better on member servers than on domain controllers. So before just adding any application to a domain controller, make sure you research the application and find out best practices.

Now let's take a look at some of the roles and features you can install onto a Windows Server 2016 machine. Knowing the different roles and features you can install will help you to design, deploy, manage, and troubleshoot technologies in Windows Server 2016. Figure 1.1 shows the Add Roles and Features Wizard in Server Manager. It shows you just some of the roles that can be installed on a Windows Server 2016 machine.

**FIGURE 1.1**    Available roles in Windows Server 2016

---
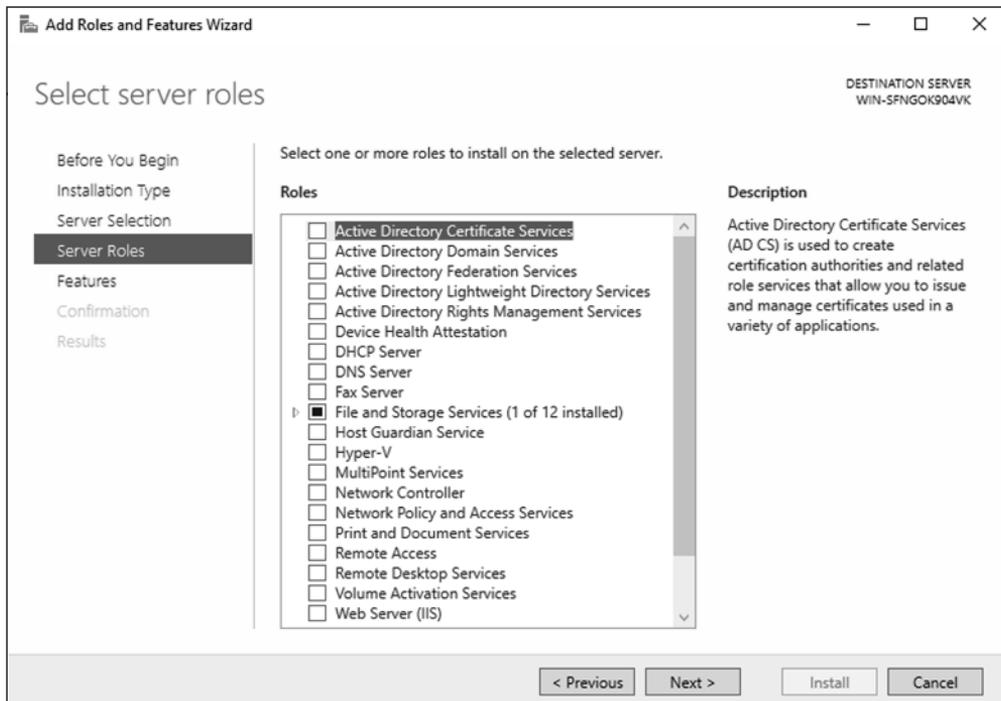
**Roles and Features**

Many of these roles were discussed in the section "Features and Advantages of Windows Server 2016." I include them here again because they are also *roles* that can also be installed on Windows Server 2016.

---

The following roles are available in Windows Server 2016:

**Active Directory Certificate Services** The AD CS server role in Windows Server 2016 allows you to build a PKI and provide public key cryptography, digital certificates, and digital signature capabilities for your organization.

>   **Feature** AD CS provides a customizable set of services that allows you to issue and manage PKI certificates. These certificates can be used in software security systems that employ public key technologies.

>   **Role** AD CS in Windows Server 2016 is the server role that allows you to build a PKI and provide public key cryptography, digital certificates, and digital signature capabilities for your organization.

**Active Directory Domain Services** The AD DS server role allows you to create a scalable, secure, and manageable infrastructure for user and resource management and to provide support for directory-enabled applications, such as Microsoft Exchange Server.

**Active Directory Federation Services** *Active Directory Federation Services (AD FS)* provides Internet-based clients with a secure identity access solution that works on both Windows and non-Windows operating systems. AD FS gives users the ability to do a *single sign-on (SSO)* and access applications on other networks without needing a secondary password.

**Active Directory Lightweight Directory Services** *Active Directory Lightweight Directory Services (AD LDS)* is a *Lightweight Directory Access Protocol (LDAP)* directory service that provides flexible support for directory-enabled applications, without the dependencies and domain-related restrictions of AD DS.

**Active Directory Rights Management Services** Active Directory Rights Management Services (AD RMS) in Windows Server 2016 is the server role that provides you with management and development tools that work with industry security technologies including encryption, certificates, and authentication to help organizations create reliable information protection solutions.

**Device Health Attestation** The Device Health Attestation helps protect your corporate network by verifying that client systems meet corporate policy. For example, you can make sure that all computers that connect to your network have their proper updates, antivirus, and proper configuration policies before connecting to the network.

**DHCP** *Dynamic Host Configuration Protocol (DHCP)* is an Internet standard that allows organizations to reduce the administrative overhead of configuring hosts on a TCP/IP-based network. Some of the features are DHCP failover, policy-based assignment, and the ability to use Windows PowerShell for DHCP Server.

**DNS**    *Domain Name System (DNS)* services are used in TCP/IP networks. DNS will convert a computer name or fully qualified domain name (FQDN) to an IP address. DNS also has the ability to do a reverse lookup and convert an IP address to a computer name. DNS allows you to locate computers and services through user-friendly names.

**Fax Server**    The fax server allows you to send and receive faxes, and it also allows you to manage fax resources such as jobs, settings, reports, and fax devices on a specific computer or on the network.

**File and Storage Services**    *File and Storage Services* allows an administrator to set up and manage one or more file servers. These servers can provide a central location on your network where you can store files and then share those files with network users. If users require access to the same files and applications or if centralized backup and file management are important issues for your organization, administrators should set up network servers as a file server.

**Host Guardian Service**    The Host Guardian Service (HGS) allows you to have a more secure environment for your network's virtual machines. The HGS role provides the Attestation & Key Protection services that enable Guarded Hosts to run Shielded virtual machines.

**Hyper-V**    The Hyper-V role allows administrators to create and manage a virtualized environment by taking advantage of the technology built into the Windows Server 2016 operating system. When an administrator installs the Hyper-V role, all required virtualization components are installed.

Some of the required components include the Windows hypervisor, Virtual Machine Management Service, the virtualization WMI provider, the virtual machine bus (VMbus), the virtualization service provider (VSP), and the virtual infrastructure driver (VID).

**MultiPoint Services**    MultiPoint Services allows multiple users, each with their own independent and familiar Windows experience, to simultaneously share one computer.

**Network Controller**    The Network Controller provides the point of automation needed for continual configuration, monitoring, and diagnostics of virtual networks, physical networks, network services, network topology, address management, and so on within a datacenter.

**Network Policy and Access Services**    Use the *Network Policy and Access Services* server role to install and configure *Network Policy Server (NPS)*, which helps safeguard the security of your network.

**Print and Document Services**    *Print and Document Services* allows an administrator to centralize print server and network printer tasks. This role also allows you to receive scanned documents from network scanners and route the documents to a shared network resource, Windows SharePoint Services site, or email addresses. Print and Document Services also provides fax servers with the ability to send and receive faxes while also giving the administrator the ability to manage fax resources such as jobs, settings, reports, and fax devices on the fax server.

**Remote Access**    Remote Access provides connectivity through DirectAccess, VPN, and Web Application Proxies. DirectAccess provides an Always On and Always Managed experience. Remote Access provides VPN access including site-to-site connectivity. Web Application

Proxies enable web-based applications from your corporate network to client devices outside of the corporate network. Remote Access also includes routing capabilities, including Network Address Translation (NAT).

**Remote Desktop Services**   Remote Desktop Services allows for faster desktop and application deployments to any device, improving remote user effectiveness while helping to keep critical data secure. Remote Desktop Services allows for both a *virtual desktop infrastructure (VDI)* and session-based desktops, allowing users to connect from anywhere.

**Volume Activation Services**   Windows Server 2016 *Volume Activation Services* will help your organization benefit from using this service to deploy and manage volume licenses for a medium to large number of computers.

**Web Server (IIS)**   The *Web Server (IIS)* role in Windows Server 2016 allows an administrator to set up a secure, easy-to-manage, modular, and extensible platform for reliably hosting websites, services, and applications.

**Windows Deployment Services**   Windows Deployment Services allows an administrator to install a Windows operating system over the network. Administrators do not have to install each operating system directly from a CD or DVD.

**Windows Server Essentials Experience**   Windows Server Essentials Experience allows an administrator to set up the IT infrastructure, and it also provides powerful functions such as PC backups to help protect your corporate data and Remote Web Access that allows access to business information from anywhere in the world. Windows Server Essentials Experience also allows you to easily connect to cloud-based applications and services.

**Windows Server Update Services**   *Windows Server Update Services (WSUS)* allows administrators to deploy application and operating system updates. By deploying WSUS, administrators have the ability to manage updates that are released through Microsoft Update to computers in their network. This feature is integrated with the operating system as a server role on a Windows Server 2016 system.

## Migrating Roles and Features to Windows Server 2016

Once you decide on which roles and features you are going to install onto your Windows Server 2016 system, then you either have to install those roles and features from scratch or migrate them from a previous version of Windows server.

Windows Server 2016 includes a set of migration tools that administrators can use to help ease the process of migrating server roles, features, operating system settings, and data. Administrators can migrate this data from an existing server that are running Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, or Windows Server 2016 to a computer that is running Windows Server 2016.

Using Windows Server Migration Tools to migrate roles, role services, and features can simplify the deployment of new servers. You can migrate roles and features on any server, including Server Core, installation option of Windows Server 2016, and virtual servers. By using Windows Server Migration Tools, an administrator can reduce migration downtime,

increase the accuracy of the migration process, and help eliminate conflicts that could otherwise occur during the migration process.

One advantage of using the migration tools is that most of them support cross-architecture migrations (x86-based to x64-based computing platforms), migrations between physical and virtual environments, and migrations between both the full and Server Core installation options of the Windows Server operating system. In Windows Server 2016, Windows Server Migration Tools also supports cross-subnet migrations.

To use Windows Server Migration Tools, the feature must be installed on both the source and destination computers. Windows Server Migration Tools installation and preparation can be divided into the following stages:

1. Installing Windows Server Migration Tools on destination servers that run Windows Server 2016

2. Creating deployment folders on destination servers that run Windows Server 2016 for copying to source servers

3. Copying deployment folders from destination servers to source servers

4. Registering Windows Server Migration Tools on source servers

If you plan to use Windows Server Migration Tools, you must be a member of the Administrators group on both the source and destination servers to install, remove, or set up the tools.

Administrators can install Windows Server Migration Tools 2016 by using either the Add Roles Or Features Wizard in Server Manager or Windows PowerShell deployment cmdlets for Server Manager.

To install Windows Server Migration Tools on a Server Core installation of Windows Server 2016, you would complete the following steps:

1. Open a Windows PowerShell session by typing **`powershell.exe`** in the current command prompt session and then pressing Enter.

2. In the Windows PowerShell session, install Windows Server Migration Tools by using the Windows PowerShell `Install-WindowsFeature` cmdlet for Server Manager. In the Windows PowerShell session, type the following, and then press Enter. (Omit the `ComputerName` parameter if you are installing the Windows Server Migration Tools on the local server.)

   ```
   Install-WindowsFeature Migration –ComputerName computer_name
   ```

## Deciding Which Windows Server 2016 Versions to Use

You may be wondering which version of Windows Server 2016 is best for your organization. After all, Microsoft offers the following six versions of Windows Server 2016.

> **NOTE** At the time this book was written, there were six versions of Windows Server 2016. But Microsoft is always improving and creating new versions of their products. Be sure to check out Microsoft's website for any other versions or changes.

**Windows Server 2016 Datacenter**   This version is designed for organizations that are looking to migrate to a highly virtualized, private cloud environment. Windows Server 2016 Datacenter has full Windows Server functionality with unlimited virtual instances.

**Windows Server 2016 Standard**   This version is designed for organizations with physical or minimally virtualized environments. Windows Server 2016 Standard has full Windows Server functionality with two virtual instances.

**Windows Server 2016 Essentials**   This version is ideal for small businesses that have as many as 25 users and 50 devices. Windows Server 2016 Essentials has a simpler interface and preconfigured connectivity to cloud-based services but no virtualization rights.

**Windows Hyper-V Server 2016**   Microsoft Hyper-V Server 2016 has the exact same Hyper-V role components as Windows Server 2016. Hyper-V 2016 Server is a stand-alone version that has the Windows hypervisor, the Windows Server driver model, and the other virtualization components only. Windows Hyper-V Server 2016 allows you to have a simple virtualization solution which allows you to reduce costs.

**Windows Storage Server 2016**   Windows Storage Server 2016 is not openly available for sale to the general public. Windows Storage Server 2016 is only available as an integrated hardware offering or as an available field upgrade from your hardware manufacturer. Windows Storage Server 2016 fully supports upgrades from previous versions.

**Windows MultiPoint Premium 2016 Server**   Windows MultiPoint Premium Server 2016 is a Stand-Alone Windows product designed for environments that have multiple users simultaneously sharing one computer. Windows MultiPoint Premium 2016 Server is the same as a Windows Server 2016 with Multipoint Services Installed. MultiPoint Services allows multiple users, each with their own independent and familiar Windows experience to simultaneously share one computer.

Once you choose what roles are going on your server, you must then decide how you're going to install Windows Server 2016. There are two ways to install Windows Server 2016. You can upgrade a Windows Server 2012 or Windows Server 2012 R2 machine to Windows Server 2016, or you can do a clean install of Windows Server 2016. If you decide that you are going to upgrade, there are specific upgrade paths you must follow.

Your choice of Windows Server 2016 version is dictated by how your current network is designed. If you are building a network from scratch, then it's pretty straightforward. Just choose the Windows Server 2016 version based on your server's tasks. However, if you already have a version of Windows Server 2012 installed, you should follow the recommendations in Table 1.1, which briefly summarize the supported upgrade paths to Windows Server 2016.

**TABLE 1.1**   Supported Windows Server 2016 upgrade path recommendations

| Current System | Upgraded System |
| --- | --- |
| Windows Server 2012 Standard | Windows Server 2016 Standard or Datacenter |
| Windows Server 2012 Datacenter | Windows Server 2016 Datacenter |

| Current System | Upgraded System |
|---|---|
| Windows Server 2012 R2 Standard | Windows Server 2016 Standard or Datacenter |
| Windows Server 2012 R2 Datacenter | Windows Server 2016 Datacenter |
| Windows Server 2012 R2 Essentials | Windows Server 2016 Essentials |
| Hyper-V Server 2012 R2 | Hyper-V Server 2016 |
| Windows Storage Server 2012 Standard | Windows Storage Server 2016 Standard |
| Windows Storage Server 2012 Workgroup | Windows Storage Server 2016 Workgroup |
| Windows Storage Server 2012 R2 Workgroup | Windows Storage Server 2016 Workgroup |

> **NOTE**  If your version of Microsoft Windows Server is not 64-bit, you can't upgrade to Windows Server 2016.

## Deciding on the Type of Installation

One of the final choices you must make before installing Windows Server 2016 is what type of installation you want. There are three ways to install Windows Server 2016.

**Windows Server 2016 (Desktop Experience)**   This is the version with which most administrators are familiar. This is the version that uses *Microsoft Management Console (MMC)* windows, and it is the version that allows the use of a mouse to navigate through the installation.

**Windows Server 2016 Server Core**   This is a bare-bones installation of Windows Server 2016. You can think of it this way: If Windows Server 2016 (Desktop Experience) is a top-of-the-line luxury car, then Windows Server 2016 Server Core is the stripped-down model with no air-conditioning, manual windows, and cloth seats. It might not be pretty to look at, but it gets the job done.

**Windows Server 2016 Nano Server**   Windows Server 2016 has introduced a brand new type of server installation called Nano Server. Nano Server allows an administrator to remotely administer the server operating system. It was primarily designed and optimized for private clouds and datacenters. Nano Server is very similar to Server Core, but the Nano Server operating system uses significantly smaller hard drive space, has no local logon capability, and only supports 64-bit applications and tools.

### 🌐 Real World Scenario

### Server Core

Here is an explanation of Server Core that I have used ever since it was introduced in Windows Server 2008.

I am a *huge* sports fan. I love watching sports on TV, and I enjoy going to games. If you have ever been to a hockey game, you know what a hockey goal looks like. Between hockey periods, the stadium workers often bring out a huge piece of Plexiglas onto the ice. There is a tiny square cut out of the bottom of the glass. The square is just a bit bigger than a hockey puck itself.

Now they pick some lucky fan out of the stands, give them a puck at center ice, and then ask them to shoot the puck into the net with the Plexiglas in front of it. If they get it through that tiny little square at the bottom of the Plexiglas, they win a car or some such great prize.

Well, Windows Server 2016 (Desktop Experience) is like regular hockey with a net, and Windows Server 2016 Server Core is the Plexiglas version.

Server Core supports a limited number of roles:

- Active Directory Certificate Services (AD CS)
- Active Directory Domain Services (AD DS)
- Active Directory Federation Services (AD FS)
- Active Directory Lightweight Directory Services (AD LDS)
- Active Directory Rights Management Services (AD RMS)
- DHCP Server
- DNS Server
- Fax Server
- File and Storage Services
- BITS Server
- BranchCache
- Hyper-V
- Network Policy and Access Services
- Print and Document Services
- Remote Access

- Remote Desktop Services
- Volume Activation Services
- Web Server (IIS)
- Windows Deployment Services
- Windows Server Update Services
- .NET Framework 3.5 Features
- .NET Framework 4.6 Features
- Streaming Media Services
- Failover Clustering
- iSCSI
- Network Load Balancing
- MPIO
- qWave
- Telnet Server/Client
- Windows Server Migration Tools
- Windows PowerShell 4.0

Server Core does not have the normal Windows interface or GUI. Almost everything has to be configured via the command line or, in some cases, using the Remote Server Administration Tools from a full version of Windows Server 2016. While this might scare off some administrators, it has the following benefits:

**Reduced Management**   Because Server Core has a minimum number of applications installed, it reduces management effort.

**Minimal Maintenance**   Only basic systems can be installed on Server Core, so it reduces the upkeep you would need to perform in a normal server installation.

**Smaller Footprint**   Server Core requires only 1GB of disk space to install and 2GB of free space for operations.

**Tighter Security**   With only a few applications running on a server, it is less vulnerable to attacks.

The prerequisites for Server Core are basic. It requires the Windows Server 2016 installation media, a product key, and the hardware on which to install it.

After you install the base operating system, you use PowerShell or the remote administrative tools to configure the network settings, add the machine to the domain, create and format disks, and install roles and features. It takes only a few minutes to install Server Core, depending on the hardware.

---

🌐 **Real World Scenario**

**Better Security**

When I started in this industry more than 20 years ago, I was a programmer. I used to program computer hospital systems. When I switched to the networking world, I continued to work under contract with hospitals and with doctors' offices.

One problem I ran into is that many doctors are affiliated with hospitals, but they don't actually have offices within the hospital. Generally, they have offices either near the hospital or, in some cases, right across the street.

Here is the issue: Do we put servers in the doctors' offices, or do we make the doctor log into the hospital network through a remote connection? Doctors' offices normally don't have computer rooms, and we don't want to place a domain controller or server on someone's desk. It's just unsafe!

This is where Windows Server 2016 Server Core can come into play. Since it is a slimmed-down version of Windows and there is no GUI, it makes it harder for anyone in the office to hack into the system. Also, Microsoft has a domain controller in Windows Server 2016 called a *read-only domain controller (RODC)*. As its name suggests, it is a read-only version of a domain controller.

With Server Core and an RODC, you can feel safer placing a server on someone's desk or in any office. Server Core systems allow you to place servers in areas that you would never have placed them before. This can be a great advantage to businesses that have small, remote locations without full server rooms.

---

## NIC Teaming

*NIC Teaming*, also known as *load balancing and failover (LBFO)*, gives an administrator the ability to allow multiple network adapters on a system to be placed into a team. Independent hardware vendors (IHVs) have required NIC Teaming, but until Windows Server 2012, NIC Teaming was *not* part of the Windows Server Operating System.

To be able to use NIC Teaming, the computer system must have at least one Ethernet adapter. If you want to provide fault protection, an administrator must have a minimum of two Ethernet adapters. One advantage of Windows Server 2016 is that an administrator can setup 32 network adapters in a NIC Team.

NIC Teaming is a very common practice when setting up virtualization. It is one way that you can have load balancing with Hyper-V.

NIC Teaming gives an administrator the ability to allow a virtual machine to use virtual network adapters in Hyper-V. The advantage of using NIC Teaming in Hyper-V is that the

administrator can use it to connect to more than one Hyper-V switch. This allows Hyper-V to maintain connectivity even if the network adapter under the Hyper-V switch gets disconnected.

An administrator can configure NIC Teaming in either Server Manager or PowerShell.

# Installing Windows Server 2016

In the following sections, I am going to walk you through two different types of installs. I will show you how to do a full install of Windows Server 2016 Datacenter (Desktop Experience), and then I will show you how to install the Server Core version of the same software and Nano Server.

> For these labs, I am using the full release of Windows Server 2016 Datacenter, but you can use Windows Server 2016 Standard.

## Installing with the Desktop Experience

In Exercise 1.1, I will show you how to install Windows Server 2016 Datacenter (Desktop Experience). This installation will have a Graphical User Interface (GUI) and this means that an administrator will be able to control the applications on the Desktop and the operating system functions with a mouse.

---

**Windows Installation**

At the time of this writing, I used the first full release of Windows Server 2016 Datacenter. For this reason, there may be screens that have changed somewhat since this book was published.

---

### EXERCISE 1.1

**Installing Windows Server 2016 Datacenter (Desktop Experience)**

1. Insert the Windows Server 2016 installation DVD, and restart the machine from the installation media.

2. At the first screen, Windows Server 2016 (see Figure 1.2) will ask you to configure your language, time and currency, and keyboard. Make your selections, and click Next.

3. At the next screen, click Install Now.

4. Depending on what version of Windows Server 2016 you have (MSDN, TechNet, and so on), you may be asked to enter a product key. If this screen appears, enter your product key, and click Next. If this screen does not appear, just go to step 5.

**FIGURE 1.2**    Windows Server 2016 Setup



5. The Select The Operating System That You Want To Install screen then appears. Choose the Windows Server 2016 Datacenter (Desktop Experience) selection (see Figure 1.3) and click Next.

**FIGURE 1.3**    Windows Server Edition
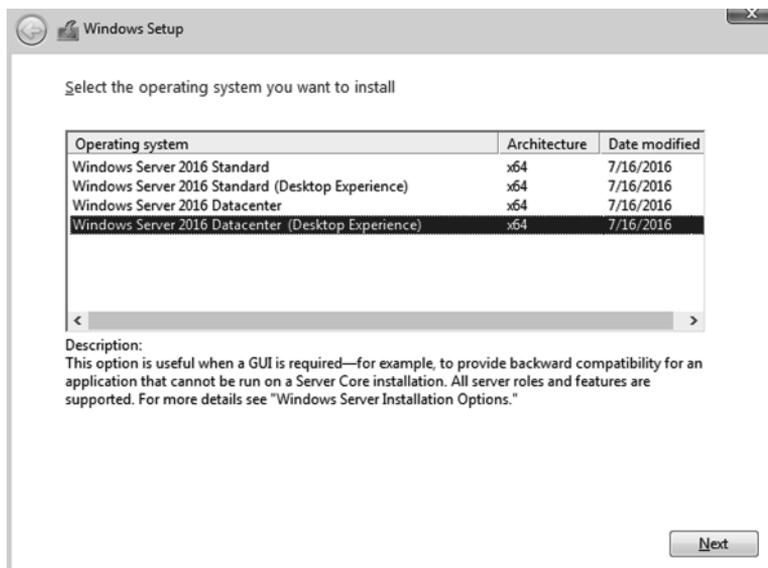
6. The license terms screen appears. After reading the Windows Server 2016 license agreement, check the I Accept The License Terms check box, and click Next.

7. On the Which type of installation do you want? Screen (see Figure 1.4), choose Custom: Install Windows Only (Advanced).

**FIGURE 1.4**    Windows Server Installation
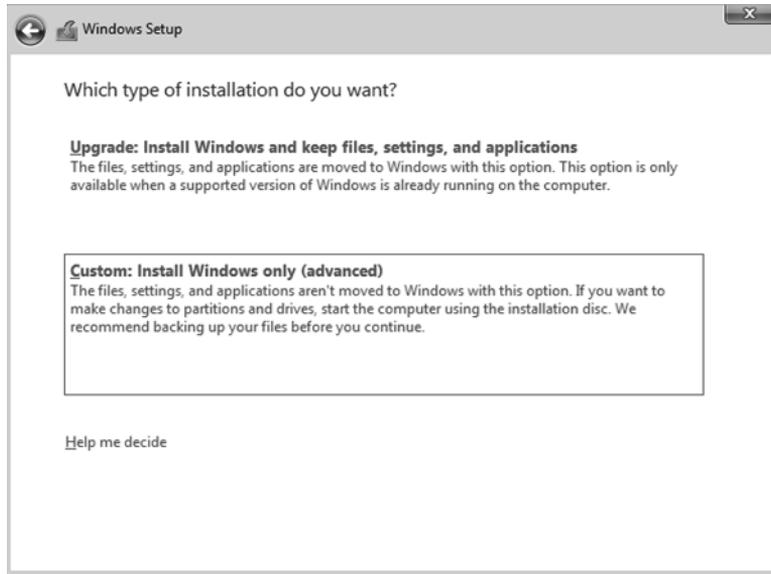


8. The next screen will ask you where you want to install Windows. If your hard disk is already formatted as NTFS, click the drive, and then click Next. If the hard disk is not yet set up or formatted, choose the New link, and create a partition. After creating the partition, click the Format link. Once the format is done, make sure you choose the new partition, and click Next.

9. The Installing Windows screen will appear next. This is where the files from your media will be installed onto the system (see Figure 1.5). The machine will reboot during this installation.

10. After the machine is finished rebooting, a screen requesting the administrator password will appear (see Figure 1.6). Type in your password. (P@ssword is used in this exercise.) Your password must meet the password complexity requirements. (Three of the following four are needed for complexity: one capitalized letter, one lowercase letter, one number, and/or one special character.) Click Finish.

**F I G U R E   1 . 5**   Installing Windows screen
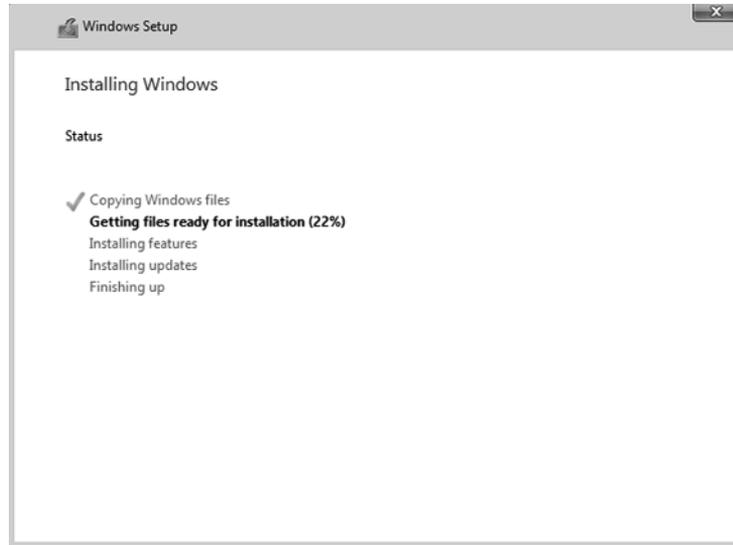


**F I G U R E   1 . 6**   Customize settings
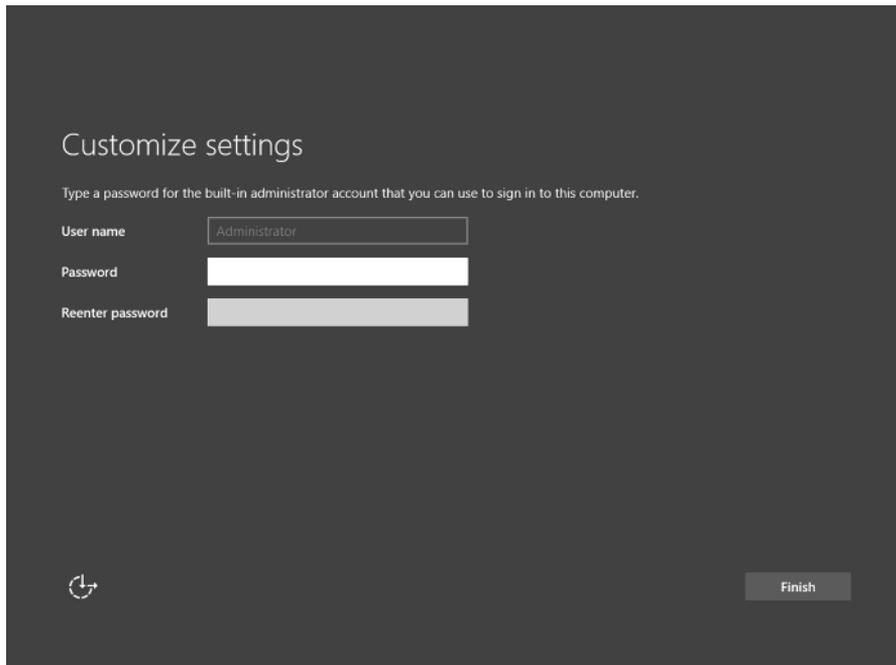
**11.** Next, log into the system. Press Ctrl+Alt+Del, and type in the administrator password. The machine will set up the properties of the administrator account.

**12.** Notice that the Server Manager dashboard automatically appears. Your Windows Server 2016 installation is now complete.

**13.** Close Server Manager.

After you have logged into the Windows Server 2016 Datacenter system, you will notice some features right away. The first is that there is a Start button in the lower-left corner of the screen.

> Administrators can also access the Start button by pressing the Windows key on a standard keyboard.

## Installing Windows Server 2016 Server Core

In Exercise 1.2, you will learn how to install Windows Server 2016 Server Core. You'll notice that the steps are similar to the ones in Exercise 1.1, with a couple of exceptions. As mentioned earlier, Server Core is a command line configuration of Windows Server 2016.

### EXERCISE 1.2

### Installing Windows Server 2016 Using Server Core

**1.** Insert the Windows Server 2016 installation DVD, and restart the machine from the installation media.

**2.** At the first screen, Windows Server 2016 will prompt you to configure your language, time and currency, and keyboard. Make your selections, and click Next.

**3.** At the next screen, click Install Now.

**4.** Depending on what version of Windows Server 2016 you have (MSDN, TechNet, and so on), you may be asked to enter a product key. If this screen appears, enter your product key, and click Next. If this screen does not appear, just go to step 5.

**5.** The Select The Operating System That You Want To Install screen then appears. Choose the Windows Server 2016 Datacenter selection (see Figure 1.7) and click Next.

**6.** The license terms screen appears. After reading the Windows Server 2016 license agreement, check the I Accept The License Terms check box and click Next.

**7.** At the Which Type Of Installation Do You Want? screen, choose Custom: Install Windows Only (Advanced).

**F I G U R E 1.7** Windows Server Edition
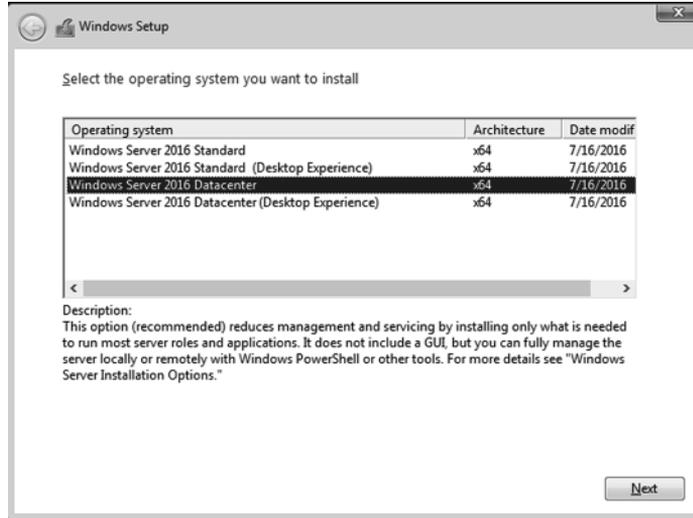


8. The next screen will ask you where you want to install Windows. If your hard disk is already formatted as NTFS, click the drive and then click Next. If the hard disk is not set up or formatted, choose the New link and create a partition. After creating the partition, click the Format link. Once the format is done, make sure you choose the new partition and click Next.

9. The Installing Windows screen will appear next. This is where the files from your media will be installed onto the system. The machine will reboot during this installation.

10. After the machine is finished rebooting, a screen requesting the administrator password will appear. Click OK (see Figure 1.8) and then type in your password. (P@ssword is used in this exercise.) Your password must meet the password complexity requirements (one capitalized letter, one number, and/or one special character).

**F I G U R E 1.8** Change Password Screen
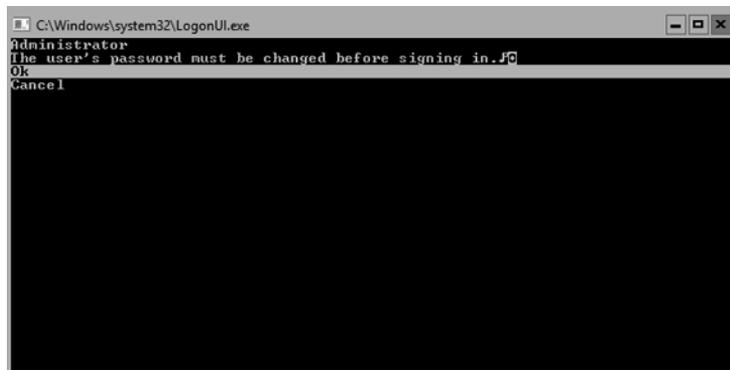
11. After the password is changed, a screen will appear telling you that the password has changed (see Figure 1.9). Hit the Enter key.

**FIGURE 1.9**    Password Changed Screen
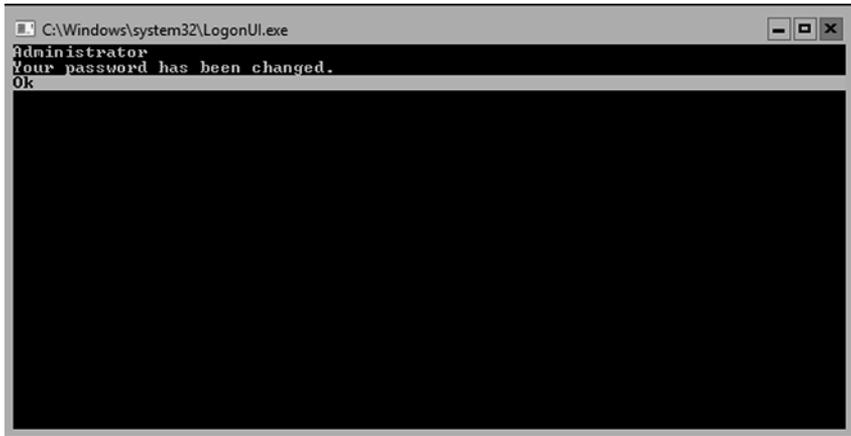


12. You will automatically get logged in. You will notice that the command prompt will automatically appear (see Figure 1.10). Your Windows Server 2016 Server Core installation is now complete. To turn off the machine, type **Shutdown /s /t 0**.

**FIGURE 1.10**    Server Core Command Prompt
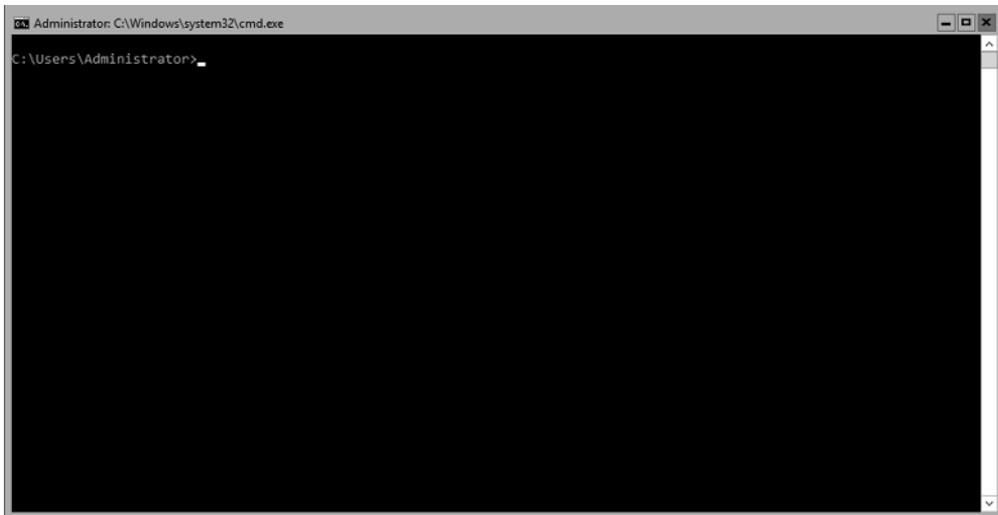
> **NOTE**   We will be showing many PowerShell commands throughout this book. The new Windows Server 2016 exams will be PowerShell intensive. I will show you the PowerShell commands needed to configure and maintain Windows Server 2016 Server Core throughout this entire book.

## Installing Windows Server 2016 Nano Server

With the release of Windows Server 2016, Microsoft has released a brand new installation option called Nano Server. Nano Server is a version of Windows Server 2016 that is controlled remotely and it was specifically designed to optimize the Windows Server for private cloud and Datacenter installations.

Windows Server 2016 Nano Server is a lot like Server Core but the advantage is that it is even a smaller installation of the operating system. Nano Server has *NO* local logon or GUI capabilities and it will allow only 64-bit applications and utilities.

Since Nano Server takes much less hard drive space and does not have many of the normal server components, its allows Nano Server to be much faster when it comes to setups, reboots, and even updates. Nano Server is available for both Standard and Datacenter editions of Windows Server 2016.

When Microsoft created Nano Server, they had some very specific ideas of how companies would use this version. For example, Nano Server is a good option for a DNS server, an IIS server, an application server for cloud based applications, or even a storage machine for file servers.

Now that you have seen some of the options on how to use Nano Server, let take a look at some of the disadvantages of Nano Servers. The first downside to using a Nano Server is that it cannot act as Domain Controller (this is a server with a copy of Active Directory installed onto the system). Also, Group Policy Objects (rules that you can put on machines or users) are also not supported on Nano Servers. Finally, Nano Servers can't be configured to use System Center Configuration Manager, System Center Data Protection Manager, NIC Teaming, or as proxy servers. Nano Servers also use a version of Windows PowerShell which has many differences as a server with regular PowerShell.

At the time this book was written, Nano Server only supports the Current Branch for Business (CBB) licensing model. But be sure to check the Microsoft website before taking any of the Microsoft Windows Server 2016 exams to make sure that this has not changed.

When it comes to installing Nano Servers, there are a few different options. There is no downloadable version of just Windows Server 2016 Nano Server. Nano Server is included on the Windows Server 2016 Standard or Datacenter physical media. Both server versions have a folder called NanoServer. The NanoServer folders contain a .wim image and a subfolder called Packages. The Packages subfolder is needed when you want to add server roles and features to the image.

But if you want a real easy way to create a Nano Server virtual hard drive (VHD), you can just download the Nano Server Image Builder. This software will help you easily create a Nano Server VHD that you can then use to boot up a server with or use in Microsoft's Hyper-V server.

In Exercise 1.3, you will learn how to install the Nano Server Image Builder and build a Nano Server VHD. For this exercise, you must have a copy of Windows Server 2016 downloaded.

**EXERCISE 1.3**

**Creating a Nano Server VHD**

1. Download the Nano Server Image Builder (see Figure 1.11) at Microsoft's website (`https://www.microsoft.com/en-us/download/details.aspx?id=54065`) by clicking the Download button. I saved the downloaded file under my Windows Server 2016 Downloads folder.

**FIGURE 1.11**   Nano Server Image Builder
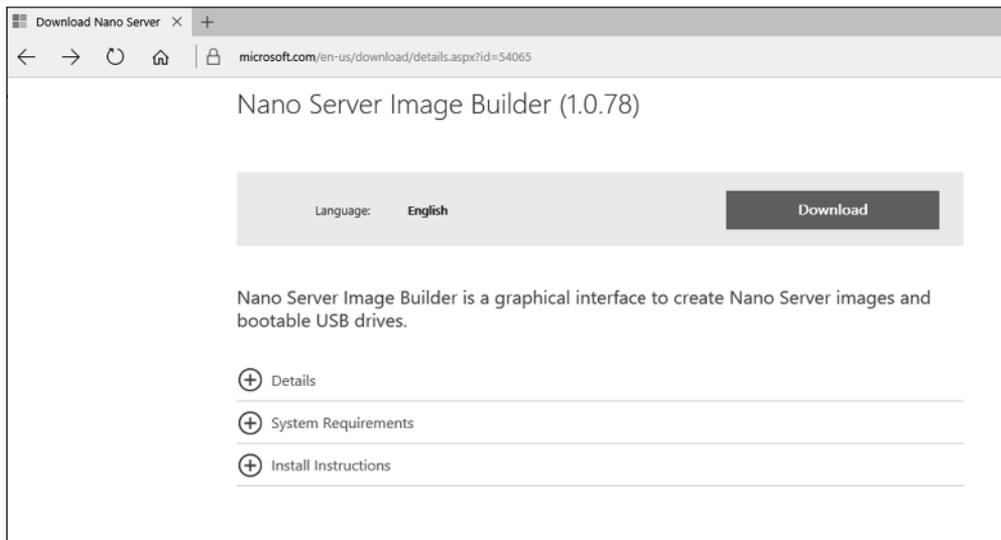


2. A file named `NanoServerImageBuilder.msi` will be created. Double-click on the file. If an Open File Security Warning Dialog box appears, click the Run button.

3. The Nano Server Image Builder Setup wizard will begin. Click Next at the intro screen.

4. At the Licensing screen, click the I accept the terms checkbox and click Next.

5. At the Destination Folder screen, choose the directory where you want to install the Nano Server Image Builder files (see Figure 1.12). Click Next.

**F I G U R E   1 . 1 2**     Nano Server Image Builder Destination
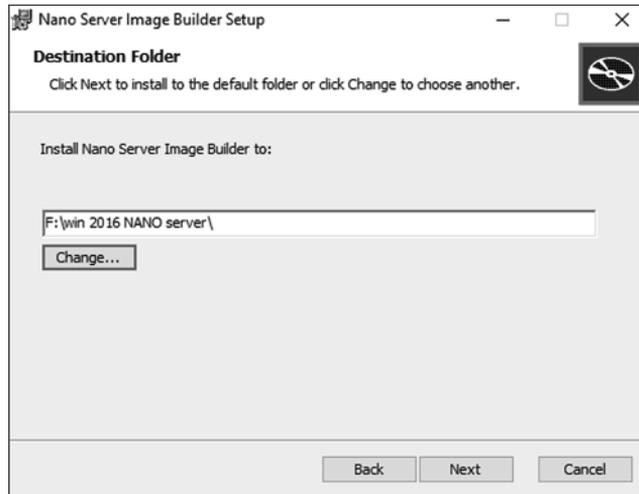


6. At the Ready to Install screen, click the Install Button. If a User Account Control box appears, click the Yes button.

7. Once the Installation is complete, click the Finish Button.

8. Open Windows Explorer and go to the destination folder that you chose in step 5. Double-click the `NanoServerImageBuilder.exe` file. If a UAC dialog box appears, click Yes.

9. For the Image Builder to work, you must also download the Windows ADK kit. This can be done at

   `https://developer.microsoft.com/en-us/windows/hardware/windows-assessment-deployment-kit`

   Click the get Windows ADK Download button.

10. It will ask you if you want to run or save the file. I saved the file to the same destination folder as the Nano Server Image Builder. Once it's downloaded, double-click the `adksetup.exe` file. If a dialog box appears, click Run.

11. Specify the destination of where you want the Windows ADK files to install and click Next.

12. At the Windows Kit Privacy screen, you can choose either option. By choosing Yes, you will participate in Microsoft's feedback program. For this exercise, I chose No. Click Next.

13. At the License Agreement screen, click Accept.

**14.** At the Features screen, accept the defaults and click Install. If a UAC screen appears, click Yes.

**15.** After the installation is complete, click the Close button.

**16.** Double-click on the `NanoServerImageBuilder.exe` file. When the UAC screen appears, click Yes.

**17.** So we now have the ability to create a Nano Server image or a bootable USB. We are going to create an Image. So click on the top choice "Create a new Nano Server image" (see Figure 1.13).

**FIGURE 1.13**    Nano Server Image Choice
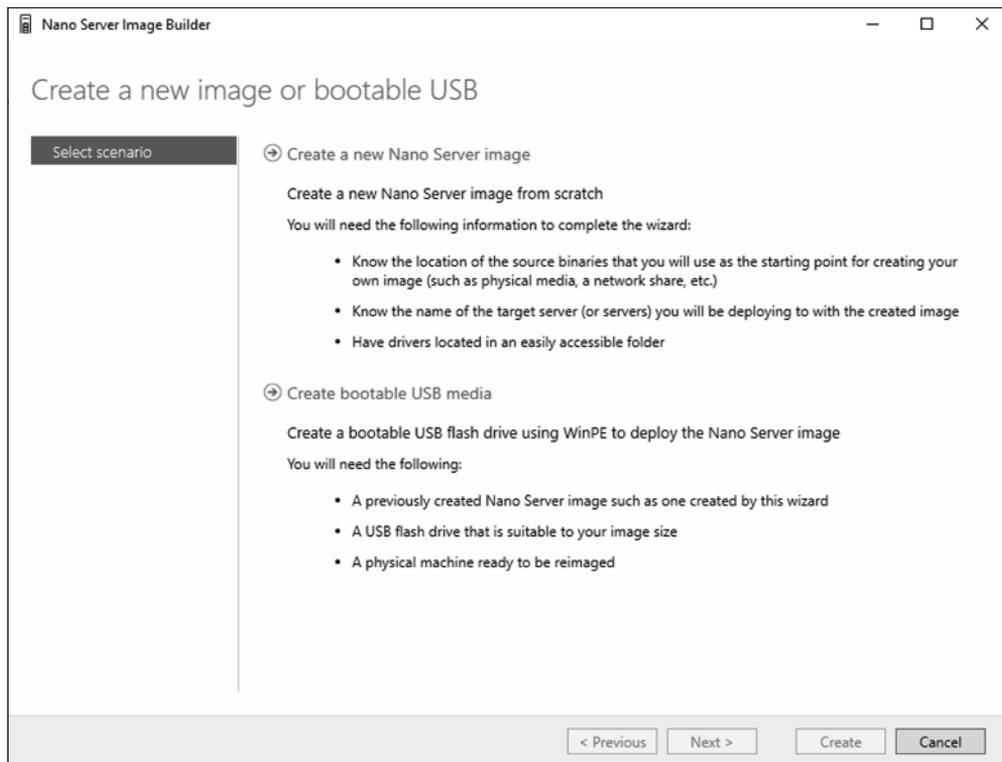


**18.** At the Before you begin screen, click Next.

**19.** At the Select Installation Media screen, point the folder to your Windows Server 2016 installation files where the NanoServer Folder resides. Click Next.

**EXERCISE 1.3** *(continued)*

> **NOTE**  If you only have a Windows Server 2016 .ISO image, right click on the ISO image and choose Open With ⩾ Windows Explorer. Then copy the NanoServer folder to another location. Then in step 20, just point to the location of the NanoServer folder.

**20.** At the License agreement screen, click the box that states I have read and agree to the terms. Then click Next.

**21.** At the Deployment type screen. I am going to choose to create a Virtual machine image named Pluto.vhd. I am keeping the default of 8 GB and I am placing the VHD in my Win 2016 Nano Server folder (see Figure 1.14). Click Next.

**FIGURE 1.14**   Deployment Type
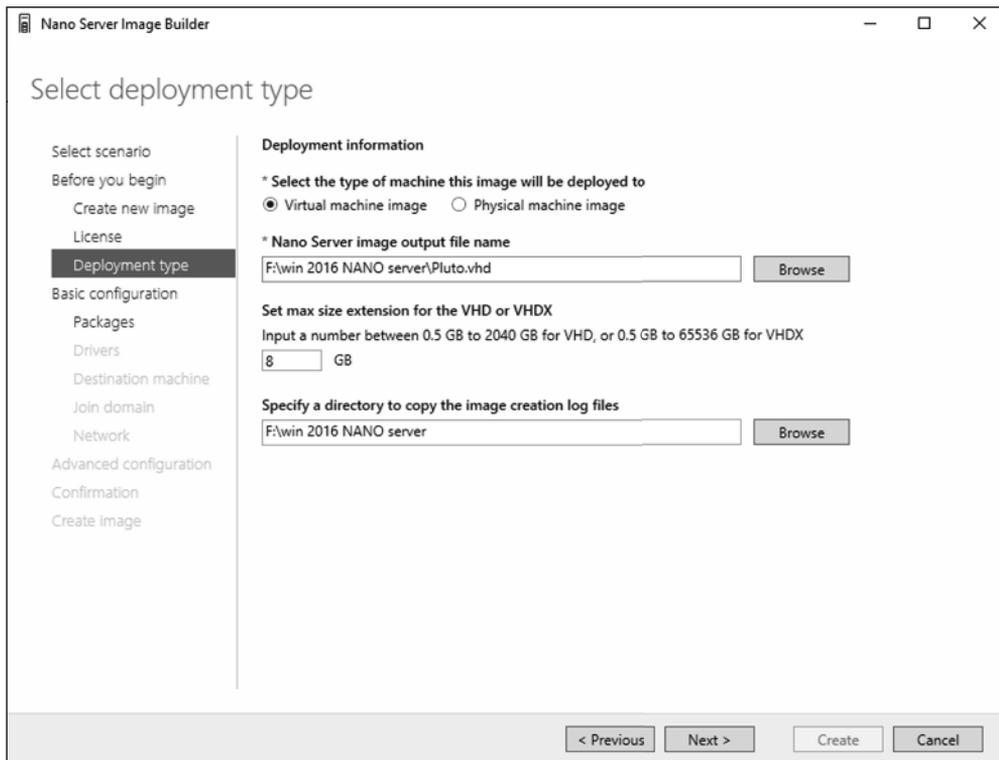


**22.** At the Basic Installation screen, click Next.

**23.** At the Select Optional Packages screen, you can choose any other options you want to install like DNS, IIS, etc. I am just going to click Next.

**24.** At the Drivers screen, add any drivers that may be needed for your installation and click Next.

**25.** Next the Destination screen will appear. Here is where you will enter the name of the computer and the Administrator's password. I am using Pluto as the computer name and P@ssw0rd as the password. Make sure your Time Zone is correct and click Next.

**26.** At this time, I am not going to join a domain. So I am just going to click Next.

**27.** I will leave the default network settings and click Next.

**28.** At the Advanced Configuration Screen, I am going to choose the top option "Create a Basic Nano Server Image" (see Figure 1.15).

**FIGURE 1.15**    Advanced Configuration Screen
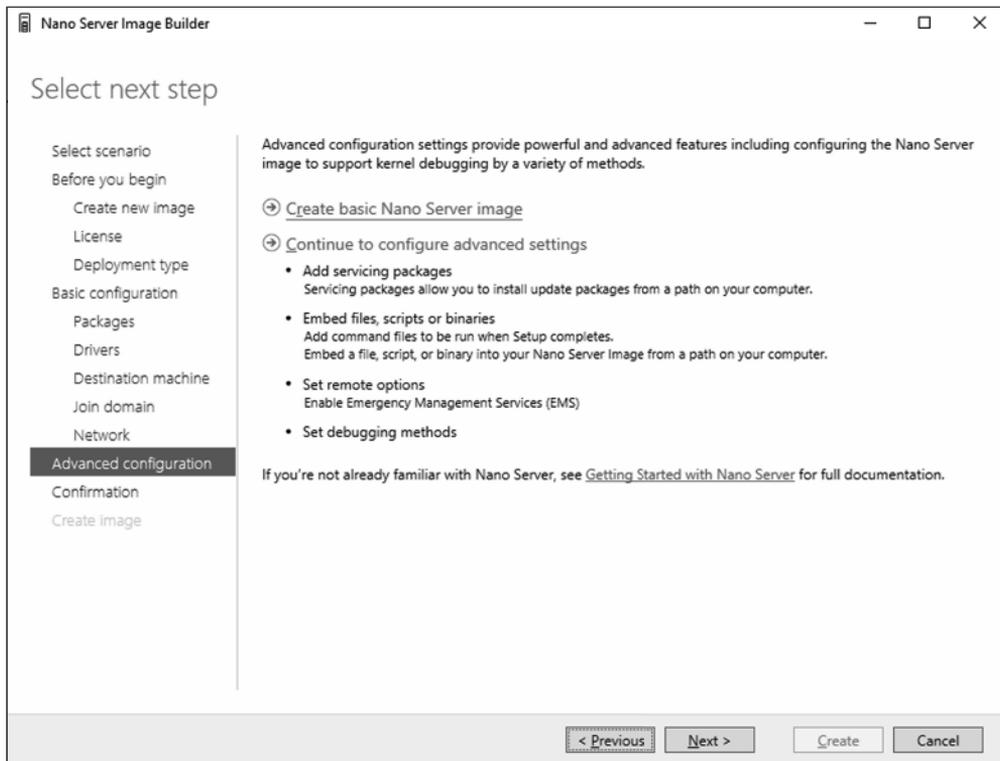


**29.** After you click the link, it will automatically take you to a Confirmation screen. Just click the Create button.

**30.** Once the image is complete, click the Close button.

**31.** Open Windows Explorer and go to the folder where you created the VHD (see Figure 1.16). Make sure the VHD (My VHD is named Pluto.vhd) has been created. You can now run this VHD in Microsoft Hyper-V.

**FIGURE 1.16**   Verifying the Created VHD
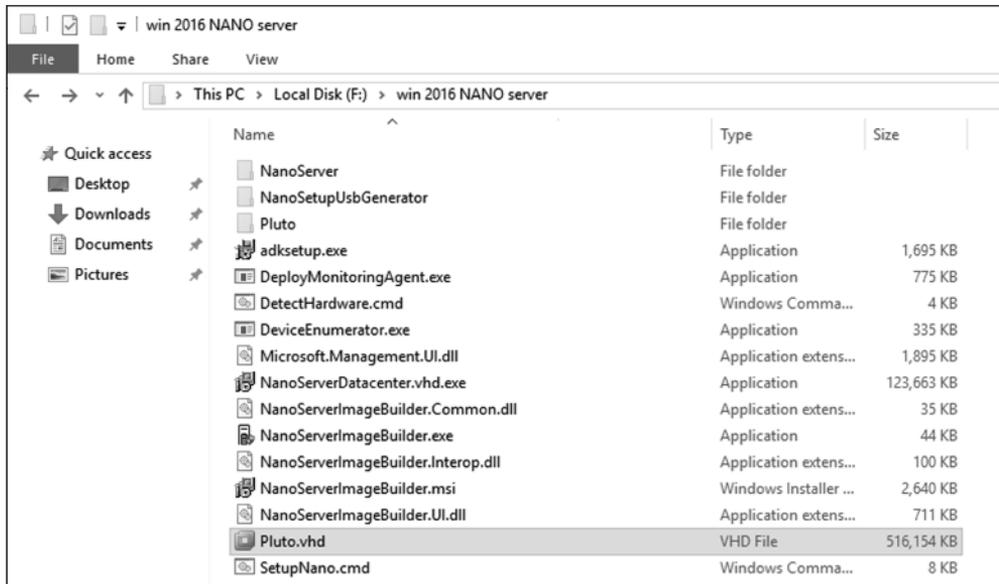


During the installation of the VHD image in Exercise 1.3, at the end of the exercise, the Nano Server Image Builder automatically created a PowerShell command to do the same installation that we just did during the exercise. The following is the PowerShell output that the Nano Server Image Builder automatically created:

```
New-NanoServerImage -MediaPath 'F:\win 2016 NANO server' -Edition 'Datacenter'
-DeploymentType Guest -TargetPath 'F:\win 2016 NANO server\Pluto.vhd' -MaxSize
8589934592 -ComputerName 'Pluto' -SetupCompleteCommand ('tzutil.exe /s
"Eastern Standard Time"') -LogPath 'C:\Users\StormWind\AppData\Local\Temp\
NanoServerImageBuilder\Logs\2016-11-13 17-48'
```

At the time this book was written, Nano Server PowerShell did not allow the following features (this list was taken directly from Microsoft's website);

▪   ADSI, ADO, and WMI type adapters

▪   Enable-PSRemoting, Disable-PSRemoting (PowerShell remoting is enabled by default.)

▪   Scheduled jobs and PSScheduledJob module

- Computer cmdlets for joining a domain { Add | Remove }
- Reset-ComputerMachinePassword, Test-ComputerSecureChannel
- Profiles (You can add a startup script for incoming remote connections with Set-PSSessionConfiguration.)
- Clipboard cmdlets
- EventLog cmdlets { Clear | Get | Limit | New | Remove | Show | Write } (Use the New-WinEvent and Get-WinEvent cmdlets instead.)
- Get-PfxCertificate cmdlet
- TraceSource cmdlets { Get | Set }
- Counter cmdlets { Get | Export | Import }
- Some web-related cmdlets { New-WebServiceProxy, Send-MailMessage, ConvertTo-Html }
- Logging and tracing using PSDiagnostics module
- Get-HotFix
- Implicit remoting cmdlets { Export-PSSession | Import-PSSession }
- New-PSTransportOption
- PowerShell transactions and Transaction cmdlets { Complete | Get | Start | Undo | Use }
- PowerShell Workflow infrastructure, modules, and cmdlets
- Out-Printer
- Update-List
- WMI v1 cmdlets: Get-WmiObject, Invoke-WmiMethod, Register-WmiEvent, Remove-WmiObject, Set-WmiInstance (Use CimCmdlets module instead.)

After Windows Server 2016 server is installed, you need to look at how to activate the server. In the next section, you will learn about the different ways you can activate a Windows Server 2016 system.

# Activating and Servicing Windows

After you complete the installation of Windows Server 2016, the next step is activating the operating system. Windows Server 2016 gives you a few different options when it comes to activation.

In the past, many administrators would use the Volume Activation Management Tool (VMAT) to activate both Microsoft operating systems and Microsoft products like Office. Administrators can still use VMAT to activate Microsoft products like Office but with the release of Windows Server 2016, there are some new ways to help administrators activate the operating systems.

So let's take a look at some of the different activation options that you have with the Windows Server 2016 operating system.

## Key Management Service

Windows Server 2016 Key Management Service (KMS) gives your Windows computers an easy and automated way to get activated. KMS allows your computers to get activated right on your local network without the need of contacting Microsoft. For this to happen, you must setup a KMS client-server network. KMS clients are able to contact KMS servers as long as your network uses either a static TCP/IP configuration or you have a Domain Name System (DNS) server setup.

To configure KMS hosts systems, you must configure and retrieve Volume Activation information. This is done by using a Software License Manager (referred to as SL Manager) script (Slmgr.vbs). This script can be run on a local system or a remote system but it needs to be run from a user's account that uses an elevated command prompt. KMS host systems can be any Windows client operating system running Windows Vista or higher and any Server above Windows Server 2003.

To create or modify the slmgr.vbs script, an administrator can use either the Wscript.exe or Cscript.exe application. Slmgr.vbs uses the Wscript.exe scripting engine by default. After an administrator makes any changes to the Slmgr.vbs script, the Software Licensing Service must be restarted. This can be done by using the Services Microsoft Management Console (MMC) or by running the net stop and net start commands at an elevated command prompt (net stop sppsvc and net start sppsvc).

The Slmgr.vbs script has different command line switches that you can use. Table 1.2 shows you some of the different switches that you can use with the Slmgr.vbs script.

**TABLE 1.2**   Slmgr.vbs switches

| Parameter | Description |
| --- | --- |
| /ato | This switch is used for retail and volume systems editions with a KMS host key or a Multiple Activation Key (MAK) installed. The /ato command prompts Windows to try to do an online activation. For any systems that are using a Generic Volume License Key (GVLK), this will make the system attempt to do a KMS activation. |
| /cdns | This switch allows an administrator to disable KMS host automatic DNS publishing. |
| /cpri | Administrators can use this switch to lower the priority of KMS host processes. |
| /dli | Administrators can use this switch on the KMS host to view the current KMS activation count. |
| /dlv | When an administrator uses this switch, the license information for the installed operating system is displayed. |

| Parameter | Description |
|---|---|
| `/ipk` | This command will try to install a 5x5 product key. |
| `/sai activationInterval` | This switch allows an administrator to change how often a KMS client attempts to activate itself when it cannot find a KMS host. The default setting is 120 minutes, but you can change the interval by replacing `ActivationInterval` with the number of minutes you want to set. |
| `/sdns` | This switch allows an administrator to enable KMS host automatic DNS publishing. |
| `/spri` | This allows an administrator to set the CPU priority of the KMS host processes to Normal. |
| `/sprt PortNumber` | Using this switch allows an administrator to change the default TCP communications port on a KMS host from 1688 to whichever port the admin wants to use. To change the default port number, replace the `PortNumber` switch with the TCP port number to use. |
| `/sri RenewalInterval` | This switch allows an administrator to change how often a KMS client attempts to renew its activation by contacting a KMS host. If you need to change the default of 10080 (7 days), just replace `RenewalInterval` with a number of minutes you want to use. |

To run `Slmgr.vbs` remotely, administrators must supply additional parameters. They must include the computer name of the target computer as well as a username and password of a user account that has local administrator rights on the target computer. If run remotely without a specified username and password, the script uses the credentials of the user running the script.

```
slmgr.vbs TargetComputerName [username] [password] /parameter [options]
```

## Automatic Virtual Machine Activation

Another Windows Server 2016 activation method is called Automatic Virtual Machine Activation (AVMA). The main advantage of AVMA is that is works the same way a proof-of-purchase works. Once that there is proof that the Windows Server 2016 operating system is used in accordance with Microsoft Software License terms, AVMA allows you to install virtual machines on that Windows Server operating system without the need of using or managing product keys for each virtual machine.

AVMA attaches the virtual machine activation to the properly activated Hyper-V machine during the startup process. One of the nice advantages to using AVMA is that AVMA will provide administrators with real time reporting data. When your virtual

servers are properly activated using volume or OEM licensing, AVMA gives an organization many benefits, like activating virtual machines in remote areas and also activating virtual machines even if no Internet connection is present.

One advantage to AVMA activations is that virtual machines are activated as long as the Hyper-V server is legally licensed. This helps consulting companies in the fact that they do not need to access client virtual machines to activate the machines as long as the Hyper-V server is properly licensed. Also, hosting companies can use the server logs to help keep the virtual machines running properly.

AVMA requires Windows Server 2016 with the Hyper-V role installed. AVMA can also run on Windows Server 2012 and Windows Server 2012 R2 if needed. Table 1.3 shows the Windows Server 2016 AVMA (5x5) Keys that are available from Microsoft's website.

**TABLE 1.3**   Windows Server 2016 AVMA Keys

| Edition | AVMA Key |
| --- | --- |
| Datacenter | TMJ3Y-NTRTM-FJYXT-T22BY-CWG3J |
| Standard | C3RCX-M6NRP-6CXC9-TW2F2-4RHYD |
| Essentials | B4YNW-62DX9-W8V6M-82649-MHBKQ |

## Active Directory–Based Activation

One of the best advantages of using Windows Servers is the ability to install Active Directory onto your corporate network. Active Directory is just a centralized database of objects for a corporation called a domain.

For companies running Active Directory, administrators can use this towards their advantage when it comes to activation. Active Directory-Based Activation (ADBA) allows administrators to activate computers right through the domain connection.

Many organizations have remote locations and at these locations there is company owned software that needs to be registered. Normally administrators would use a retail key or a Multiple Activation Key (MAK) to get these products activated. The nice thing about ADBA is that as long as the computers are connected to the domain, the software and products can be activated through the domain.

When an Administrator joins a Windows computer to the domain, the ADBA will automatically activate the computers version of Windows either online with Microsoft or through the use of an activation proxy.

## Servicing Windows Server 2016

Now that we looked at some of the ways to activate your Windows Server 2016 systems, let's take a look at how you can service your Windows Server systems. Table 1.4 will show the different versions for Windows Server 2016 and which servicing model each version uses.

**TABLE 1.4**    Servicing Models for Windows Server 2016

| Installation Option | LTSB Servicing | CBB Servicing |
| --- | --- | --- |
| Desktop Experience | Yes | No |
| Server Core | Yes | No |
| Nano Server | No | Yes |

## Long Term Servicing Branch

Before the release of Windows Server 2016, Windows operating systems used the "5+5" servicing models. What this meant was there were 5 years of mainstream support and 5 years of extended support for the different versions of the Windows operating systems. This model will continue to be used in Windows Server 2016 (Desktop Support and Server Core) but it will be known as Long Term Servicing Branch (LTSB).

## Current Branch for Business

Administrators who decide to install Windows sever 2016 Nano Server will be choosing to use the Current Branch for Business (CBB) servicing model. This version of servicing is a more aggressive version and it was specifically designed with the cloud in mind. As the cloud continues to quickly evolve, the CBB servicing model is meant for that lifecycle. The CBB servicing model will continue to provide new features and functions to Windows Server allowing the server to evolve and grow with the rapidly changing industry. Microsoft's goal is to release updates multiple times per year for Nano Server thus keeping it changing with the industry.

# Using Windows Deployment Services

Another way that many IT departments deploy operating systems has been through the use of Windows Deployment Services (WDS). WDS allows an IT administrator to install a Windows operating system without using an installation disc. Using WDS allows you to deploy the operating system through a network installation. WDS can deploy Windows XP, Windows Server 2003, Windows Vista, Windows 7, Windows 8, Windows 10, Windows Server 2008/2008 R2, Windows Server 2012, Windows Server 2012 R2, and Microsoft Windows Server 2016.

The following are some of the advantages of using WDS for automated installation:

- You can remotely install Windows 7/8/10.
- The procedure simplifies management of the server image by allowing you to access Windows 7/8/10 distribution files from a distribution server.
- You can quickly recover the operating system in the event of a computer failure.

Here are the basic steps of the WDS process from a PXE-enabled WDS client:

1. The WDS client initiates a special boot process through the PXE network adapter (and the computer's BIOS configured for a network boot). On a PXE client, the user presses F12 to start the PXE boot process and to indicate that they want to perform a WDS installation.

2. A list of available Windows PE boot images is displayed. The user should select the appropriate Windows PE boot image from the boot menu.

3. The Windows Welcome screen is displayed. The user should click the Next button.

4. The WDS user is prompted to enter credentials for accessing and installing images from the WDS server.

5. A list of available operating system images is displayed. The user should select the appropriate image file to install.

6. The WDS user is prompted to enter the product key for the selected image.

7. The Partition And Configure The Disk screen is displayed. This screen provides the ability to install a mass storage device driver, if needed, by pressing F6.

8. The image copy process is initiated, and the selected image is copied to the WDS client computer.

The following sections describe how to set up the WDS server and the WDS clients and how to install Windows 7/8/10 through WDS.

## Preparing the WDS Server

With the WDS server, you can manage and distribute Windows 7/8/10 operating system images to WDS client computers. The WDS server contains any files necessary for PXE booting, Windows PE boot images, and the Windows 7/8/10 images to be deployed.

The following steps for preparing the WDS server are discussed in the upcoming sections:

1. Make sure that the server meets the requirements for running WDS.

2. Install WDS.

3. Configure and start WDS.

4. Configure the WDS server to respond to client computers (if this was not configured when WDS was installed).

For WDS to work, the server on which you will install WDS must meet the requirements for WDS and be able to access the required network services.

## WDS Server Requirements

The WDS server must meet these requirements:

- The computer must be a domain controller or a member of an Active Directory domain.
- At least one partition on the server must be formatted as NTFS.

- WDS must be installed on the server.
- The operating system must be Windows Server 2003, Windows Server 2008/2008 R2, Windows Server 2012 / 2012 R2, or Windows Server 2016.
- A network adapter must be installed.

## Network Services

The following network services must be running on the WDS server or be accessible to the WDS server from another network server:

- TCP/IP installed and configured
- A DHCP server, which is used to assign DHCP addresses to WDS clients (Ensure that your DHCP scope has enough addresses to accommodate all of the WDS clients that will need IP addresses.)
- A DNS server, which is used to locate the Active Directory controller
- Active Directory, which is used to locate WDS servers and WDS clients as well as authorize WDS clients and manage WDS configuration settings and client installation options

## Installing the WDS Server Components

You can configure WDS on a Windows Server 2003/2008/2008 R2, Windows Server 2012 / 2012 R2, or Windows Server 2016 computer by using the Windows Deployment Services Configuration Wizard or by using the WDSUTIL command line utility. Table 1.5 describes the WDSUTIL command line options.

**TABLE 1.5**　WDSUTIL command line options

| WDSUTIL Option | Description |
| --- | --- |
| /initialize-server | Initializes the configuration of the WDS server |
| /uninitialized-server | Undoes any changes made during the initialization of the WDS server |
| /add | Adds images and devices to the WDS server |
| /convert-ripimage | Converts Remote Installation Preparation (RIPrep) images to WIM images |
| /remove | Removes images from the server |
| /set | Sets information in images, image groups, WDS servers, and WDS devices |

**TABLE 1.5**   WDSUTIL command line options *(continued)*

| WDSUTIL Option | Description |
| --- | --- |
| /get | Gets information from images, image groups, WDS servers, and WDS devices |
| /new | Creates new capture images or discover images |
| /copy-image | Copies images from the image store |
| /export-image | Exports to WIM files images contained within the image store |
| /start | Starts WDS services |
| /stop | Stops WDS services |
| /disable | Disables WDS services |
| /enable | Enables WDS services |
| /approve-autoadddevices | Approves Auto-Add devices |
| /reject-autoadddevices | Rejects Auto-Add devices |
| /delete-autoadddevices | Deletes records from the Auto-Add database |
| /update | Uses a known good resource to update a server resource |

The first step in setting up WDS to deploy operating systems to the clients is to install the WDS role. You do this by using Server Manager.

One of the advantages of using the Windows deployment server is that WDS can work with Windows image (`.wim`) files. Windows image files can be created through the use of the Windows Sysprep utility.

One component to which you need to pay attention when using the Windows deployment server is *Preboot Execution Environment (PXE)* network devices. PXE boot devices are network interface cards (NICs) that can talk to a network without the need for an operating system. PXE boot NIC adapters are network adapters that have a set of preboot commands within the boot firmware.

This is important when using WDS because PXE boot adapters connect to a WDS server and request the data needed to load the operating system remotely. Remember, most of the machines for which you are using WDS do not have an operating system on the computer. You need NIC adapters that can connect to a network without the need for an operating system for WDS to work properly.

For the same reason, you must set up DHCP to accept PXE machines. Those machines need a valid TCP/IP address so that they can connect to the WDS server.

## Preparing the WDS Client

The WDS client is the computer on which Windows 7/8/10 will be installed. WDS clients rely on a technology called PXE, which allows the client computer to boot remotely and connect to a WDS server.

To act as a WDS client, the computer must meet all of the hardware requirements for Windows 7/8/10 and have a PXE-capable network adapter installed, and a WDS server must be present on the network. Additionally, the user account used to install the image must be a member of the Domain Users group in Active Directory.

After the WDS server has been installed and configured, you can install Windows 7/8/10 on a WDS client that uses a PXE-compliant network card.

To install Windows 7/8/10 on the WDS client, follow these steps:

1. Start the computer. When prompted, press F12 for a network service boot. The Windows PE appears.

2. The Windows Welcome screen appears. Click the Next button to start the installation process.

3. Enter the username and password of an account that has permission to access and install images from the WDS server.

4. A list of available operating system images stored on the WDS server appears. Select the image to install and click Next.

5. Enter the product key for the selected Windows 7/8/10 image and click Next.

6. The Partition And Configure The Disk screen appears. Select the desired disk-partitioning options, or click OK to use the default options.

7. Click Next to initiate the image-copying process. The Windows Setup process will begin after the image is copied to the WDS client computer.

# Understanding Features On Demand

One of the problems in previous versions of Windows Server was how roles and features were stored on the hard disk. Before the introduction of Windows Server 2012, even if a server role or feature was disabled on a server, the binary files for that role or feature were still present on the disk. The problem with this approach is that, even if you disable the role, it still consumes space on your hard drive.

Features On Demand in Windows Server 2012 solves this issue because not only can administrators disable a role or feature, they can also completely remove the role or feature's files. Windows Server 2016 has continued with Features on Demand and administrators can choose what Roles and Features they want to use, when they want to use them.

Once this is done, a state of Removed is shown in Server Manager, or the state of Disabled With Payload Removed is shown in the Deployment Image Servicing and Management (`Dism.exe`) utility. To reinstall a role or feature that has been completely removed, you must have access to the installation files.

> The Deployment Image Servicing and Management (`Dism.exe`) utility is talked about throughout this entire book. DISM will be discussed in great detail when we discuss Windows imaging.

If you want to remove a role or feature completely from the system, use `-Remove` with the `Uninstall-WindowsFeature` cmdlet of Windows PowerShell.

If you want to reinstall a role or feature that has been removed completely, use the Windows PowerShell `-Source` option of the `Install-WindowsFeature Server Manager` cmdlet. Using the `-Source` option states the path where the WIM image files and the index number of the image will be located. If an administrator decides not to use the `-Source` option, Windows will use Windows Update by default.

When you're using the Features On Demand configuration, if feature files are not available on the server computer and the installation requires those feature files, Windows Server 2016 can be directed to get those files from a side-by-side feature store, which is a shared folder that contains feature files. It is available to the server on the network, from Windows Update, or from installation media. This can be overwritten using the `-Source` option in the Windows PowerShell utility.

---

### Source Files for Roles or Features

Offline virtual hard disks (VHDs) cannot be used as a source for installing roles or features that have been completely removed. Only sources for the same version of Windows Server 2016 are supported.

---

To install a removed role or feature using a WIM image, follow these steps:

1. Run the following command:

   ```
   Get-windowsimage –imagepath \install.wim
   ```

   In step 1, *imagepath* is the path where the WIM files are located.

2. Run the following command:

   ```
   Install-WindowsFeature featurename -Source wim: path:index
   ```

   In step 2, *featurename* is the name of the role or feature from `Get-WindowsFeature`. *path* is the path to the WIM mount point, and *index* is the index of the server image from step 1.

To add or remove a role or feature, you must have administrative rights to the Windows Server 2016 machine.

# Summary

In this chapter, you studied the latest advantages of using Windows Server 2016. You also learned about the different roles and features you can install on a Windows Server 2016 machine. You also explored how to migrate those roles and features from a Windows Server 2008, 2008 R2, and Windows Server 2012 machine to a Windows Server 2016 machine.

I discussed the different upgrade paths that are available and which upgrades are best for your current network setup. You learned that another important issue to decide when installing Windows Server 2016 is whether to use Server Core or the GUI installation.

You learned how to install Windows Server 2016 Datacenter (Desktop Experience), and you installed the Windows Server 2016 Server Core. Remember, Server Core is a slimmed-down version of Windows Server. With no GUI desktop available, it's a safer alternative to a normal Windows install.

I discussed a feature called Features On Demand. This feature allows you to remove roles and features from the operating system and remove the associated files completely from the hard drive, thus saving disk space.

# Video Resources

There are videos available for the following exercises:

1.1

1.2

You can access the videos at `http://sybextestbanks.wiley.com` on the Other Study Tools tab.

# Exam Essentials

**Understand the upgrade paths.** It's important to make sure you understand the different upgrade paths from Windows Server 2012 and Windows Server 2012 R2 to Windows Server 2016.

**Understand Windows Server 2016 server roles.** Understand what the Windows Server 2016 server roles do for an organization and its users.

**Understand Features On Demand.** Understand the feature called Features On Demand. Microsoft loves to ask exam questions about its new features, and this will be no exception. Understand how features and roles stay on the system until you physically remove them from the hard drive.

**Understand Windows Deployment Services.** Know how to install and configure a Windows Deployment Services (WDS) server. Know the WDS network requirements and components.

# Review Questions

1. You are the administrator for the ABC Company. You are looking to install Windows Server 2016, and you need to decide which version to install. You need to install a version of Windows that is just for logon authentication and nothing else. You want the most secure option and cost is not an issue. What should you install?

   **A.** Windows Server 2016 Datacenter (Desktop Experience)

   **B.** Windows Server 2016 Datacenter Server Core

   **C.** Windows Server 2016 Standard (Desktop Experience)

   **D.** Windows Server 2016 Web Server Core

2. You are the IT manager for a large organization. One of your co-workers installed a new Windows Server 2016 Datacenter Server Core machine, but now the IT team has decided that it should be a Windows Server 2016 Datacenter (Desktop Experience). What should you do?

   **A.** Reinstall Windows Server 2016 Datacenter Server Core on the same machine.

   **B.** Install a new machine with Windows Server 2016 Datacenter Server Core.

   **C.** Convert the current Windows Server 2016 Datacenter Server Core to the Windows Server 2016 Datacenter (Desktop Experience) version.

   **D.** Dual-boot the machine with both Windows Server 2016 Datacenter Server Core and Windows Server 2016 Datacenter (Desktop Experience).

3. You are the administrator for your company, and you are looking at upgrading your Windows Server 2012 Standard with GUI to Windows Server 2016. Which version of Windows Server 2016 does Microsoft recommend you use to keep the GUI interface?

   **A.** Windows Server 2016 Datacenter (Desktop Experience)

   **B.** Windows Server 2016 Standard (Desktop Experience)

   **C.** Windows Server 2016 Datacenter

   **D.** Windows Server 2016 Standard

4. You are looking at upgrading your Windows Server 2012 R2 Datacenter with GUI machine to Windows Server 2016. Your organization is considering virtualizing its entire server room, which has 25 servers. To which version of Windows Server 2016 would you upgrade while keeping the GUI interface?

   **A.** Windows Server 2016 Datacenter (Desktop Experience)

   **B.** Windows Server 2016 Standard (Desktop Experience)

   **C.** Windows Server 2016 Datacenter

   **D.** Windows Server 2016 Standard

5. You have been hired to help a small company set up its first Windows network. It has had the same 13 users for the entire two years it has been open, and the company has no plans to expand. What version of Windows Server 2016 would you recommend?

   **A.** Windows Server 2016 Datacenter (Desktop Experience)

   **B.** Windows Server 2016 Standard (Desktop Experience)

   **C.**  Windows Server 2016 Datacenter

   **D.**  Windows Server 2016 Essentials

**6.** You have been hired to help a small company set up its Windows network. It has 20 users, and it has no plans to expand. What version of Windows Server 2016 would you recommend?

   **A.**  Windows Server 2016 Datacenter

   **B.**  Windows Server 2016 Standard

   **C.**  Windows Server 2016 Essentials

   **D.**  Windows Server 2016 Datacenter (Desktop Experience)

**7.** Which of the following are benefits of using Windows Server 2016 Server Core? (Choose all that apply.)

   **A.**  Reduced management

   **B.**  Minimal maintenance

   **C.**  Smaller footprint

   **D.**  Tighter security

**8.** You are a server administrator, and you are trying to save hard drive space on your Windows Server 2016 Datacenter machine. Which feature can help you save hard disk space?

   **A.**  `HDSaver.exe`

   **B.**  Features On Demand

   **C.**  ADDS

   **D.**  WinRM

**9.** You are the IT Director for your company. Your company needs to install a version of Windows Server 2016 that uses the Current Branch for Business servicing model. What version would you install?

   **A.**  Windows Server 2016 Datacenter

   **B.**  Windows Server 2016 Standard

   **C.**  Windows Server 2016 Essentials

   **D.**  Windows Server 2016 Nano Server

**10.** What type of domain controller would you install into an area where physical security is a concern?

   **A.**  Primary domain controller

   **B.**  Backup domain controller

   **C.**  Read-only domain controller

   **D.**  Locked-down domain controller