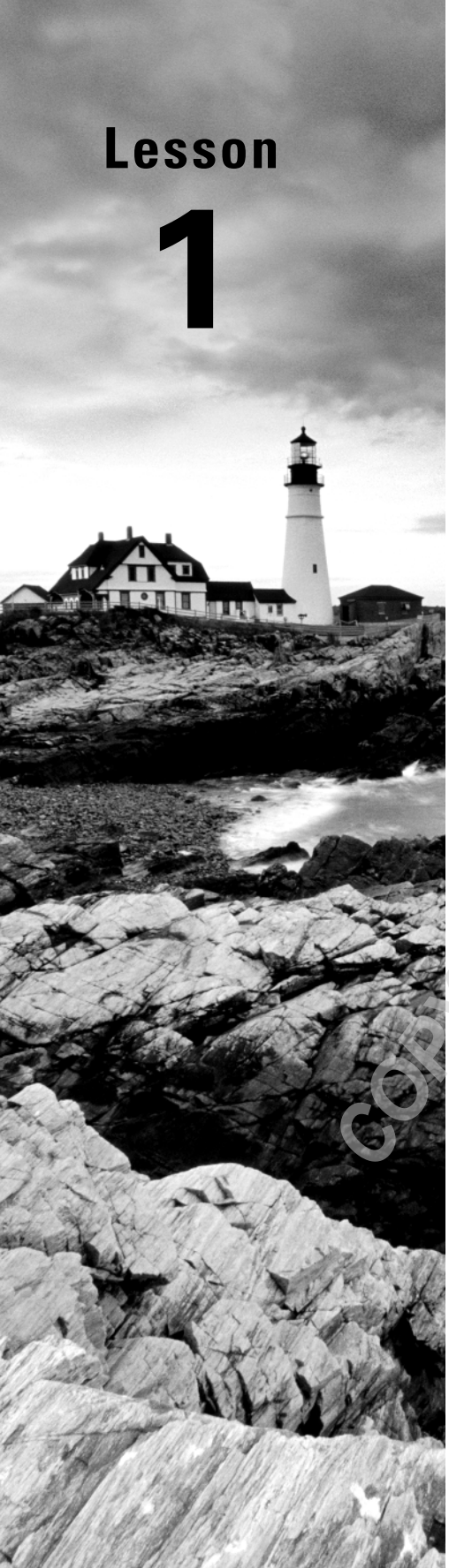


Lesson

1

Server Overview

Objective Domain Matrix

Technology Skill	Objective Domain Description	Objective Domain Number
Installing Windows Server 2016	Understand server installation options.	1.3
Introducing Server Roles	Identify application servers.	2.1
Comparing Physical Servers and Virtual Servers	Understand server virtualization.	2.5
Selecting Server Hardware	Identify major server hardware components.	5.1
Understanding Updates	Understand updates.	6.3

Key Terms

BIOS
clean installation
disk cloning
drives
firmware
motherboard
network connections
Nano Server
ports
power supply
processor
RAM
server
Server Core
server features
server role
system preparation tool
unattended installation
upgrade installation
virtual server
Windows Activation
Windows Deployment Services (WDS)
Windows Updates

Real World Scenario

Lesson 1 Case

You just got hired at the Acme Corporation. They have several Windows Server 2012 and Windows Server 2012 R2 Servers and a Windows Server 2016 Server. While talking to your management team, you determine that you need to upgrade all of the servers to Windows Server 2016 and you need to create a web farm consisting of 3 new web servers and a single backend SQL server, also running Windows Server 2016. Therefore, you need to figure out the best way to get to your goal.

Understanding What a Server Does

With today's computers, any computer on the network can provide services or request services depending on how the network is set up. A *server* is a computer that is a meant to be a dedicated service provider, and a client is a computer that requests services. A network that is made up of dedicated servers and clients is known as a client/server network. A server-based network is the best network for sharing resources and data, while providing centralized network security for those resources and data. Networks with Windows Server 2016 are usually client/server networks.

If you have been using Windows 7, Windows 8/8.1, or Windows 10 for a significant amount of time, you should realize that your computer is providing services and requesting services (although it most likely requesting services more than it is providing services). When you access a web page over the Internet, access your email, access a data file on another computer, or access a printer that is connected to the network, you are requesting services. While Windows servers are designed to provide a wide range of network services, Windows 7, Windows 8/8.1, and Windows 10 can provide printer and file sharing and web pages (although you are limited by the number of concurrent connections especially when compared to Windows servers and are not optimized for multi-user access). Therefore, while these versions of Windows are designed as clients, they can also provide services.

While computers with Windows Server 2016 are designed to provide services, they can also request services from other computers. For example, they can access a web server locally or over the Internet, access a software repository, or print to a network printer.

When determining the hardware and software needs, you need to look at the role that the computer needs to fill and the load the computer will be placed under. You can then start researching the hardware (including the number of computers, number of processors, amount of RAM, and amount of disk storage) and software requirements to reach those goals. You also need to look at disaster recovery including looking at the steps you will need to take if a server fails and you lose data.

Don't forget to plan your server for growth. Most servers should be designed for 3–5 years of service. So make sure you look at what your landscape may look at 3–5 years from deployment of the server. This will help you avoid purchasing and reinstalling the server several months later. It should also be noted that the bare basic of a server leaves little room for growth.

Introducing Server Roles

Before selecting the hardware and software components of a server, you must first understand what your server is supposed to do. The first step is to identify the server roles and network services that the server will need to provide. You also need to look at how many people will be accessing the server at once to help determine the load the server needs to fulfill.

Certification Ready?

Can you list and describe the basic server roles? 2.1

A *server role* is a primary duty that a server performs. You should note that a server could have multiple roles. Some of the more common server roles include:

- File services
- Print services
- Web services
- Remote access
- Application servers
- Email server
- Database server

A file server allows you to centrally locate files to be accessed by multiple people. Since the files are centrally located, it makes it easier for multiple users to access and find files (assuming they are organized well) and it is easier to back up these files since they are located in a single place. When using Microsoft Windows to provide file sharing, you will usually be using Server Message Block (SMB) to access Microsoft Shares or shared folders. Windows Servers can also provide NFS shares for Unix/Linux users.

Print services allow multiple users to access a centrally located printer. This allows you share an expensive printer that is fast or is a heavy-duty printer or supports advanced options such as color. Printers can be accessed as a network printer that is connected directly to the network or through a Microsoft Windows server (again using SMB).

Since the Internet has become more prevalent in today's business application, so has the use of web services. A web server will provide web services so that users can access web pages using their browser. These web services may be used to do research, provide leads for sales, allow customers to purchase goods and services, and provide customer support over the Internet. It can also be used to provide an easy method to access databases, run reports, track sales leads, provide customer support, and even help you with payroll and human resources. Since you are using your standard browser such as Internet Explorer, you will be using the Hypertext Transfer Protocol (HTTP) or HTTP Secure (HTTPS) protocols. Microsoft provides web services using Internet Information Services (IIS).

Remote access is a service that supports multiple inbound requests to connect to the server or network. It can provide terminal services so that multiple users can log on to a server remotely and access a desktop, start menu, and programs much like if they were sitting in front of the server. On the other hand, remote access can also provide network

access over the Internet using a virtual private network (VPN), which allows a user to be at home yet have full access to their internal network resources such as email and data files.

Lastly, the application server role provides an integrated environment for deploying and running server-based business applications. In other words, the server will provide a network application. Different from accessing a file from a shared folder and your PC doing all of the work, the server will also do some of the processing.

When talking about server and server applications, you may hear the terms front end and back end. In client/server applications, the client part of the program is often called the front end, and the server part is called the back end. The front end is the interface that is provided to a user or another program. It may be accessed via a web page or a customized application that runs on the client PC. The back end will often contain a database that is used to store, organize, query and retrieve data.

One commonly used application server that is essential for most corporations is the mail server. The mail server is a server that stores and manages electronic messages (email) among users. If you are using Microsoft email products, you will be using Microsoft Exchange to act as your mail servers, and you would most likely access the email using Microsoft Outlook or a web browser.

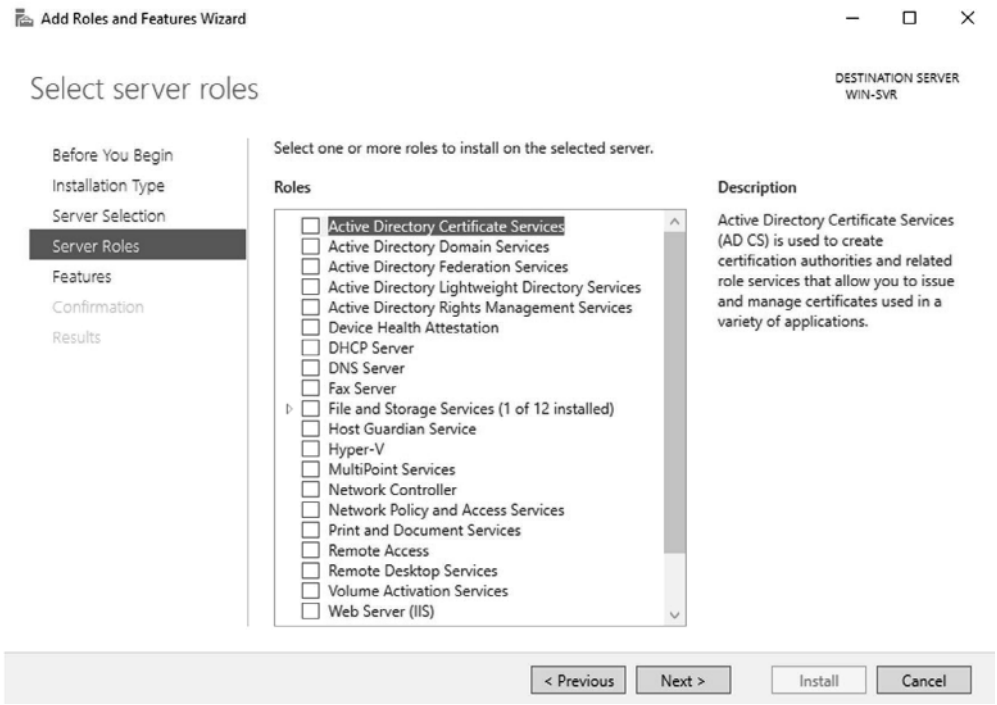
Another example of an application server is if you have a sales tracking application or inventory control applications. You would access this type of server on your company network by using a customized program or using your browser. You will then request information or input some data, which will then be retrieved from or sent to the backend server running a database such as Microsoft SQL server.

When Windows Server 2016 is installed, an administrator has a very important decision to make. They need to decide which roles and features will be installed on the new server. Many administrators do not properly utilize their servers; they may overuse or underutilize them. Domain controllers can help an administrator authenticate users on the network. But once they have authenticated the users, their tasks have been completed and then are not very busy during the day. Domain controllers have some tasks that they must complete all day, but the server where they occupy is not as heavily used when compared to say a SQL Server or an Exchange mail server.

If a domain controller is being used as a virtual machine or if there are more than enough servers, then having a domain controller with no other applications on it (except DNS) may be acceptable. But if the servers are limited, then maybe consider putting other services or applications on the server. Remember, some applications work better on a member server than they do on domain controllers. So make sure to research an application to determine best practices.

Knowing the different roles and features that can be installed on a Windows Server 2016 machine can help an administrator to design, deploy, manage, and troubleshoot technologies in Windows Server 2016. Some of the available roles in Windows Server 2016 can be seen in Figure 1.1, which shows the Add Roles and Features Wizard in Server Manager.

FIGURE 1.1 Available roles in Windows Server 2016



The following roles can be installed on a Windows Server 2016 machine:

Active Directory Certificate Services (AD CS) The AD CS server role allows an administrator to build a public key infrastructure (PKI) and provide public key cryptography, digital certificates, and digital signature capabilities for an organization. AD CS provides a set of customizable services that allows an administrator to issue and manage PKI certificates. These certificates can be used in software security systems that employ public key technologies.

Active Directory Domain Services (AD DS) The AD DS server role allows an administrator to create 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 (AD FS) AD FS provides Internet-based clients with a secure identity access solution that works on 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 (AD LDS) AD LDS is a 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 (AD RMS) AD RMS is the server role that provides an administrator 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 Helps protect a corporate network by verifying that client systems meet corporate policy. For example, an administrator can make sure that all computers connected to a network have their proper updates, antivirus, and proper configuration policies before connecting to the network.

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

Domain Name System (DNS) 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 an administrator to locate computers and services using their user-friendly names.

Fax Server Allows an administrator to send and receive faxes. It also allows an administrator to manage fax resources such as jobs, settings, reports, and fax devices on a specific computer or on the network.

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 a network where an administrator 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 an organization, then administrators should set up the network servers as file servers.

Host Guardian Service (HGS) Allows an administrator to have a more secure environment for the organization's virtual machines. The HGS role provides the Attestation & Key Protection services that enable Guarded Hosts to run Shielded virtual machines.

Hyper-V 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 Allows multiple users, each with their own independent and familiar Windows experience, to simultaneously share one computer.

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 (NPS) Administrators use this server role to install and configure Network Policy Server (NPS), which helps safeguard the security of a network.

Print and Document Services Allows an administrator to centralize print server and network printer tasks. This role also allows an administrator 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 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 a corporate network to client devices outside of the corporate network. Remote Access also includes routing capabilities, including Network Address Translation (NAT).

Remote Desktop Services Allows for faster desktop and application deployments to any device, improving remote user effectiveness while aiding 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 Helps an organization benefit from using this service to deploy and manage volume licenses for a medium to large number of computers.

Web Server (IIS) 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 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 Allows an administrator to set up the IT infrastructure and provides a powerful functions such as PC backups to help protect corporate data and Remote Web Access that allows access to business information from anywhere in the world. Windows Server Essentials Experience also allows for easy connection to cloud-based applications and 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.

Configure Windows Server Security Settings

All Windows operating systems include security settings that an administrator can use to help harden computer security profiles. Microsoft publishes these security baselines and

are based on Microsoft security recommendations. These are created from real-world security experience obtained through a partnership with commercial organizations and the US government.

These security baselines include recommended settings for Windows Firewall, Windows Defender, and other security settings. These are provided as Group Policy object (GPO) backups that an administrator can import into Active Directory Domain Services (AD DS) and then deploy them to domain-joined servers. Ad administrator can also use the Local Script tools to configure standalone (non-domain-joined) servers.

Back Up Information and Systems

An administrator should perform scheduled backups, including any applications and data stored on Windows Server. This will help protect against attacks on the server. An administrator should perform backups frequently so that they can easily restore to a point-in-time prior to an attack.

An administrator can perform backup's on-premises by using solutions such as System Center Data Protection Manager or cloud-based backups by using Microsoft Azure Backup Server. There are also a number of backup solutions available from Microsoft partners.

Management and Monitoring Using Operations Management Suite

Microsoft Operations Management Suite (OMS) is a cloud-based IT management solution that helps administrators manage and protect their on-premises and cloud infrastructure. OMS is a cloud-based service, and an administrator can manage their apps, services, and infrastructure with minimal cost. OMS is updated periodically with new features and can help reduce an organizations ongoing maintenance and upgrade costs.

OMS also works with on-premises System Center components to broaden an organizations existing management investments on the cloud. System Center and OMS work together to provide a full hybrid management experience.

OMS offers the following capabilities and features:

- Automation and control—this feature automates administrative processes with runbooks using Windows PowerShell. Runbooks can access apps, operating systems, or services that are managed using PowerShell. It also provides configuration management with Windows PowerShell Desired State Configuration (DSC), which can enforce an organization's configuration settings on-premises and in Azure automatically.
- Insight and analytics—this feature can collect, correlate, search, and act on logs and performance data generated by Windows operating systems and apps. It provides real-time insights for all of an organization's workloads and servers, on-premises and in Azure.
- Protection and recovery—this feature can back up recovery workloads and servers. Azure Backup protects app data for on-premises and cloud-based servers. Azure Site Recovery helps provide disaster recovery by coordinating replication, failover, and recovery of on-premises Hyper-V virtual machines.

- Security and compliance—this feature identifies, assesses, and mitigates security risks. To ensure the ongoing security of an on-premises and cloud workloads and servers, it uses:
  - Security and Audit solution—collects and analyzes security events
  - Antimalware solution—provides current malware protection status
  - System Updates solution—provides current software update status

Protect Privileged Identities

Privileged identities are accounts that have an elevated privilege, such as a user account that is a member of the Domain Admins, Enterprise Admins, or Local Administrators. These can also include accounts that have been granted privileges directly, such as being able to perform backups or other rights listed in the User Rights Assignment node in the Local Security Policy console.

Administrators need to protect these privileged identities from attackers. It's important to understand how identities can get compromised; then an administrator can try to plan on preventing attackers from accessing these accounts.

Privileged identities can get compromised when an organization doesn't have guidelines in place on how to protect them. Some examples how privileged identities can get compromised:

- An organization is using more privileged accounts than are necessary.
- Being signed in with elevated privileges all the time, which allows for unlimited duration, can make the account susceptible to attack and increases the odds that the account can be compromised.
- Social engineering research. Most credential attackers start out by researching an organization and then conducting social engineering.
- Leveraging accounts with elevated privileges. Attackers can gain access to accounts with elevated permissions. One of the more common methods of doing so is by using the Pass-the-Hash or Pass-the-Token attacks.

TABLE 1.1 How to Prevent Attackers from Gaining Access to Privileged Identities

Methods used for preventing an attacker from gaining access to privileged identities	How to mitigate
More privileges than are necessary	Implement Just Enough Administration (JEA) for all IT administrators who administer Windows Server and the apps and services running on Windows Server by using Windows PowerShell.
Signed in using elevated privileges all the time	Implement Just in Time Administration (JIT) for all users who require elevated privileges so that the elevated privileges can only be used for a limited amount of time.

Methods used for preventing an attacker from gaining access to privileged identities	How to mitigate
Compromising identity and Pass-The-Hash attacks	Implement Microsoft Advanced Threat Analytics (ATA) to help detect compromised identities in on-premises workloads and servers. ATA is an on-premises solution that can be used to manage physical and virtualized workloads.
Pass-The-Hash attacks	Implement Credential Guard to help protect credentials from attacks. Can also implement Remote Credential Guard to help protect credentials from attacks such as Pass-the-Hash or Pass-the-Token that can be performed on servers that host Remote Desktop connections.
Just Enough Administration (JEA)	JEA is a security technology that helps restrict IT administrative rights using Windows PowerShell remoting. JEA uses the built-in capabilities of the Windows PowerShell scripting environment and implements role-based access control (RBAC). An administrator can configure JEA as a Windows PowerShell session endpoint on any computer to manage that computer or remote computers. With JEA, an administrator connects using a regular, non-elevated user credentials. After JEA authorizes the account, the JEA runs the Windows PowerShell commands specified by using an elevated virtual account on the targeted computer. With this approach the user account is never actually signed in by using elevated credentials.
Just in Time Administration (JIT)	JIT Administration is a security best practice that allows an administrator to only use elevated identities when performing IT administration tasks. Microsoft provides JIT administration using the following: ▪ Local Administrator Password Solution (LAPS)—available as a free download to help manage local administrator password on Windows operating systems in your organization. ▪ Microsoft Identity Manager 2016—an on-premises identity and access management system that provides JIT administration.
Advanced Threat Analytics (ATA)	ATA is an on-premises product that helps detect identity compromise in an organization. ATA has the ability to capture and parse network traffic for authentication, authorization, and information gathering protocols. ATA uses this data to build a profile about users and other entities on a network so that it can detect anomalies and known attack patterns.

TABLE 1.1 How to Prevent Attackers from Gaining Access to Privileged Identities *(continued)*

Methods used for preventing an attacker from gaining access to privileged identities	How to mitigate
Credential Guard	Credential Guard uses virtualization-based security for encryption so that only privileged system processes can access them. It is used to help protect privileged identities by protecting the credentials on Windows Server 2016. Credential Guard uses: ▪ Virtualization-based security (required) ▪ Secure boot (required) ▪ TPM 2.0 either discrete or firmware (preferred—provides binding to hardware) The virtualization-based security requires: ▪ 64-bit CPU ▪ CPU virtualization extensions plus extended page tables ▪ Windows hypervisor
Remote Credential Guard	Remote Credential Guard helps protect credentials over a Remote Desktop connection by keeping the credentials on the device hosting the RDP connection and redirecting Kerberos requests back to the device that establishes the connection. If the server (or client) hosting the Remote Desktop connection is compromised, the credentials are not exposed because the credentials and credential derivatives are never sent to the device hosting the Remote Desktop connection. To use Remote Credential Guard, the Remote Desktop client and server must meet the following requirements: ▪ Must be joined to an Active Directory domain and be in the same domain or a domain with a trust relationship. ▪ Must use Kerberos authentication. ▪ Must be running at least Windows 10 version 1607 or Windows Server 2016. ▪ The Remote Desktop classic Windows app is required. The Remote Desktop Universal Windows Platform app doesn't support Remote Credential Guard. You can enable Remote Credential Guard by using a registry setting on the Remote Desktop server and Group Policy or a Remote Desktop Connection parameter on the Remote Desktop client.

Methods used for preventing an attacker from gaining access to privileged identities	How to mitigate
Harden the Windows Server	Windows Server 2016 includes built-in security mechanisms and powerful security tools that can be configured to further lock down the server.
Control Flow Guard	Control Flow Guard is built into Windows to help protect the operating system and applications from a class of memory corruption—based attacks.

Windows Defender	Windows Defender is included in the Windows operating system. It helps protect Windows devices against viruses, malware, spyware, and other threats. Windows Defender has been optimized for running on Windows Server and is enabled by default in Windows Server 2016.
	The advanced security features include:
	▪ Virus protection and removal
	▪ Malware protection and removal
	▪ Spyware protection and removal
	▪ Boot-time protection
	▪ Real-time protection
	▪ Cloud-based protection
	  ▪ Network inspection and protection
	  ▪ Free automatic updates to antimalware definitions and Windows Defender itself
	Can configure Windows Defender by using Group Policy, Windows PowerShell, Windows Management Instrumentation (WMI), or interactively through the Windows Defender user interface. The Windows Server security baselines also include Microsoft recommended settings for Windows Defender.

TABLE 1.1 How to Prevent Attackers from Gaining Access to Privileged Identities *(continued)*

Methods used for preventing an attacker from gaining access to privileged identities	How to mitigate
Device Guard	Device Guard provides the ability to specify which binaries are authorized to run on a server, including user mode and kernel mode binaries. Helps protect against the following threats: ▪ Exposure to new malware for which no malware signature is yet known ▪ Exposure to unsigned code as most malware is unsigned ▪ Malware that gains access to the kernel and then captures sensitive information or damages the system Device Guard code integrity policies can be run in the following modes: ▪ In audit mode, Device Guard will trigger an audit log event whenever a non-authorized binary is running but will not block the binary from running. The Device Guard logs are available in the following event log: `Logs\Microsoft\Windows\CodeIntegrity\Operational`. Audit mode allows an administrator to identify apps that are note wanted in the organization. Can create a code integrity policy file based on the captured audit information in the event log. ▪ In enforcement mode, Device Guard will block any binary that should be denied. Should configure Device Guard for enforcement mode after a selected group of devices in audit mode has identified the apps to allow.
Secure Boot	Secure Boot is an industry standard that helps ensure that a device boots only software that is trusted by the device manufacturer. Secure Boot helps protect devices from rootkits and other low-level malware attacks by blocking unauthorized (non-signed) software. When a device starts, the device firmware checks the signature for each piece of boot software to ensure they are trusted. If all boot software signatures can be confirmed, the firmware starts the operating system. Need to ensure that Secure Boot is enabled in the device's firmware.

Methods used for preventing an attacker from gaining access to privileged identities	How to mitigate
Operations Management Suite (OMS)	An administrator can use OMS to help detect threats as well as identify devices that are not current on software updates and antimalware definitions.
Improve threat detection	Threat detection is an essential part of Windows Server security. The sooner a threat can be detected the quicker an administrator can react before an attacker can reach full control. Microsoft provides threat detection for servers using Windows Defender Advanced Thread Protection (ATP).

Selecting Server Hardware

When choosing what server to use and what hardware components make up the server, keep the following in mind. First, the server is designed to provide network services. Since a server is designed to be used by multiple users at the same time, the server is usually much more powerful than most client PCs. Remember that, if the server fails or becomes inaccessible, the problem will affect multiple people. Therefore, you need to choose hardware that is less prone to failure than a normal client PC and has some redundancy built in. You also need to make up plans so you know how to deal with these problems when they occur.

Certification Ready?

What subsystems affect server performance the most? 5.1

The primary subsystems that make up a server are:

- Processor
- Memory
- Storage
- Network

If any of these fails, the entire system can fail. In addition, if any one of these is asked to do more than what it was designed for, it can cause a bottleneck that may affect the performance of the entire system.

While you strive for a 100% up-time, it is next to impossible to get it over a long enough period of time. However, by anticipating the type of failure that could occur, adding additional servers, components, or technology that will make the system more fault tolerant, and making up good plans so that you can react quickly when a failure occurs, you can mediate much of this to reduce your chances of a failure and to reduce the effect of a failure. In addition, while you need to spend money to make a system more fault tolerant, just about every organization has a limit on how much money they can put toward a server or network service.

The subsystems just listed are not the only components that make up the server but are the primary ones that are often looked at when determining what a server can handle. Servers may also include sound cards, but normally do not need to provide sound to multiple users using the sound card. Instead, data will be sent over the network to an individual client, and the client sound card will produce the sound. The same could also be said for video. You are not going to have 20 monitors connected to a single computer providing graphics. Therefore, you do not normally require a high-performance video system for the server.

Processor

The computer, including servers, is built around one or more integrated chips called the *processor*. It is considered the brain of the computer since all of the instructions it performs are mathematical calculations and logical comparisons. Today's processors are mostly produced by Intel and AMD.

Today, the clock speed of the processor is usually expressed in gigahertz (GHz). A gigahertz is 1 billion (1,000,000,000) cycles per second. During each cycle, a circuit will react in a predictable way (bring in a value, perform a calculation, or perform a comparison). It is these reactions that make the computer do what it does. Of course, if a processor runs at a faster speed, it would be safe to assume it could do more in a quicker amount of time.

Over the last several years, though, speed is not the only factor that determines processor performance. Today, processors sold today are multi-core processors, which are like having two or more processing cores packaged as one. In addition, they use other technologies to keep the processor working at peak efficiency much like using an assembly line approach or trying to anticipate what it needs to do first so that it can keep the pipelines always working.

Having additional cores doesn't always mean a linear increase in performance. For example, having two cores doesn't always means that you get double the performance. In these cases, performance is limited by how well the software is optimized to use both cores.

Another factor is how much data a processor can process. Today's processors are 64-bit processors as compared to the older 32-bit processors. A 64-bit processor is a processor with a default word size of 64 bits and 64-bit external data bus. Most people don't realize that today's processors can already handle 64-bit calculations (remember every value,

small and large numbers, and numbers with decimal points are broken down into 0s and 1s (bits)). Most processors internally can process 128, 256, and maybe larger numbers. But one of the main benefits of 64-bit processors is that they can process significantly more memory than 32-bit processors (4 GB with a 32-bit address bus and 64 GB with a 36-bit address bus). Technically a 64-bit processor can access up to 16.3 billion gigabytes (16 exabytes). The AMD64 architecture currently has a 52 bit limit on physical memory (which supports up to 4 petabytes or 4048 terabytes) and only supports a 48-bit virtual address space (256 terabytes). Usually, you will reach the limit of the motherboard or memory chips before you reach the limit of the processor.

With more data in memory, a 64-bit processor can work faster because it can access larger amounts of RAM instead of swapping data back and forth with the much slower disks. In addition, with the larger internal registrys, it can process larger numbers without breaking them into several smaller numbers, and it can even take several smaller numbers and do some mathematically calculation or comparison to these numbers at the same time. Today, just about every computer processor sold is a 64-bit processor.

Today's 64-bit processors include virtualization technology (VT), which enables a processor to act as if it were several processors working in parallel, to enable several operating systems to run at the same time in the same machine. As of this writing, to run Microsoft's Hyper-V, which is Microsoft's virtualization software, you need to have processors and BIOS that support virtualization technology.

If an operating system and programs are written to use the larger 64-bit calculations and use the additional accessible memory, the processing power of a computer can be significantly increased. Most programs designed for a computer running a 32-bit version of Windows will work on a computer running 64-bit versions of Windows. Notable exceptions are some antivirus programs and some hardware drivers. The biggest problem that you may encounter is finding 64-bit drivers for some of your older hardware devices.

RAM

RAM, which stands for random access memory, is the computer's short-term or temporary memory. It stores instructions and data that the processor accesses directly. If you have more RAM, you can load more instructions and data from the disks. In addition, having sufficient RAM can be one the largest factor in your overall computer performance. Unfortunately, if power is discontinued from the RAM such as what occurs when you shut off your PC, the contents of the RAM disappear. This is the reason you use disks for long-term storage.

Storage

Traditionally, hard *drives* are half electronic/half mechanical devices that store magnetic fields on rotating platters. Today, some hard drives, known as solid-state drives, are electronic devices with no mechanical components. Since solid-state drives do not contain mechanical components, they are much faster than half electronic/half mechanical devices. While most personal computers have only local storage consisting of internal hard drives, servers may connect to external storage through a network-attached storage (NAS) or storage area network (SAN).

Most systems today have some form of optical drive. Older systems will have compact disk drives, which use disks similar to a music CD player. Newer systems have either a DVD or Blu-Ray drive. In either case, the optical drives store information using laser light. Traditional, optical disks were considered as read-only devices, but many systems have burning capabilities that allow the user to write data to special optical disks.

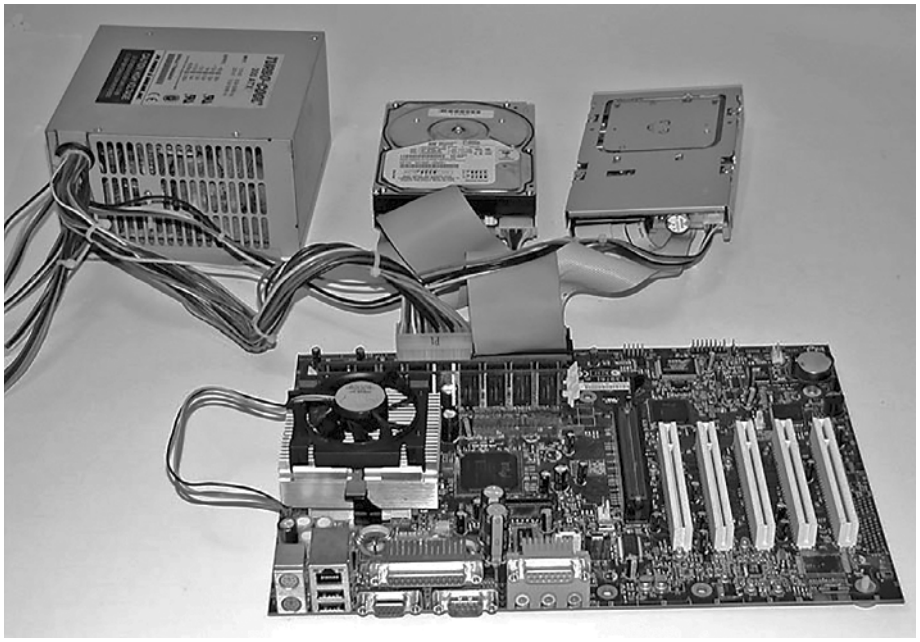
Network Connections

The last primary component that makes up a server is the *network connection*. Without a network connection, the server will not be able to communicate with other servers and the clients. Most servers will include one or more network interface cards or NICs. Since servers are designed to support many network connections, you must have the available bandwidth from the server. Today, the minimum speed of today's server network cards are 1 Gbits/sec or faster.

The Motherboard

Another component that brings these four subsystems together is the *motherboard*. For the processor to communicate with the rest of the system, the processor plugs in or connects to a large circuit board called the motherboard or system board. The motherboard allows the processor to branch out and communicate with all of the other computer components. While everything is made around the processor, the motherboard is considered the nervous system of the PC. While the capabilities of the motherboard have been greatly expanded (most include sound and network connectivity), you can further expand the capabilities of the system by installing expansion cards, sometimes referred to as daughter boards. See Figure 1.2.

FIGURE 1.2 A motherboard connected to power supply and disk drives



On the motherboard, you will find the processors, RAM, motherboard chipset, and the motherboard BIOS. The chipset would represent the nerve clusters that connect your various components including the keyboard, disk drives, and RAM. Depending on the design of the motherboard, one chipset will run faster than another chipset or have more redundant features. Of course, these types of systems usually cost more.

On the motherboard and expansion cards, you will find firmware. *Firmware* is software contained in read-only memory (ROM) chips. Different from RAM, ROM instructions are permanent and can't be changed or erased except with special software. So when you shut off your computer, those instructions remain so that when you turn your computer on again, it knows how to boot the system, test the system, and find a boot device such as your hard drive.

Instructions that control much of the computer's input/output functions, such as communicating with disks, RAM, and the monitor kept in the System ROM chips are known as the ***BIOS*** (basic input/output system). You can think of the BIOS as the instincts of the computer. By having instructions (software) written on the BIOS, the system already knows how to communicate with some basic components such as a keyboard and how to read some basic disks such as IDE drives. It also looks for additional ROM chips, which may be on the motherboard or on expansion cards that you add to the system. These additional ROM chips will have additional instructions to operate additional devices such as adding SCSI or RAID drives.

If you have not realized it by now, the instructions written on the BIOS is software. Different from the normal software you purchase at a store or order off the Internet, it is not written on a disk. Unfortunately like any software, the BIOS may need to have a bug fixed or may need to be expanded to support a new type of hardware that did not exist when the BIOS was written. Sometimes a newer BIOS version can lead to better system performance. To overcome some problems, you would have to check with your system or motherboard manufacturer to see if they have a new version of the BIOS that you can download and apply to your system. The process of updating your system ROM BIOS is called flashing the BIOS.

Unfortunately, flashing the BIOS is a delicate process. If the process gets interrupted partway while you are flashing the BIOS or you install the wrong version, your system may not become accessible, and you may need to replace your motherboard to overcome the problem.

Therefore, if it is your first time in flashing a system, you should do it a couple of times with someone who has done it before. In addition, you should enter your BIOS or CMOS Setup program and write down all of your current settings in case you have to restore your previous settings. Lastly, be sure to thoroughly review the system or motherboard manufacturer to determine what version of the BIOS your system has and which is the correct version to download and install. You will then download the BIOS image and some executable program to flash the BIOS.

To enter the BIOS or CMOS setup program, you would press a key or combination of keys early during the boot process before the operating system loads. Common keys are usually the Del key or F10 key. To find out which key or keys, you should look at the screen during boot up or access the server or motherboard manual.

You want to make sure you don't have any mishaps such as power failures or someone tripping over the power cord while you are doing the upgrade. Remember if the process stops partway through, the system may become unusable.

Power Supplies and Cases

Before moving on, there should be a quick discussion on power supplies and cases. A case provides an enclosure that helps protect the components that are inside of the case. The case with the power supplies and additional fans are usually designed to provide a fair amount of airflow through the system to keep the system cool. Typically if you have items that are designed for performance, they can produce a good amount of heat, and too much heat is always bad for electronic and mechanical devices.

The *power supply* can be thought of as the blood of the computer. The computer runs on electricity. Without it, the computer will be just a box. Since power supplies are half electronic and half mechanical devices, they are considered high failure items when you compare then to pure electronic devices such as memory chips or processors. Mechanical devices tend to wear out over a period of time. Therefore, servers may have redundant power supplies. In addition, to resist power outages or even power fluctuations, the server or server room may be connected to one or more uninterruptable power supplies (UPSs) and/or power generators.

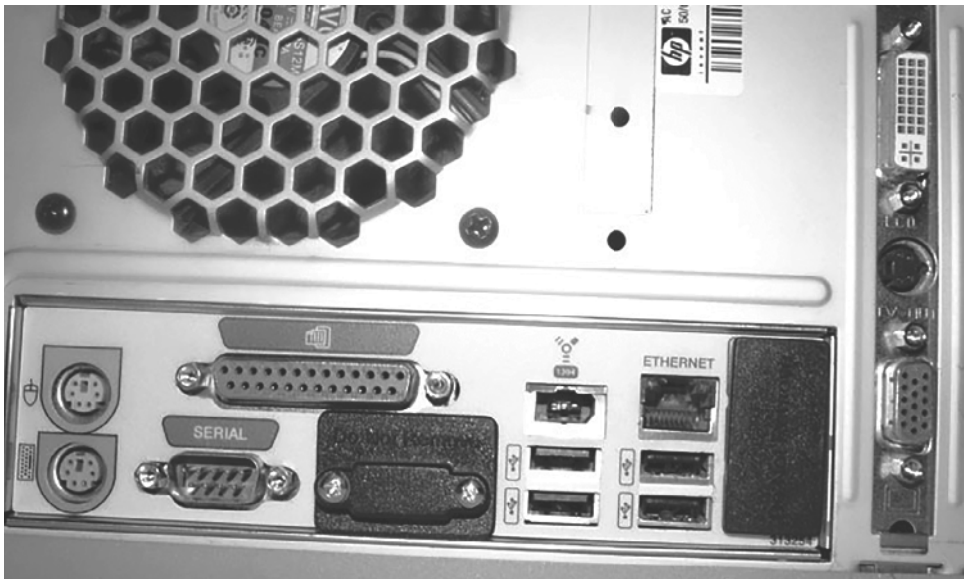
Ports

Servers are still computers. As with any computer, you still need to be able to add external devices to the server. *Ports* are plug sockets that enable an external device such as a printer, keyboard, mouse or external drive. These ports are usually identified by the shape of the plug socket, the number of pins, the number of rows of pins, and the orientation of the pins (male or female). The most popular ports are:

- Parallel port—2-row, 25-pin female D port. Considered a legacy port that used to connect printers.
- Serial port—2-row, 9 pin male D port. While considered a legacy port, is often used to connect to switches and routers to configure them. It can also be used to connect legacy keyboards, mice, and printers.
- VGA port—3-row, 15-pin female D connector. Used to connect a monitor to the computer.
- Universal Serial Bus (USB)—A popular device that can be used to connect keyboards, mice, printers, modems, and external disk drives.
- PS/2Mouse or Keyboard port—6-pin Mouse mini0DIN. Port used to connect a legacy mouse.
- RJ-45 Connector—Used to connect a 10Base-T/100Base-T/1000Base-T network cable.
- DVI-I—A high-quality video interface designed to replace VGA ports.

See Figure 1.3.

FIGURE 1.3 Common ports (PS/2 keyboard and mouse ports, serial port, parallel port, 1394 port, several USB port, Ethernet port, DVI-I port, and VGA port)



Comparing Servers and Workstations

When you purchase any computer, you can usually choose between a mobile computer, a personal computer, a workstation, or a server. Mobile computers are not designed to be stand-alone servers. A personal computer and workstation are designed for a single user. The workstation usually contains components for faster performance over a standard inexpensive personal computer so that they can perform heavy graphics or extensive mathematical calculations. But again, a workstation is designed for only one person.

A server, on the other hand, has two goals. First since servers are designed to support many users, they often have an increased load compared to a single user computer. Second, since many users can rely on accessing a server, the server needs to be reliable. Therefore, servers often contain components that are fault-tolerant and reliable (such as redundant power supplies, redundant hard drives, and redundant network cards). Therefore, systems designated as servers contain additional circuitry to detect problems with the system including the system overheating, a fan has failed, and even if a system has been opened. Of course, the system being opened is more of a security feature than a fault-tolerant component.

While servers typically have high-performance items, they often do not have the newest and fastest items. Instead, the server will have components that perform well but that have been thoroughly tested and are considered reliable.

Comparing Physical Servers and Virtual Servers

Certification Ready?

What can virtual servers do for a corporation? 2.5

So far, the discussion has been focused mostly on physical servers. Over the last few years, virtualization has become more popular. Virtual machines or *virtual servers* technology enable multiple operating systems to run concurrently on a single machine. This allows for a separation of services so that changes on one virtual server will not affect the other virtual servers. In addition, it allows a better utilization of hardware since most hardware is sitting idle most of the time with nothing to do. Therefore, by placing several virtual servers on a powerful server, you can better utilize the hardware while keeping cost to a minimum. In addition, it can easily and quickly create Windows test environments in a safe, self-contained environment.

One leader of virtualization is VMware. To compete against VMware, Microsoft includes Hyper-V, which is a replacement to Microsoft's Virtual Server and Virtual PC.

Locating the Server

After you select and purchase the server and its components, you also need to figure out where it should go. The server room is the work area of the Information Technology (IT) department that contains the servers and most of the communication devices including switches and routers. The room should be secure, with only a handful of people allowed to have access to it. Of course, the room should be secure and locked when not in use and possibly include some type of biometric access that also provides a log of who enters the server room. The server room should also provide clean power and uninterruptable power and proper cooling. It should also contain equipment to perform proper backups.

When you purchase a server, you can choose from numerous sizes and form factors. Larger server rooms with lots of servers will typically contain servers that fit horizontally into a rack. Since these servers are the same width, you can stack 10–20 servers within a rack or server cage. The size of a piece of rack mounted equipment is frequently described as a number in "U". For example, one rack unit is often referred to as "1U", 2 rack units as "2U", and so on. One rack unit is 1.75 inches (44.45 mm) high.

Other servers stand upright and are usually not made to be stacked on top of each other. Of course, servers that stand upright typically take up more room than a stackable server, especially when you have multiple servers.

Selecting the Software

Software is the instructions that the hardware follows and makes the computer do what it does. It also provides us with an interface so that we can use, configure, and manage the computer. With a server, you would first choose the operating system, choose the roles that

the operating system provides, and then install any additional software to make the server do what you want. Fortunately, Microsoft includes a wide range of network programs and servers included with their Windows Server products and also has a wide range of additional products to expand what a server can do.

Windows NT (first released in 1993) is a family of operating systems produced by Microsoft. Since then, Microsoft has built on top of the previous version and has released Windows 2000 Server, Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016.

The newest client operating system released by Microsoft is Windows 10. In the past when a Microsoft client operating system was released, the server version was also released. Windows 7 is paired with Windows Server 2008 R2. Windows 8 is paired with Windows Server 2012, and Windows 8.1 is paired with Windows Server 2012 R2. However, Microsoft decided to release Microsoft Server 2016 almost a year after the release of Windows 10.

Windows Server 2016 builds on previous Windows servers operating systems, expanding existing technology and adding new features to enable IT professionals to increase the reliability and flexibility of their server infrastructures. New virtualization tools, Web resources, and management enhancements help save time, reduce costs, and provide a platform for a dynamic and efficiently managed data center and provide security enhancements. Powerful tools such as Internet Information Services (IIS) version 10, updated Server Manager and Hyper-V platforms, and Windows PowerShell version 5.0 combine to give customers greater control, increased efficiency, and the ability to react to front-line business needs faster than ever before. If you don't know what all of these means, hang on, we will eventually go over all of this.

Similar to previous Windows Servers operating systems, there are multiple editions of Windows 2016.

Windows Server 2016 Essentials Edition This edition corresponds to the Windows Small Business Server from earlier versions of Windows Server, and it is designed for small businesses. It allows up to 25 users and 50 devices. It supports two processor cores and up to 64 gigabytes (GB) of random access memory (RAM). It does not support many of the features of Windows Server 2016, including virtualization.

Windows Server 2016 Standard Edition This edition is designed for physical server environments with little or no virtualization. It provides many of the roles and features available for the Windows Server 2016 operating system, and it supports up to 64 processor sockets and up to 4 terabytes (TB) of RAM. It includes licenses for up to two virtual machines and supports Nano Server installation. Licensing is processor core based.

Windows Server 2016 Datacenter Edition Because it includes unlimited Windows Server–based virtual machine licenses for unlimited Windows Server–based virtual machines that run on the same physical server, this edition is ideal for highly virtualized infrastructures, including private cloud and hybrid cloud environments. It provides all of the roles and features available for the Windows Server 2016 operating system, and it supports up to 64 processor sockets, up to 640 processor cores, and up to 4 TB of RAM. It also includes

new features such as Storage Spaces Direct and Storage Replica, along with new Shielded Virtual Machines and features for software-defined data center scenarios. Licensing is processor core based.

Microsoft Hyper-V Server 2016 This edition acts as a stand-alone virtualization server for virtual machines. It includes all new features around virtualization in Windows Server 2016. Although it supports limited file server features, it does not support other Windows server roles. Although the host operating system has no licensing cost, the virtual machines must be licensed separately. It supports up to 64 processor sockets and up to 4 TB of RAM. It supports domain joining. Different from the Standard and Datacenter editions, Hyper-V Server edition does not have a GUI, but it does have a user interface that displays a menu of configuration tasks.

Windows Storage Server 2016 Workgroup Edition This edition is meant as an entry-level unified storage appliance. It allows 50 users, one processor core, and 32 GB of RAM.

Windows Storage Server 2016 Standard Edition This edition is meant as a unified storage appliance that supports up to 64 sockets but is licensed on a two-socket, incrementing basis. It supports up to 4 TB of RAM, and it includes two virtual machine licenses. It includes Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP) server roles, but does not support others, including Active Directory Domain Services (AD DS), Active Directory Certificate Services (AD CS), and Active Directory Federation Services (AD FS). Licensing is processor core based.

For small data centers that consist of only a few servers, you should consider Windows Server 2016 Standard edition. For large data centers that will use powerful physical servers or blades, you should consider purchasing a Datacenter edition for each physical server or blade. However, both are licensed based on the number of cores within the physical processors.

Since 64-bit processors have become the industry standard for systems ranging from the most scalable servers to desktop PCs, Windows Server 2016 is only available in 64-bit version. Like earlier Windows server operating system, Windows Server 20016 will provide for 32-bit applications with Windows on Windows 64, or WOW64. Both 32-bit and 64-bit applications can run natively on x64 processors, with Windows Server managing the transitions—resulting in excellent performance for both. The end result is a platform that utilizes the existing wealth of 32-bit applications while also providing a smooth migration path to 64-bit computing.

Introducing Server Roles in Windows Server 2016

A server is designed to provide services. Therefore, Windows Server 2016 has organized the most common services into server roles, whereas a server role describes the function of the server. When you define a server role in Windows Server 2016 (see Table 1.2), you are installing and configure a set of software programs that allow a computer to perform a specific function for multiple users or other computers within a network.

TABLE 1.2 Available roles in Windows Server 2016

Role Name	Description
Active Directory Certificate Services	Provides service for creating and managing public key certificates used in software security systems that employing public key technologies to prove the identity of person, device, or service, which can be used by secure mail, secure wireless networks, virtual private networks (VPNs), Internet Protocol Security (IPSec), Encrypting File System (EFS), smart card logon, and others. For ease of use, the digital certificates interface with Microsoft's Active Directory.
Active Directory Domain Services	To transform a server into a domain controller to provide a directory service via Microsoft's Active Directory (AD), which stores information about users, computers, and other devices on the network. Active Directory helps administrators securely manage this information and facilitates resource sharing and collaboration between users. Active Directory is required for directory-enabled applications such as Microsoft Exchange Server (email server) and to apply other Windows Server technologies such as Group Policy.
Active Directory Federation Services	Active Directory Federation Services provides Web single sign-on (SSO) technologies to authenticate a user to multiple Web applications using a single user account.
Active Directory Lightweight Directory Services (ADLDS)	For applications that require a director for store application data as a data store without installing Active Directory domain services. Since this run as a non-operating-system service allows multiple instances of AD LDS to run concurrently on a single server, and each instance can be configured independently for servicing multiple applications.
Active Directory Rights Management Services (AD RMS)	Technology that works with Active Directory RMS enabled applications to help safeguard digital information from unauthorized use by specifying who can use the information and what they can do with it (open, modify, print, forward, and/or take other actions with the information).
Dynamic Host Configuration Protocol (DHCP) Server	Allows servers to assign, or lease, IP addresses to computers and other devices that are enabled as DHCP clients.
Domain Name System (DNS) Server	Provides naming service that associates names with numeric Internet addresses. This makes it possible for users to refer to network computers by using easy-to-remember names instead of a long series of numbers. Windows DNS services can be integrated with Dynamic Host Configuration Protocol (DHCP) services on Windows, eliminating the need to add DNS records as computers are added to the network.

TABLE 1.2 Available roles in Windows Server 2016 *(continued)*

Role Name	Description
Fax Server	Sends and receives faxes, and allows you to manage fax resources such as jobs, settings, reports, and fax devices on this computer or on the network.
File and Storage Services	Provides technologies for storage management, file replication, distributed namespace management, fast file searching, and streamlined client access to files.
Hyper-V	Provides the services that you can use to create and manage virtual machines (virtualized computer system that operates in an isolated execution environment which allows you to run multiple operating systems simultaneously) and their resources.
Network Policy and Access Services	Delivers a variety of methods (including using VPN servers, dial-up servers, routers, and 802.11 protected wireless access points) to provide users with local and remote network connectivity, to connect network segments, and to allow network administrators to centrally manage network access and client health policies.
Print and Document Services	Enables users to print to and manage centralized printers that are connected directly or indirectly to print servers.
Remote Access	Provides seamless connectivity through DirectAccess, Virtual Private Network (VPN), and Web Application Proxy.
Remote Desktop Services	Allows users to connect to a terminal server to remotely run programs, use network resources, and access the Windows desktop on that server.
Web Server (IIS)	Enables sharing of information on the Internet, an intranet, or an extranet via a unified Web platform that integrates Internet Information Server (IIS) 10 to provides web pages, File Transfer Protocol (FTP) services or newsgroups, ASP.NET, Windows Communication Foundation, and Windows SharePoint Services.
Windows Deployment Services	Used to install and configure Microsoft Windows operating systems remotely on computers with Pre-boot Execution Environment (PXE) boot ROMs.
Windows Server Update service	Allows network administrators to specify the Microsoft updates that should be installed and to create separate groups of computers for different sets of updates.

Introducing Server Features in Windows Server 2016

Windows Server 2016 Features are software programs that are not directly part of a role. Instead, they are often used to augment the functionality of one or more role or enhance the functionality of the entire server. The features that are included in Windows Server 2016 are shown in Table 1.3.

TABLE 1.3 Features available in Windows Server 2016

Feature Name	Description
.NET Framework 3.5 Features	Combines .NET Framework 2.0 Application Programming Interface (APIs) with new technologies to build applications with appealing user interfaces and provide various forms of security for those services.
NET Framework 4.6 Features	Provides a consistent programming model and APIs that are required for some programs to function.
Background Intelligent Transfer Service (BITS)	Short for Background Intelligence Service, allows a client computer to transfer files in the foreground or background asynchronously so that the responsiveness of other network applications are preserved.
BitLocker Drive Encryption	Helps protect data on disks by encrypting the entire volume.
Containers	Provides services and tools to create and manage Windows Server Containers and their resources. Containers are isolated, resource-controlled, and portable operating environments that can be moved from server to server as needed.
Failover Clustering	Allows multiple servers to work together to provide high availability of services and applications. If one server fails, a second server is available to take over its work.
Group Policy Management	A Microsoft Management Console snap-in that allows easy management of Active Directory Group Policies to secure or standardize a network environment.
LPR Port Monitor	Enables the computer to print to printers that are shared using a Line Printer Daemon (LPD) service. LPD service is commonly used by UNIX-based computers and printer-sharing devices.
Message Queuing	Provides guaranteed message delivery, efficient routing, security, and priority-based messaging between applications.

TABLE 1.3 Features available in Windows Server 2016 *(continued)*

Feature Name	Description
Multipath I/O	Along with the Microsoft Device Specific Module (DSM) or a third-party DSM, provides support for using multiple data paths to a storage device on Windows.
Network Load Balancing	Distributes traffic across several servers, using the TCP/IP networking protocol. NLP is particularly useful for ensuring that stateless application such as web servers running IIS are scalable by adding additional servers as the load increases.
Peer Name Resolution Protocol	Allows applications to register and resolve names on your computer so that other computers communicate with these applications.
Quality Windows Audio Video Experience	A networking platform for audio and video streaming applications on IP home networks.
Remote Assistance	Enables you or a support person to offer assistance to users with computer issues or questions.
Remote Differential Compression	Computes and transfers the differences between two objects over a network using minimal bandwidth.
Remote Server Administration Tools	Includes a MMC snap-in and a command-line tool to remotely manage roles and features.
RPC over HTTP Proxy	Relays RPC traffic from client applications over HTTP to the server as an alternative to clients accessing the server over a VPN connection.
Simple TCP/IP Services	Supports Character Generator, Daytime, Discard, Echo and Quote of the Day TCP/IP services.
SMTP Server	Supports the transfer of email messages between email systems. SMTP is short for Simple Mail Transfer Protocol.
SNMP Services	Includes the SNMP service and SNMP WMI provider. SNMP is short for Simple Network Management Protocol. SNMP is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention.
Telnet Client	Uses the Telnet protocol to connect to a remote Telnet server and run applications on that server.
TFTP Client	Allows to read files or write files to a remote Trivial FTP (TFTP) server.

Feature Name	Description
Windows Defender	Helps protect your machine against malware.
Windows Internal Database	A relational data store that can be used only by Windows roles and features.
Windows PowerShell	A command-line shell and scripting language.
Windows Process Activation Service	Generalizes the IIS process model, removing the dependency on HTTP.
Windows Search Service	Allows you to back up and recover your operating system, applications, and data.
Windows Server Backup	Allows you to back up and recover your operating system, applications, and data.
Windows Server Migration Tools	Includes Windows PowerShell cmdlets that facilitate migration of server roles, operating system settings, files, and shares from other servers running Windows Server 2016 or earlier operating systems to Windows Server 2016.
WINS Server	WINS, short for Windows Internet Naming Service, provides a distributed database for registering and querying dynamic mappings of NetBIOS names for computers and groups used on your network.
Wireless LAN Service	Configure and starts the WLAN AutoConfig service, regardless of whether the computer has any wireless adapters.
XPS Viewer	Used to read, set permissions for, and digitally sign XPS documents.

Comparing Full Version Server Core and Nano Server

Starting with Windows Server 2008, you can install Windows in one of two modes: Windows Server 2016 with Desktop Experience or Windows Server 2016 Server Core, both of which are provided on the installation DVD. When you think of the Full Version, the full version is the normal version that you would expect of Windows with a fully functionally GUI interface.

Server Core installation provides a minimal environment with no File Explorer or Desktop shell for running specific server roles and no Start button. See Figure 1.4. Just about the only thing that you can see is a command prompt window to type in commands. Since the system has a minimal environment, the system runs more efficiently, focusing on what it needs to provide instead of processing fancy graphics for you to manage the system.

It also reduces the attack surface for those server roles because not all of the components that Windows has will be running that could be exploited by a hacker.

FIGURE 1.4 A server running Server Core

A Server Core machine can be configured for the following roles:

- Active Directory Lightweight Directory Services (ADLDS)
- DHCP Server
- DNS Server
- Domain controller/Active Directory Domain Services
- File Services (including DFSR and NFS)
- IIS 10
- web server (but does not include ASPNET, .Net Framework, IIS Management Console, IIS Legacy Snap-In and IIS FTP Management)
- Print Services
- Streaming Media Services
- Terminal Services including Easy Print, TS Remote Programs, and TS Gateway
- Windows Server Virtualization

A Server Core machine can be configured for the following features:

- Backup
- Bitlocker Drive Encryption
- Failover Clustering

- Multipath IO
- Network Load Balancing
- Removable Storage
- Simple Network Management Protocol (SNMP)
- Subsystem for UNIX-based applications
- Telnet client
- Windows Internet Name Service (WINS)

Nano Server is a new installation option that was introduced with Windows Server 2016. Nano Server is administered remotely and optimized for hosting in private clouds and data centers. The Nano Server runs from a VHD, either from within Hyper-V or you can boot directly from the VHD at startup. It has a smaller hardware footprint than Windows Server Core, it has no local sign-in capability, and it supports only 64-bit applications, tools, and agents.

Installing Windows Server 2016

Before you can start using, managing, or configuring an operating system, you will need to first install the operating system.

Certification Ready?

Can you list all of the methods to install Windows? 1.3

Although the hardware requirements to support Windows Server 2016 will depend on the servers that the server is hosting, the load on the server, and how responsive you want your server to be. However, Table 1.4 show the Windows Server 2016 on a physical machine:

- Processor: A 64-bit processor running 1.4 GHz
- RAM: 512 MB
- Free hard drive space: 32 GB

TABLE 1.4 System requirements for Windows Server 2016

Component	Requirement
Processor	Minimum: 1.4 GHz (x64 processor) Maximum number of physical sockets: 1 (Foundation) 4 (Web and Standard), 8 (Enterprise), 64 (Datacenter)
Memory	Minimum: 512 MB RAM Maximum: 24 TB
Disk Space Requirements	Minimum: 32 GB or greater
Display	Super VGA (1024 × 768) or higher resolution monitor
Other	DVD Drive, Keyboard and Microsoft Mouse (or compatible pointing device), network adapter, and Internet access

If you want to run the Desktop Experience, you should increase the requirements even more. Although Microsoft states that you would need an additional 4 GB of free disk space, you should consider two core processors running at 1.4 GHz, 2 GB of memory, and 50 GB free as the minimum if you desire fair performance. Then based on the server roles and applications the server will run, you will increase the requirements even further. You should also add additional disk space if you are to perform a network installation or for computers with more than 16 GB of RAM.

In addition, storage and network adapters must be PCI Express compliant. Ethernet adapters should be at least gigabit throughput. The graphics device and monitor should be capable of Super VGA (1024 × 768). If you need to install Windows Server 2016, you will also need a DVD drive.

The requirements for Nano Server will depend on the features and roles installed. The smallest Nano Server VHD will be approximately 440 MB. But after installing IIS or commonly used drivers, the VHD with IIS will be just over 500 MB.

Remember, the amount of RAM and disk space is not the place to skimp. At the time this book was written, the requirements listed above were the current requirements. Make sure to check the Microsoft website for the most current information.

Nano Server Installation

Windows Server 2016 introduced a new type of server installation called Nano Server. Nano Server allows an administrator to remotely administer the server operating system. It was largely designed and created for private clouds and datacenters.

Nano Server is similar to Microsoft Windows Server Core, but the Nano Server operating system uses considerably less hard drive space, has no local logon or GUI capabilities, and only supports 64-bit applications and tools.

Installing Windows Server 2016 Nano Server

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

When Microsoft created Nano Server, they had some very specific thoughts of how this version could be used, such as using Nano Server as a DNS server, an IIS server, an application server for cloud-based applications, or even a storage unit for file servers.

However, there are a few disadvantages of Nano Servers. A Nano Server cannot act as Domain Controller, Group Policy objects (GPOs) are not supported, and Nano Servers cannot be configured to use System Center Configuration Manager, System Center Data Protection Manager, NIC Teaming, or as proxy servers. Nano Servers also uses a version of Windows PowerShell that has many differences as a server using regular PowerShell.

At the time this book was written, Nano Server supports only the Current Branch for Business (CBB) licensing model.

When it comes to installing Nano Servers, there are some 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 an administrator wants to add server roles and features to the image.

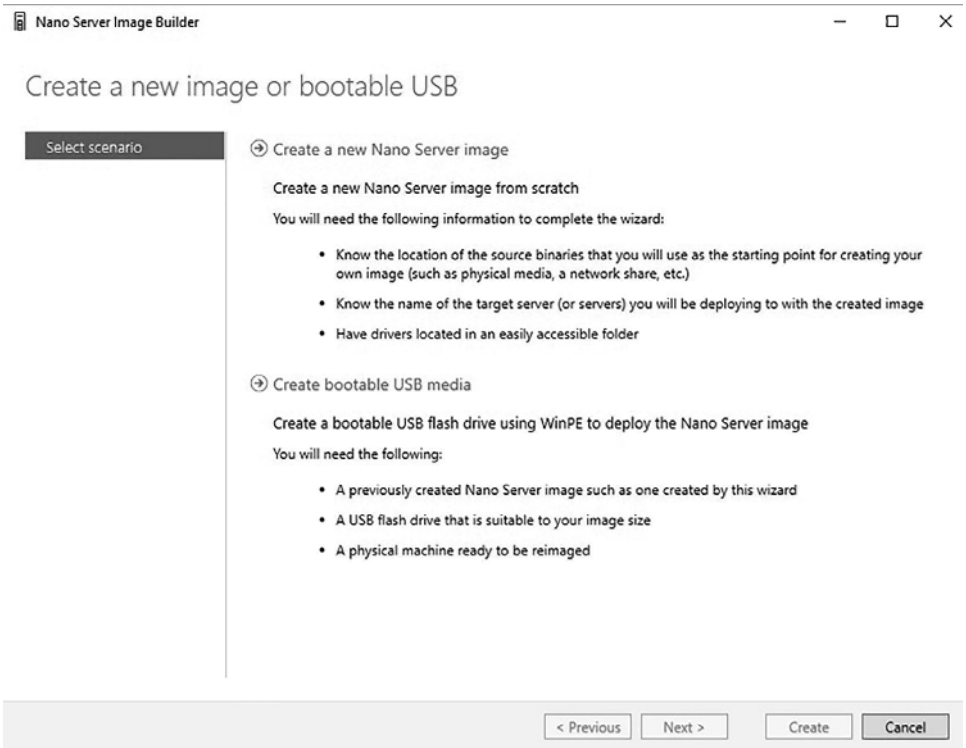
However, if an administrator wants a simple way to create a Nano Server virtual hard drive (VHD), they can just download the Nano Server Image Builder. This software tool helps administrators easily create a Nano Server VHD that can then be used to boot a server with or use in Microsoft's Hyper-V server.

Creating a Nano Server VHD

1. Download the Nano Server Image Builder from Microsoft's website at `https://www.microsoft.com/en-us/download/details.aspx?id=54065` by clicking the Download button.
2. A file named `NanoServerImageBuilder.msi` will be created. Double-click 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 introduction screen.
4. At the Licensing screen, click the I Accept The Terms check box and then click Next.
5. At the Destination Folder screen, choose where to install the Nano Server Image Builder files. Click Next.
6. At the Ready To Install screen, click the Install button. If a User Account Control box appears, click the Yes button.

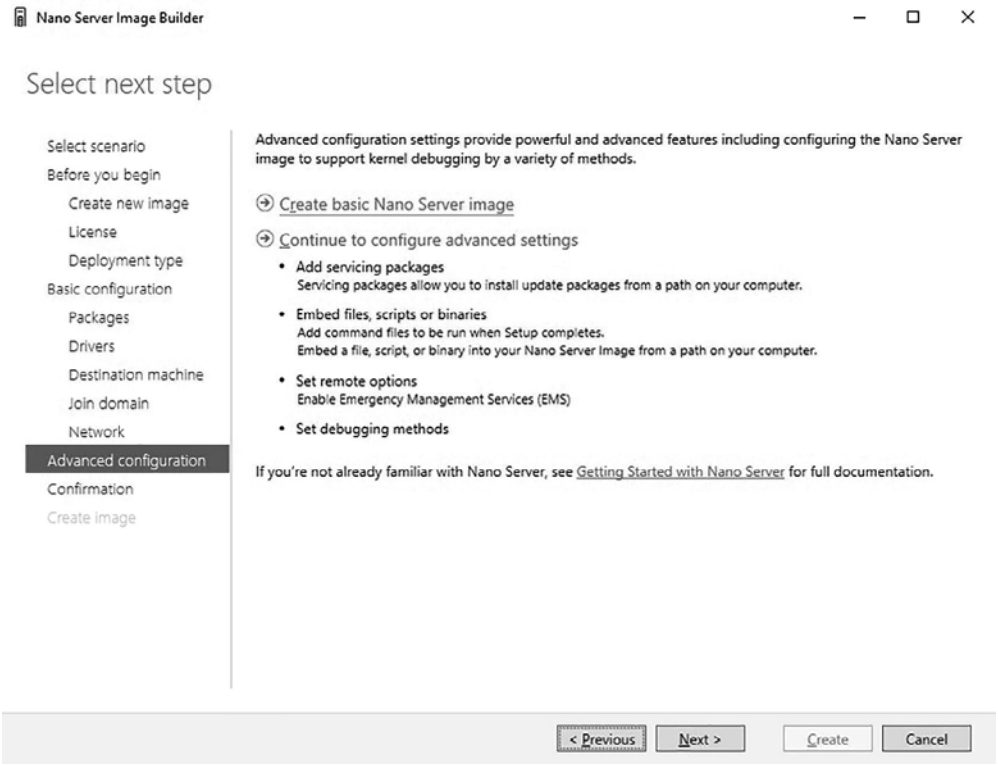
7. Once the Installation is complete, click the Finish button.
8. Open Windows Explorer and navigate to the destination folder chosen from step 5. Double-click the `NanoServerImageBuilder.exe` file. If a UAC dialog box appears, click Yes.
9. In order for the Image Builder to work, an administrator must also download the Windows ADK kit from Microsoft. This can be found at `https://developer.microsoft.com/en-us/windows/hardware/windows-assessment-deployment-kit`. Click the version you want to download.
10. The administrator will be asked if they want to run or save the file. This option is up to the administrator. Some will save the file to the same destination folder as the Nano Server Image Builder. Once downloaded, double-click the `adksetup.exe` file (if saved). If a dialog box appears, click Run.
11. Specify the destination of where to place the Windows ADK files to install and click Next.
12. At the Windows Kit Privacy screen, you can choose either option. By choosing Yes, the administrator will be asked to participate in Microsoft's feedback program. This is up to the administrator; 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 the `NanoServerImageBuilder.exe` file. When the UAC screen appears, click Yes.
17. Now the administrator has the ability to create a Nano Server image or a bootable USB. For this exercise, you are going to create an image. So click the top choice, Create A New Nano Server Image. See Figure 1.5.
18. At the Before You Begin screen, click Next.
19. At the Select Installation Media screen, point the folder for the Windows Server 2016 installation files where the NanoServer Folder resides. Click Next.
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, choose how to create the virtual machine image. Assign a name and set the size and specify a directory to copy the image creation log files. Click Next.
22. At the Basic Installation screen, click Next.
23. At the Select Optional Packages screen, choose any other options to install such as DNS, IIS, etc. Then click Next.

FIGURE 1.5 Nano Server image choice



24. At the Drivers screen, add any drivers needed for the installation and click Next.
25. Next the Destination screen will appear. Enter the name of the computer and the administrator's password. Make sure the Time Zone is correct and click Next.
26. At this time, choose whether to join a domain or not. For this exercise, you are not going to join a domain. Just click Next.
27. Leave the default network settings and click Next.
28. At the Advanced Configuration Screen, choose the top option, Create a Basic Nano Server Image. See Figure 1.6.
29. Once the link is clicked, will see a Confirmation screen. Click the Create button.
30. Once the image is complete, click the Close button.
31. Open Windows Explorer and go to the folder where the VHD was created. Ensure that the VHD file has been created. The administrator can now run this VHD in Microsoft Hyper-V.

FIGURE 1.6 Advanced Configuration screen



Interactive Installs

Advantages to using unattended installations as a method for automating Windows Server 2016 include:

- Can be configured to provide an automated query response while still allowing users to selectively provide specified input during the installation.
- Can be expanded to include installation instructions for applications, additional language support, service packs, and device drivers.
- Can be used to install clean copies of Windows Server 2016 or upgrade an existing operating system to Windows Server 2016.
- Saves time and money since users do not have to interactively respond to each installation query.
- Windows Server 2016 physical media does not need to be distributed to all the computers on which it will be installed.

Disadvantages of using unattended installation as a method for automating Windows Server 2016 include:

- An administrator does not physically walk through the installation of Windows Server 2016 on the client machine. If there are any problems, it will be unknown until the end user has issues.
- Require more initial setup than a standard installation of Windows Server 2016.
- Someone must have access to each client computer and must initiate the unattended installation process on the client side.

VHD/VHDX Installation Source

In addition to virtual networks, administrators need to administer virtual hard disks that are attached to the virtual machines. A virtual hard disk in Hyper-V, apart from a pass-through disk, is a VHD or VHDX file that simulates a hard drive on the virtual machine.

Windows Server 2016 Hyper-V has a feature called Shared Virtual Hard Disk. This allows an administrator to cluster virtual machines by using shared virtual hard disk (VHDX) files. Shared virtual hard disks allow an administrator to build a high availability infrastructure, which is key if setting up either a private cloud deployment or a cloud-hosted environment for managing large workloads. Shared virtual hard disks allow two or more virtual machines to access the same virtual hard disk (VHDX) file.

Native Boot allows an administrator to create a virtual hard disk (VHDX), install Windows to it, and then boot it up, either on the computer side-by-side with the existing installation or as a new device. A native-boot VHDX can be used as the running operating system on designated hardware without any other parent operating system. This differs from a scenario where a VHDX is connected to a virtual machine on a computer that has a parent operating system.

Windows disk-management tools such as the DiskPart tool and the Disk Management Microsoft Management Console (Diskmgmt.msc) can be used to create a VHDX file. A supported Windows image (.wim) file can be applied to a VHD, and the VHDX can be copied to multiple systems. The Windows boot manager can be configured to boot directly into the VHD.

The VHDX can also be connected to a virtual machine for use with the Hyper-V Role in Windows Server.

VHDXs can be applied to computers or devices that have no other installations of Windows, without a virtual machine or hypervisor. A hypervisor is a layer of software under the operating system that runs virtual computers. This allows for more flexibility in workload distribution because a single set of tools can be used to manage the images for virtual machines and designated hardware.

An administrator can also deploy the VHDX to a computer that already has Windows installed on it and use a boot menu to select between the existing version of Windows or the version on the VHD.

Prerequisites for VHD/VHDX are:

- An administrator machine with the Windows Assessment and Deployment Kit (Windows ADK) tools installed.
- A generalized Windows image (.WIM file).
- A bootable Windows PE drive.
- A destination computer or device on which to install the VHDX. This device requires 30 GB or more of free disk space. Can install the VHDX to a device already running other operating system installations, or as the only operating system on a device.

Understanding Virtual Memory and Paging File

If a computer lacking RAM and needs to run a program or perform an operation, Windows can use virtual memory to compensate. Virtual memory combines a computer's RAM with temporary space on the hard disk. When RAM runs low, virtual memory moves data from RAM to space called a paging file. By default, the paging file is stored as `C:\pagefile.sys`.

Unfortunately, if something needs to be accessed from the virtual memory on disk, it is significantly slower than accessing it directly from RAM.

Managing the Paging File

To manage the paging file in Windows Server 2016, perform the following:

1. Right-click Computer and select Properties.
2. In the left pane, click Advanced System Settings. If prompted for an administrator password or confirmation, type the password or provide confirmation.
3. On the Advanced tab, under Performance, click Settings.
4. Click the Advanced tab, and then, under virtual memory, click Change.
5. Clear the "Automatically manage paging file size for all drives" check box.
6. Under Drive {Volume Label}, click the drive that contains the paging file to change.
7. Click the Custom Size radio button, type a new size in megabytes in the Initial Size (MB) or Maximum Size (MB) box, click Set, and then click OK.

Increasing the size of the paging files usually doesn't require a restart for the changes to take effect; however, if an administrator decreases the size, then the computer will need to be restarted. It is recommended that an administrator doesn't disable or delete the paging file.

The default paging file size is equal to 1.5 times the total RAM. However, this default configuration may not be optimal in all situations, such as with servers that contain large databases. Therefore, unless an administrator has an application that uses a larger paging file, the administrator should consider adding more RAM to the system. In addition, if there are multiple physical drives, the administrator can move the paging file from the boot volume to another volume.

Performing Clean Installations

A *clean installation* is installing the software from scratch on a new drive or on a newly reformatted drive. Many people find that doing a clean install of an operating system is the best way to go because you are starting fresh. The disadvantage is that the system and all of its software needs to be reinstalled, patched, and configured and data copied over, something that may take hours or even days.

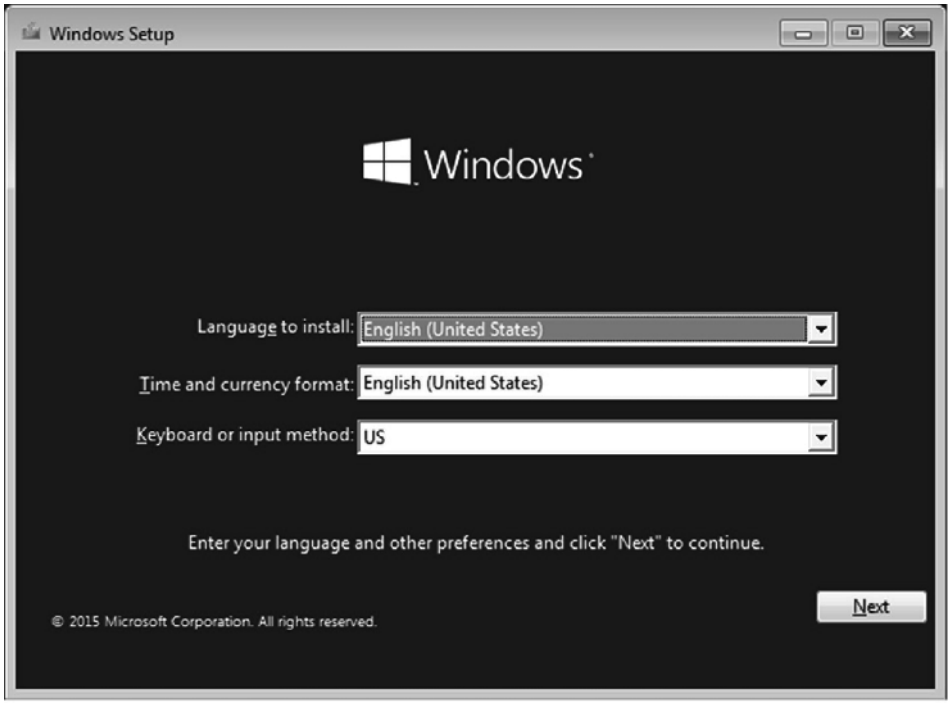
To boot from a DVD drive, you insert the DVD into your DVD/Blu-ray drive and turn on the computer. If the system does not boot from the DVD, you might need to configure the BIOS Setup program to boot from the DVD/Blu-ray drive, and you might need to configure the boot order so that the DVD/Blu-ray drive booting will occur before any other boot drives.

Install Windows Server 2016 with Desktop Experience

To install Windows Server 2016 with Desktop Experience, perform the following steps.

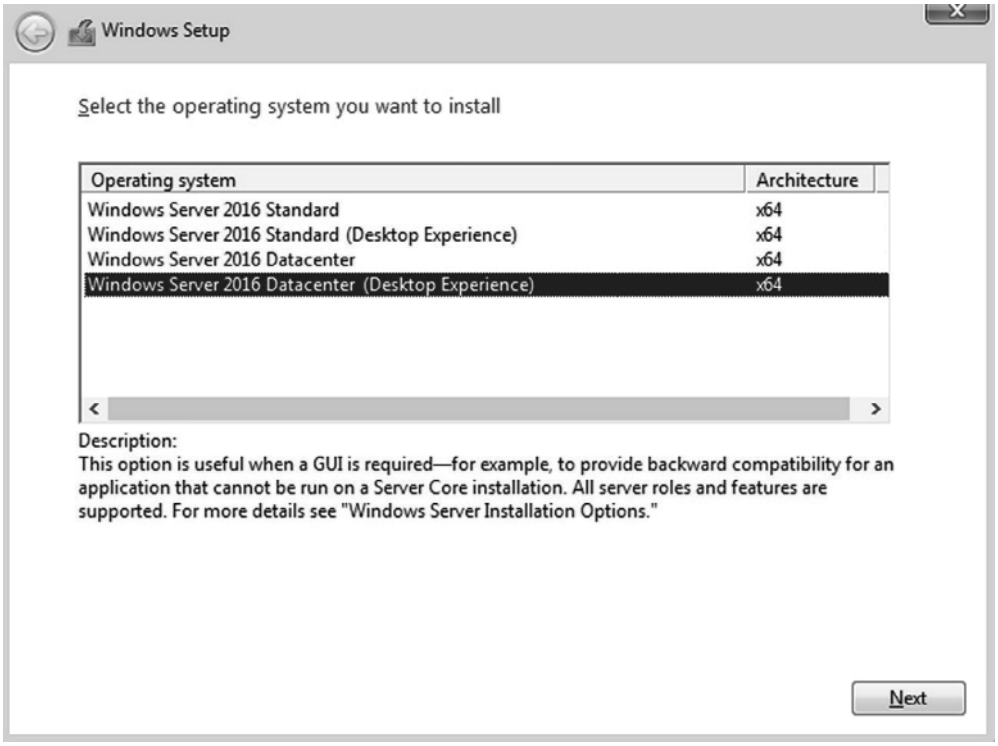
1. Insert the Windows Server 2016 disc into the DVD drive and turn on the computer. Press any key to boot from the DVD (if necessary).
2. The computer switches to the Windows graphical interface and the Windows Setup page appears, as shown in Figure 1.7. Using the drop-down lists provided, select the appropriate language to install, the time and currency format, and the keyboard or input method. Then, click Next.

FIGURE 1.7 The Windows Setup page



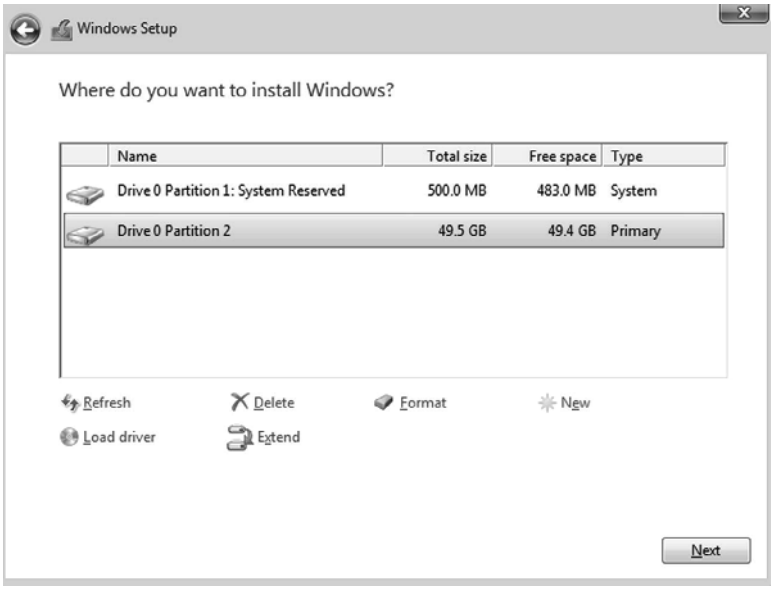
3. On the Windows Server 2016 Install Now page, click Install now.
4. When the Activate Windows page appears, in the text box, type the Windows Server 2016 activation key and then click Next.
5. On the Select the Operating System to Install page (as shown in Figure 1.8), select Windows Server 2016 Datacenter (Desktop Experience). Click Next.

FIGURE 1.8 Selecting which operating system to install



6. On the License Terms page, select the "I accept the license terms" option and then click Next.
7. Click the Custom: Install Windows Only (Advanced) option.
8. The Where Do You Want to Install Windows? page appears, as shown in Figure 1.9. From the list provided, select the partition on which you want to install Windows Server 2016, or select an area of unallocated disk space where the Setup program can create a new partition. Then click Next.
9. After several minutes, during which the Setup program installs Windows Server 2016, the computer reboots. When the Customize Settings page appears, in the Password and Reenter Password text boxes, type **Pa$$w0rd**. Click Finish.

FIGURE 1.9 The Where Do You Want to Install Windows? page



The Where Do You Want to Install Windows? page enables you to create, manage, and delete the partitions on your disks. It also allows you to load specialized storage drivers.

Clicking the Drive options (advanced) button on the page causes four additional buttons to appear. These buttons have the following functions:

- Delete removes an existing partition from a disk, permanently erasing all its data. You might want to delete partitions to consolidate unallocated disk space, enabling you to create a new, larger partition.
- Extend enables you to make an existing partition larger, as long as unallocated space is available immediately following the selected partition on the disk.
- Format enables you to format an existing partition on a disk, thereby erasing all its data. You do not need to format any new partitions you create for the install, but you might want to format an existing partition to eliminate unwanted files before installing Windows Server 2016 on it.
- New creates a new partition of a user-specified size in the selected area of unallocated space.

In some cases, it might be necessary to install a driver supplied by a hardware manufacturer before the disks (for example, RAID drivers) in the computer appear in the Setup program. During the Windows Server 2016 installation procedure, the Setup program enables you to select the partition or area of unallocated disk space where you want to install the operating system. The Where Do You Want to Install Windows? page lists the partitions on all the computer's disk drives that the Setup program can detect with its default drivers. In

most cases, all the computer's drives should appear in the list; if they do not, it is probably because Windows does not include a driver for the computer's drive controller.

If the computer's hard drives are connected to a third-party controller, rather than the one integrated into most motherboards, the list of partitions might appear empty, and you might need to supply a driver for the Setup program to see the drives. Check the controller manufacturer's website for a driver supporting Windows Server 2016, or another recent version of Windows Server.

To load the disk driver, on the Where Do You Want to Install Windows? page, click the Load driver button. You will then be prompted to insert the storage medium that contains the drivers (CD, DVD, or USB flash drive). You can then browse to the location of the driver and click OK. Then, select the driver and click Next. You would then continue with the rest of the Windows Server 2016 installation.

Performing an Upgrade

If you want to upgrade or move an older server operating system to Windows Server 2016, you can use existing hardware and upgrade to Windows Server 2016 or you can install Windows Server 2016 on new hardware and migrate the roles, features, settings, and data from the older servers to the new server. You can upgrade from Windows Server 2008 R2 with Service Pack 1, Windows Server 2012, or Windows Server 2012 R2 to Windows Server 2016.

If you have a 64-bit computer running Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2, you can upgrade it to Windows Server 2016 based on the following paths:

- Windows Server 2008 R2 Standard (with Service Pack 1) or Windows Server 2008 R2 Enterprise (with Service Pack 1) to Windows Server 2016 Standard or Windows Server 2016 Datacenter
- Windows Server 2008 R2 Datacenter (with Service Pack 1) to Windows Server 2016 Datacenter
- Windows Web Server 2008 R2 (with Service Pack 1) to Windows Server 2016 Standard
- Windows Server 2008 R2 Datacenter (with Service Pack 1) to Windows Server 2016 Datacenter
- Windows Server 2008 R2 Enterprise (with Service Pack 1) to Windows Server 2016 Standard or Windows Server 2016 Datacenter
- Windows Server 2008 R2 Standard (with Service Pack 1) to Windows Server 2016 Standard or Windows Server 2016 Datacenter
- Windows Web Server 2008 R2 (with Service Pack 1) to Windows Server 2016 Standard
- Windows Server 2012 Datacenter or Windows Server 2012 R2 Datacenter to Windows Server 2016 Datacenter
- Windows Server 2012 Standard or Windows Server 2012 R2 Standard to Windows Server 2016 Standard or Windows Server 2016 Datacenter

If you want to run Windows Server 2016 on a new machine or you are not using one of the previous upgrade paths, you must perform a migration.

You cannot perform an upgrade that includes one language to another with a different language.

When you want to upgrade to Windows Server 2016, you should follow these guidelines:

- Verify that the current server will support Windows Server 2016. In addition, make sure you have the appropriate drivers before installation.
- Update your antivirus program, run it, and then disable it. After you install Windows, remember to re-enable the antivirus program, or install new antivirus software that works with Windows Server 2016.
- Back up your files. You can back up files to an external hard disk, a DVD or CD, or a network folder.
- Connect to the Internet. Make sure your Internet connection is working so that you can get the latest installation updates. These updates include security updates and hardware driver updates that can help with installation. If you don't have an Internet connection, you can still upgrade or install Windows.

If your system is a production system, verify and/or test all applications to make sure they are compatible with Windows Server 2016.

Upgrading to Windows Server 2016

To upgrade a server to Windows Server 2016, perform the following steps.

1. Log on to a server running Windows Server 2012 R2 as **adatum\administrator** with the password of **Pa$$w0rd**.
2. Insert the Windows Server 2016 installation disc into the DVD drive. Then open the DVD drive, and double-click the Setup program. The Windows Setup window opens.
3. On the Get Important Updates page, the Download And Install Updates (Recommended) option is already selected. Click Next.
4. On the Product Key page, in the Enter Product key text box, type the product key and then click Next.
5. Select the desired Windows version, Windows Server 2016 or Windows Server 2016 (Desktop Experience). Click Next.
6. On the License Terms page, click the Accept button.
7. On the Choose What to Keep page, you can select Keep Personal Files and Apps, or Nothing. The Keep Personal Files And Apps option will be grayed out if you are installing an edition of Windows that is different from the one you're currently using. Click Next. If you are prompted to indicate whether you want to continue using this selection, click the Yes button.

8. On the Ready To Install page, click the Install button.

   After several minutes, during which the Setup program upgrades Windows Server 2012 or Windows Server 2012 R2 to Windows Server 2016 and restarts the computer several times, the system finalizes the installation and the Windows sign-on screen appears.

In the past, Microsoft has provided tools to check your system to see if it is ready for the operating system. Today, you would use the Microsoft Assessment and Planning (MAP) Toolkit, which is designed to give you essential infrastructure knowledge for planning your migration to Windows Server 2016. The MAP Toolkit takes inventory of your current server environment, determines hardware and device compatibility and readiness, and then generates actionable reports of recommended upgrades for migration. Power savings benefits are calculated with MAP's Power Savings Assessment tool, enabling you to quickly determine potential savings with Windows Server 2016 prior to deployment.

Download

The Microsoft Assessment and Planning (MAP) Toolkit is located at: `https://www.microsoft.com/en-us/download/details.aspx?id=7826`.

Migrating Roles and Features to Windows Server 2016

Once an administrator decides which roles and features are going to be installed, then they can either 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 ease the process of migrating server roles, features, operating system settings, and data. Administrators can migrate this data from an existing server that is 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 the Windows Server Migration Tools to migrate roles, role services, and features can streamline the deployment of new servers. An administrator 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 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.

To use the 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.

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 using Windows PowerShell, 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
```

Disk Cloning and System Preparation Tool

One way to install Windows Server 2016 is to use *disk cloning* software such as Norton Ghost to create an image file, which is a sector-by-sector copy stored in a large file. To use the disk cloning software, you use the installation disk to install Windows onto a master computer (also called reference computer), update and patch the computer, customize Windows, and install any additional software. You then use the cloning software to copy the contents of a hard drive to a file. You use the disk cloning software to copy the contents of the image to a target computer.

If you create a cloned copy of Windows and apply the cloned copy to multiple computers, each copy of Windows cloned to a target computer using the same image has the same parameters, including the same computer name and security identifier (SID). Unfortunately, for these computers to operate properly without conflict on a network, these parameters have to be unique.

To overcome this problem, you run the System Preparation Tool (Sysprep), which removes the security identifiers and all other user-specific or computer-specific information

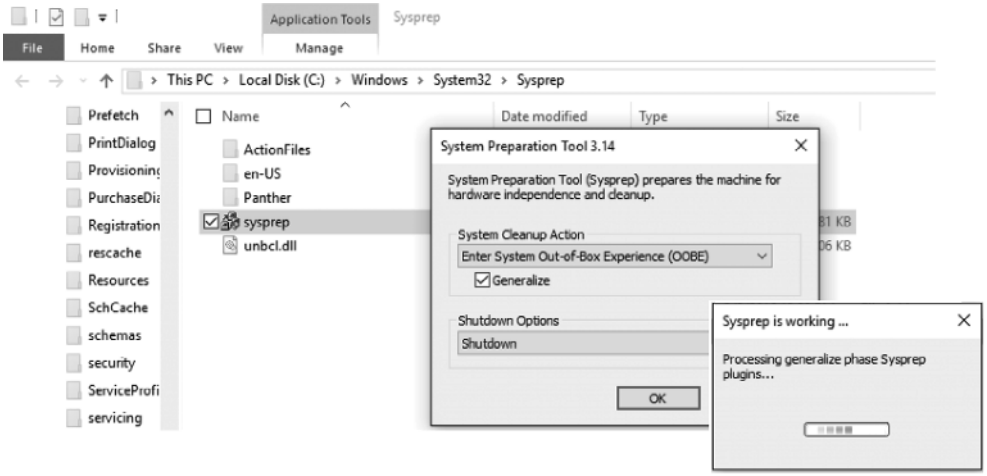
from the computer before you run the disk cloning software to make the cloned disk image. When you copy the cloned image to the disk image, a small wizard runs that enables you to specify the computer name and other computer-specific information. The SID and other information is re-created automatically. The Sysprep utility is located in the `c:\Windows\System32\sysprep` or the `c:\Windows\SysWOW64\sysprep` folder.

Most of the time, you will execute the following command:

```
Sysprep.exe /oobe /generalize
```

See Figure 1.10.

FIGURE 1.10 Running the `Sysprep.exe` command



The `/generalize` will prepare the Windows installation to be imaged. If this option is specified, all unique system information is removed from the Windows installation. The security ID (SID) resets, any system restore points are cleared, and event logs are deleted. The next time the computer starts, a specialize configuration pass runs. A new security ID (SID) is created, and the clock for Windows activation resets, if the clock has not already been reset three times.

The `/oobe` (oobe stands for Out of the Box Experience) will restart the computer into Windows Welcome mode. Windows Welcome enables end users to customize their Windows operating system, create user accounts, name the computer, and other tasks. Any settings in the oobe system configuration pass in an answer file are processed immediately before Windows Welcome starts.

Performing an Unattended Installation

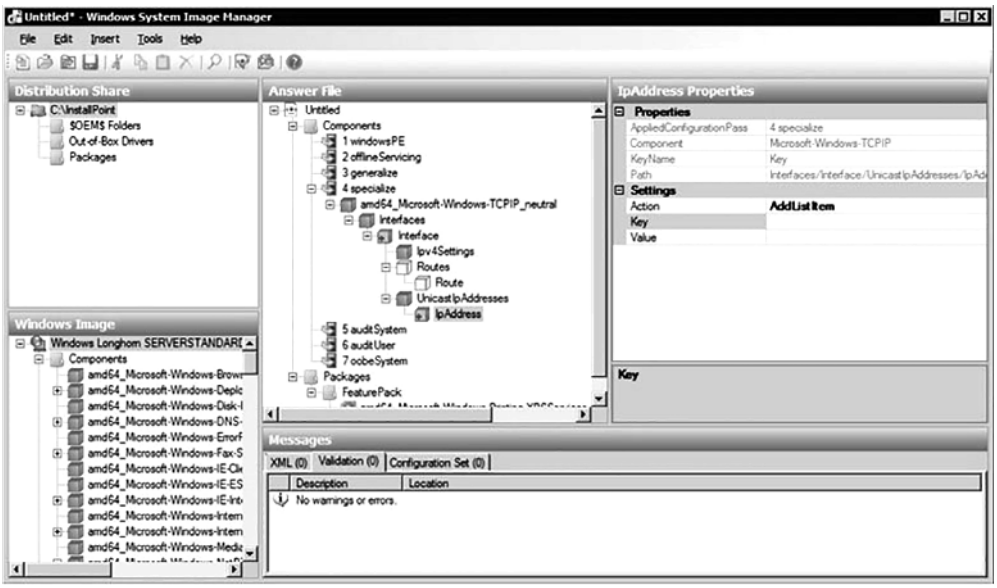
An *unattended installation* is an installation that requires little interaction to install. To perform an unattended installation of Windows you would use an answer file. An answer file is an XML file that stores the answers for a series of graphical user interface (GUI)

dialog boxes. The answer file for Windows Setup is commonly called `autounattend.xml`. Since the answer file is an XML file, you can use any text editor such as Notepad to create and modify the answer file.

A sample answer file can be found at `https://social.technet.microsoft.com/wiki/contents/articles/36609.windows-server-2016-unattended-installation.aspx`. However, you will find it much easier if you use the Windows System Image Manager (SIM) to create the answer file. It can also be used to validate the answer file.

To install Windows SIM, you first need to download and install Windows Automated Installation Kit (AIK) for Windows 10 from the Microsoft website (`https://developer.microsoft.com/en-us/windows/hardware/windows-assessment-deployment-kit`). To start Windows SIM, you then click the Start button, select Microsoft Windows AIK, and select Windows System Image Manager (see Figure 1.11).

FIGURE 1.11 Windows System Image Manager



After you create an answer file called `autounattend.xml`, you place the file to removable media, such as a USB flash device, CD/DVD drive, or floppy disk. You then insert the removable media into the destination computer and boot the destination computer from DVD. Setup automatically searches for `autounattend.xml` and performs the installation with the parameters specified without any interaction from you.

Using Windows Deployment Services

Windows Deployment Services (WDS) is a technology from Microsoft for network-based installation of Windows operating system including Windows 7, Windows 8/8.1, Windows 10, Windows Server 2012 R2, and Windows Server 2016. The deployment of

Windows can be fully automated and customized through the use of unattended installation scripting files.

The Windows installation files can be distributed within a Windows Imaging Format (WIM) file. WIM is the file-based imaging format that Windows Server uses for rapid installation on a new computer. WIM files store copies (known as images) of the operating systems, such as Windows PE, Windows 10, or Windows Server 2016. Maintaining an operating system in a WIM file is easy because you can add and remove drivers, updates, and Windows components offline, without ever starting the operating system.

Windows Deployment Services uses the WIM files to install Windows. If set up properly, you need to boot a computer with Windows PE or perform a PXE boot. Windows Preinstallation Environment (Windows PE) is a minimal Win32 operating system with limited services, built on the Windows kernel. It is used to prepare a computer for Windows installation, to copy disk images from a network file server, and to initiate Windows Setup.

You then connect to the WDS server and install Windows from a configured image. A configuration script is executed that verifies the computer's configuration and hardware requirements. It can also be used to run the Diskpart tool to partition and format the disk. If necessary, the script can back up the user's data to a shared folder on another computer. Eventually, the script connects to a shared folder containing the Windows Setup files and runs the Windows Setup program to install the operating system fully unattended.

Understanding Windows Licensing

One of the biggest costs to any IT department is the cost of software. When you add the client copies of Windows and Office, the cost of the server operating system and the cost of additional enterprise software such as Exchange or SQL, it can easily add up to thousands of dollars. Therefore, you need to look at your available options to get the best price for what you need to do.

A software license is given to you from a software company including Microsoft that gives you permission to use a specific software package and usually comes with many restrictions. Most licenses from corporations such as Microsoft are more like a lease rather than purchasing the actual software. The typical restriction limits you to use only one copy of the software per license and prohibit you to distribute or copy the license in any way (except for backup purposes). Licenses for enterprise-class server software (such as Microsoft Exchange or Microsoft SQL) could also require a Client Access License (CAL) for each user that is to access the server software.

The least inexpensive license to obtain is the OEM (Original Equipment Manufacturer) license, which can only be purchased with a new computer from a system builder such as HP or IBM. Unfortunately, these licenses are tied to a specific machine and cannot be transferred later to a new machine. The OEM is usually responsible for technical support on the software that you bought.

The retail license (usually purchased from your office or computer store or over the Internet) allows you move it from one machine to another. Of course, retail software

usually costs more than OEM software. Another disadvantage of using retail software from Microsoft you need to enter a key code and activate the software. Another disadvantage is that if you move the software to another computer or you make semi-significant changes such as adding RAM or a new hard drive, you may need to re-activate the software.

Lastly, Microsoft has several volume licensing programs available to organize their licenses and stay up to date with the newest software at a discounted price. The Open license is intended for businesses with at least 5 PCs and Select License and Enterprise Agreement Plans are licensing programs intended for corporations with at least 250 PCs. Each of these programs may have additional benefits such as free take-home licenses and training.

Volume licensing can be further broken down into Multiple Activation Key (MAK) and Key Management Services (KMS). With MAK, each key has to be registered and activated individually, while Key Management Services (KMS) uses a KMS server to automatically connect to Microsoft's license warehouse and activate the key.

Understanding Windows Activation

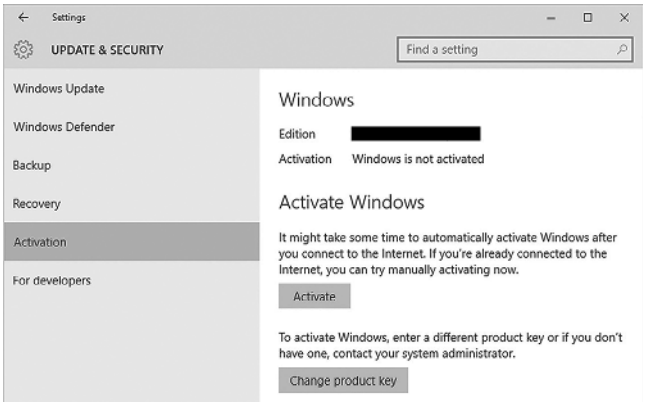
Activation helps verify that your copy of Windows is genuine and that it has not been used on more computers than the Microsoft Software Terms allow. Windows Server 2016 requires product activation, which validates each Windows Server 2016 license through an online activation service at Microsoft by phone, through KMS, or through Active Directory Domain Services, in order to be fully functional. During the activation step, you install the proper license key for Windows.

There are no activation grace periods. If you do not activate Windows Server 2016, you cannot use the personalization settings or customize the operating system.

As part of the planning, you must ensure that you have the correct number of licenses for your Windows operating systems, including Windows Server 2016. Windows Server 2016 is licensed by physical processor core, not by server. You can purchase additional licenses for two physical processor cores at a time.

You can activate Windows in two ways: manually or automatically. With manual activation, you must enter the product key and activate over the Internet to the special clearinghouse website, or over the phone by using a retail product key or a *multiple activation key (MAK)*. To activate over the Internet, you open Settings, click Update & Security, and click Activate, as shown in Figure 1.12. When you use a MAK, you can activate multiple computers, up to a set activation limit.

FIGURE 1.12 Activating Windows



You can also use *Original Equipment Manufacturer (OEM) keys* with computers. Manufacturers provide OEM keys, which are typically tied to specific computers. OEM keys are usually distributed with systems running Windows 7 or higher but can also be found on systems running Windows Server operating systems.

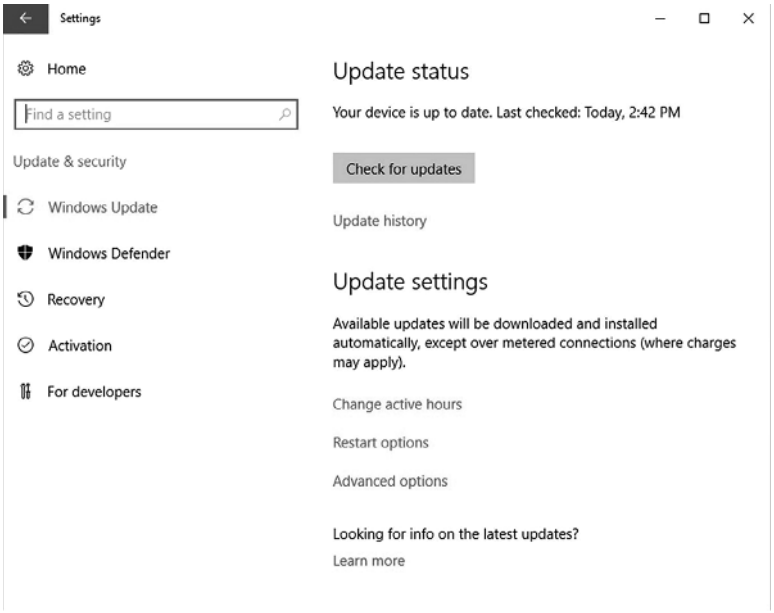
If you have many clients and servers, consider setting up a Volume Activation Services server. When you install the Volume Activation Services server role, you can choose Key Management Service or Active Directory–Based Activation. After adding the Volume Activation Services role, you can use the Volume Activation Tools GUI to configure activation. When you use Volume Activation Services, each activated computer must contact the KMS server periodically to renew its activation status. To report on activated licenses, you can use the Volume Activation Management Tool (VAMT), which is part of the Windows Assessment and Deployment Kit (ADK).

Configuring Update Settings

Windows Update provides your Windows 10 and Windows 2016 users with a way to keep their computers current by checking a designated server. The server provides software that patches security issues, installs updates that make Windows and your applications more stable, fixes issues with existing Windows programs, and provides new features. The server can be hosted by Microsoft, or it can be set up and managed in your organization by running the Windows Server Update Services (WSUS) or System Center 2016 Configuration Manager.

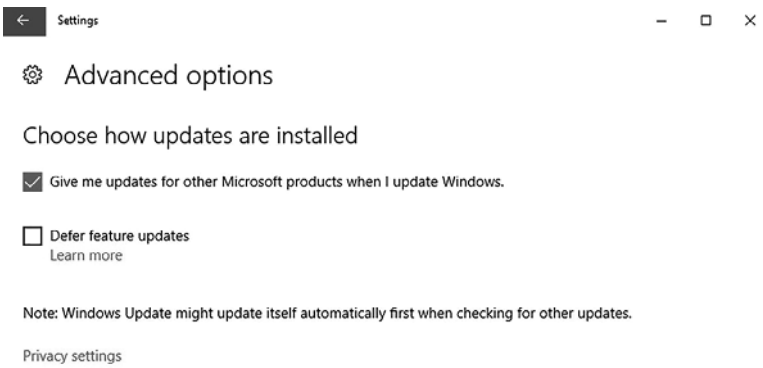
When you first install Windows Server 2016, you can choose how you want Windows Update to function. On a Windows Server 2016 computer, you can open Settings and click Update & Security to open the Windows Update page (see Figure 1.13).

FIGURE 1.13 The Windows Update page



By clicking Advanced options, you can configure for Automatic Updates, give updates for other Microsoft products when Windows is updated, defer upgrades, and view update history (as shown in Figure 1.14).

FIGURE 1.14 The Windows Update Advanced Options page



For corporations, you can also use Windows Server Update Services (WSUS) or System Center 2016 Configuration Manager to keep your systems updated. Smaller organizations

might use WSUS or cloud-based services such as Microsoft Intune to keep systems up to date. The advantage of using one of these systems is that it allows you to test the patch, schedule the updates, and prioritize client updates. Once you determine a patch is safe, you can enable it for deployment.

Under Advanced options, you can customize how updates are installed. By default, the "Choose how updates are installed" option is set to Automatic (recommended), which means Windows will pick a time when you don't use your computer to install the updates and reboot the system. Most organizations would prefer the "Notify to schedule restart" option so that Windows will not reboot your computer when you least expect it.

Windows Server 2016 lets you defer upgrades to your PC. By selecting the Defer upgrades option, new Windows features won't be downloaded or installed for several months. This option is typically used to help avoid problems with an update that might cause problems within your organization.

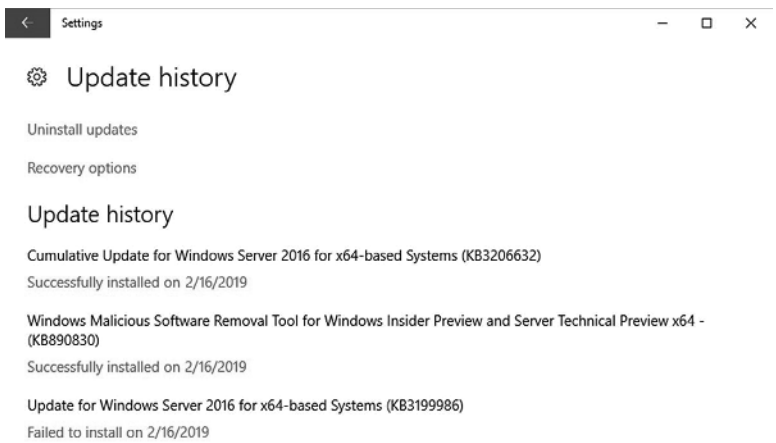
Deferring upgrades does not affect security updates, but it does prevent you from getting the latest Windows features as soon as they are available.

If Windows Update fails to retrieve any updates, you should check your proxy settings in Internet Explorer to see whether the program can get through your proxy server (if any) or firewall. You should also make sure you can access the Internet, such as by going to the Microsoft website.

You can view your update history by opening the Advanced Options and selecting View your update history. On the Update History page, each update, including the KB article number, the version, and the date installed, is shown. If you click Successfully Installed On <*date*> for a specific update, it will give a short description of the update.

At the top of the View Your Update History page, you can click Uninstall Updates to open the Control Panel Installed Updates page, as shown in Figure 1.15. To uninstall or roll back an update, right-click the desired update and choose Uninstall. You will then be prompted to uninstall the update. When you click Yes, the update will be uninstalled.

FIGURE 1.15 The Control Panel Installed Updates page



Skill Summary

In this lesson you learned:

- A server is a computer that is a meant to be a dedicated service provider, and a client is a computer that requests services.
- Before selecting the hardware and software components of a server, you should identify the server roles and network services that the server will need to provide and how many people will be accessing the server at once to help determine the load the server needs to fulfill.
- The primary subsystems that make up a server are processor, memory, storage, and network.
- The computer, including servers, is built around one or more integrated chips called the processor. It is considered the brain of the computer since all of the instructions it performs are mathematical calculations and logical comparisons.
- A 64-bit processor is a processor with a default word size of 64 bits and 64-bit external data bus, which allows you to access much more RAM than a 32-bit processor.
- The amount of RAM can be one the largest factor in your overall computer performance.
- For the processor to communicate with the rest of the system, the processor plugs in or connects to a large circuit board called the motherboard or system board. The motherboard allows the processor to branch out and communicate with all of the other computer components.
- Instructions that control much of the computer's input/output functions, such as communicating with disks, RAM, and the monitor kept in the System ROM chips are known as the BIOS (basic input/output system).
- The process of updating your system ROM BIOS is called flashing the BIOS.
- While a server needs to have solid performance, the server needs to be reliable.
- Virtual machines technologies enable multiple operating systems to run concurrently on a single machine.
- Windows Server 2016 has organized the most common services into server roles. A server role describes the function of the server.
- Windows Server 2016 Features are software programs that are not directly part of a role, or they can support or augment the functionality of one or more roles or enhance the functionality of the entire server.
- Server Core installation provides a minimal environment with no Windows Explorer shell for running specific server roles and no Start button.
- Before installing software, you should look at the system requirements as a starting point to make sure your server meets those requirements.

- A clean installation is installing the software from scratch on a new drive or on newly reformatted drive. Many people find that doing a clean install of an operating system is the best way to go because you are starting fresh.
- In some instances, you will want to take a current system and upgrade from an older version of Windows to Windows Server 2016.
- One way to install Windows Server 2016 is to use disk cloning software such as Norton Ghost to create an image file, which is a sector-by-sector copy stored in a large file.
- If you clone a computer, you need to run the System Preparation Tool (Sysprep), which removes the security identifiers and all other user-specific or computer-specific information from the computer before you run the disk cloning software to make the cloned disk image.
- An Answer file is an XML file that stores the answers for a series of graphical user interface (GUI) dialog boxes, which is used to automatically install Windows.
- Windows Deployment Services (WDS) is a technology from Microsoft for network-based installation of Windows operating system including Windows 7, Windows 8/8.1, Windows 10, Windows Server 2012 R2, and Windows Server 2016. The deployment of Windows can be fully automated and customized through the use of unattended installation scripting files.
- Microsoft product activation is an anti-piracy technology designed to verify that software products are legitimately licensed.
- After installing Windows, check to see if Microsoft has any fixes, patches, service packs, and device drivers, and apply them to the Windows system.

Knowledge Assessment

Fill in the Blank

1. A _____ is a primary duty that a server performs.
2. The computer including servers is built around one or more integrated chips called the _____.
3. A _____ processor can typically process more data at the same time and can access much more memory than a 32-bit processor.
4. Making sure you have sufficient _____ is one of the biggest factors in performance even more than disk and processor.
5. For the processor to communicate with the rest of the system, the processor plugs in or connects to a large circuit board called the _____.
6. Firmware is software contained in _____ chips.
7. Instructions that control much of the computer's input/output functions, such as communicating with disks, RAM, and the monitor kept in the System ROM chips are known as the _____.
8. The process of update your system ROM BIOS is called _____ the BIOS.
9. _____ installation provides a minimal environment with no Windows Explorer shell for running specific server roles and no Start button.
10. A(n) _____ is an XML file that stores the answers for a series of graphical user interface (GUI) dialog boxes.

Multiple Choice

1. What technology provided by Microsoft is used to perform network-based installation of Windows operating systems including Windows 7, Windows 8/8.1, Windows 10, and Windows Server 2016?
   - **A.** IAS
   - **B.** Server Core
   - **C.** SIM
   - **D.** WDS

2. What does the name of the answer file on a USB drive have to be to perform an automatic installation?
   - **A.** `autounattend.xml`
   - **B.** `auto.xml`
   - **C.** `auto.txt`
   - **D.** `automatic.xml`
3. What is the program you should you use to create or validate an answer file used to install Windows?
   - **A.** IAS
   - **B.** Server Core
   - **C.** SIM
   - **D.** WDS
4. What is the maximum amount of memory that Windows Server 2016 Standard Edition?
   - **A.** 2 GB
   - **B.** 4 GB
   - **C.** 1 TB
   - **D.** 24 TB
   - **E.** 64 TB
5. How many days grace period do you have where you will have to activate Windows Server 2016?
   - **A.** 3 days.
   - **B.** 10 days.
   - **C.** 15 days.
   - **D.** 30 days.
   - **E.** There is no grace period.
6. Which of the following is not a primary subsystem found in a server?
   - **A.** Processor
   - **B.** Memory
   - **C.** Sound
   - **D.** Storage
7. What type of installation do you use that starts from scratch?
   - **A.** A clean upgrade
   - **B.** A clean installation
   - **C.** A formatting installation
   - **D.** A backup installation

8. What command would you use to prepare a Windows installation for imaging that will remove the SID and computer name?
   - **A.** Sys
   - **B.** Sysprep
   - **C.** SIDPrep
   - **D.** WDSPrep
9. What does Microsoft use to fight pirated copies of Windows?
   - **A.** WDS
   - **B.** IAS
   - **C.** Sysprep
   - **D.** Activation
10. Which edition of Windows Server 2016 gives you the most access to processors and memory?
   - **A.** Foundation
   - **B.** Standard
   - **C.** Enterprise
   - **D.** Datacenter

True/False

1. If you have a power outage while you are flashing the BIOS, you can just restart the process when the power is restored.
2. Windows Server 2016 can be only on 64-bit processors.
3. The lowest edition of Windows Server 2016 is the Standard edition.
4. When you clone a server with Windows Server 2016, you just need to blank the computer name and administrator password.
5. The standard protocol to share files on Windows Server 2016 is SMB

Competency Assessment

Scenario 1-1: Server Analysis

You are designing a new network for the Acme Corporation. You expect to have a lot of sales over the Internet. How many servers do you think you will need, what hardware requirements should you use, and what role would you assign to each server? Hint: when you purchase something over the Internet, what type of server do you access to purchase

something? Then what type of server do you think you will need in the background that will keep track of those sales?

Scenario 1-2: Identify Ports

Look at the back of your computer and draw a diagram that shows all of the ports and the purpose of the port.

Proficiency Assessment

Scenario 1-3: Installing Windows Server 2016

Go to Microsoft's website and find and download the evaluation copy of Windows Server 2016. Burn the image to a DVD. Then boot a computer and install Windows Server 2016 following the steps listed in the Clean Installation section. When configuring your disk, only use half of the disk for your C drive.

Scenario 1-4: Using Windows Updates

Use the Windows Update program to patch Windows.

Real World Scenario

Workplace Ready: Selecting the Right Server

If you are new to server administration, trying to determine the right server can be quite challenging. So what can you do?

First, you will need to do a lot of reading including looking for the minimum requirements and always go beyond the minimum. If it says it needs 2 GB of memory, plan for at least 4 GB. If it needs a single processor running at 2 GHz, plan for dual processors running at 2.4 GHz. If it is the specification for the operating system, always double them as a minimum. In addition, when you are researching look for load recommendations or load specifications or guidelines.

Next, if you have a similar server, you should at its current load and try to compare to the predicted load to see if it is different. You can also look at processor, memory, disk, and network performance.

You should also ask people who use the server about perceived performance to see if it is adequate or if it should be increased. You should then verify the performance by using the network application in the same way and measure how long it takes for a task to be done.