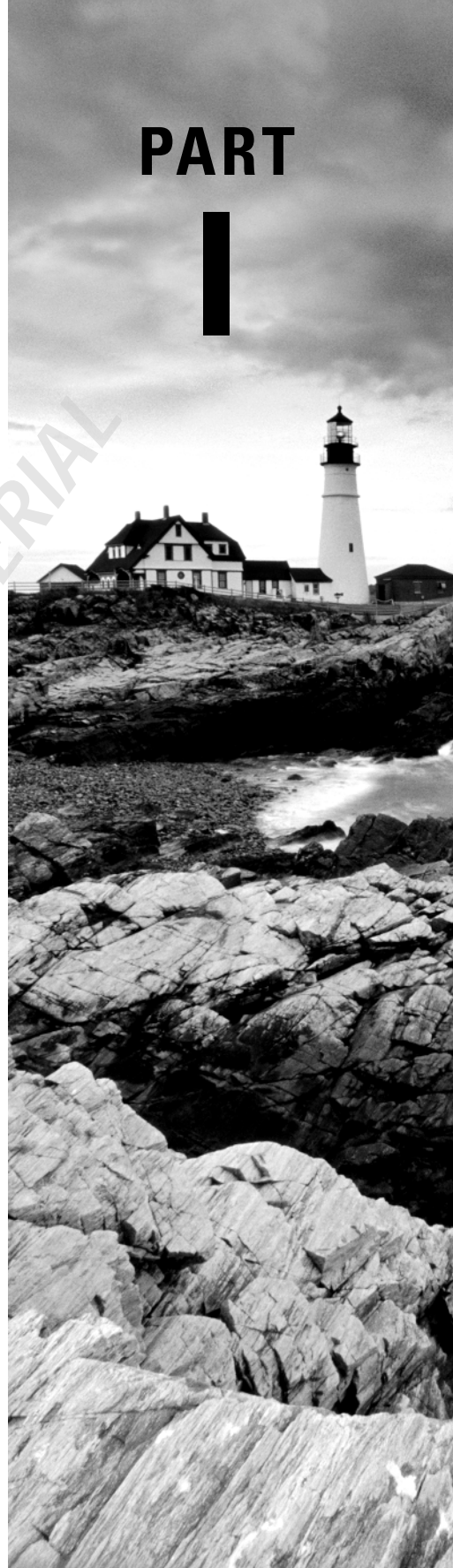


Exam 70-410: Installing and Configuring Windows Server 2012 R2

- CHAPTER 1 ■ Install Windows Server 2012 R2
- CHAPTER 2 ■ Configure Network Services
- CHAPTER 3 ■ Plan and Install Active Directory
- CHAPTER 4 ■ Configure Windows Server 2012 R2
- CHAPTER 5 ■ Administer Active Directory
- CHAPTER 6 ■ Manage GPOs
- CHAPTER 7 ■ Manage Security
- CHAPTER 8 ■ Configure TCP/IP
- CHAPTER 9 ■ Use Virtualization in Windows Server 2012

PART

I



Chapter 1

Install Windows Server 2012 R2

THE FOLLOWING 70-410 EXAM OBJECTIVES ARE COVERED IN THIS CHAPTER:

✓ **Install servers**

- Plan for a server installation
- Plan for server roles
- Plan for a server upgrade
- Install Server Core
- Optimize resource utilization by using Features on Demand
- Migrate roles from previous versions of Windows Server
- Configure Server Core
- Add and remove features in offline images
- Deploy roles on remote servers
- Convert Server Core to/from full GUI
- Configure NIC teaming

✓ **Configure local storage**

- Design storage spaces
- Configure basic and dynamic disks
- Configure MBR and GPT disks
- Manage volumes
- Create and mount virtual hard disks
- Configure storage pools and disk pools



This chapter covers the installation of Windows Server 2012 R2. It shows how to install both the full version of Windows Server 2012 R2 and the Server Core version. It also shows you how to use some PowerShell commands in Windows Server 2012 R2 Server Core.

Let's dive right into the server by talking about some of the new features and advantages of Windows Server 2012 R2.

Features and Advantages of Windows Server 2012 and Server 2012 R2

Before I show how to install and configure Windows Server 2012 R2, let's take a look at some of the new features and the advantages it offers.



Since many of you will be upgrading from Windows Server 2003 and Windows Server 2008/2008 R2, these are the new features introduced by Microsoft since then. I will specifically identify any new features or advantages that are new to Windows Server 2012 R2 only.

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

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

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

Active Directory Rights Management Services *Active Directory Rights Management Services (AD RMS)* provides management and development tools that let you work with

industry security technologies, including encryption, certificates, and authentication. Using these technologies allows organizations to create reliable information protection solutions.

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

BranchCache *BranchCache* allows data from files and web servers on a wide area network (WAN) to be cached on computers at a local branch office. By using BranchCache, you can improve application response times while also reducing WAN traffic. Cached data can be either distributed across peer client computers (distributed cache mode) or centrally hosted on a server (hosted cache mode). BranchCache is included with Windows Server 2012 R2 and Windows 8.



In this book, I will refer to *Windows 8*, which includes both Windows 8 and Windows 8.1. This is also true for *Windows Server 2008*. It will be used for both Windows Server 2008 and Windows Server 2008 R2. If, for some reason, both versions of Server 2008 did not cover an item, I will actually say 2008 R2.

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

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

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

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

Hyper-V *Hyper-V* is one of the most changed features in Windows Server 2012 R2. Microsoft's new slogan is "Windows Server 2012 R2, built from the cloud up," and this has a lot to do with Hyper-V. It allows an organization to consolidate servers by creating and managing a virtualized computing environment. It does this by using virtualization technology that is built into Windows Server 2012 R2.

Hyper-V allows you to run multiple operating systems simultaneously on one physical computer. Each virtual operating system runs in its own virtual machine environment. I cover Hyper-V in detail in Chapter 9: “Use Virtualization in Windows Server 2012.”

IPAM *IP Address Management (IPAM)* is one of the features introduced with Windows Server 2012 R2. IPAM allows an administrator to customize and monitor the IP address infrastructure on a corporate network.

Kerberos Authentication Windows Server 2012 R2 uses the *Kerberos authentication* (version 5) protocol and extensions for password-based and public key authentication. The Kerberos client is installed as a *security support provider (SSP)*, and it can be accessed through the *Security Support Provider Interface (SSPI)*.

Managed Service Accounts (gMSAs) Stand-alone *managed service accounts*, originally created for Windows Server 2008 R2 and Windows 7, are configured domain accounts that allow automatic password management and *service principal names (SPNs)* management, including the ability to delegate management to other administrators.

Networking There are many networking technologies and features in Windows Server 2012 R2, including BranchCache, Data Center Bridging (DCB), NIC Teaming, and many more.

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

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

Smart Cards Using *smart cards* (referred to as *two-factor authentication*) and their associated *personal identification numbers (PINs)* is a popular, reliable, and cost-effective way to provide authentication. When using smart cards, the user not only must have the physical card but also must know the PIN to be able to gain access to network resources. This is effective because even if the smart card is stolen, thieves can't access the network unless they know the PIN.

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

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

Planning the Windows Server 2012 R2 Installation

Before you install Windows Server 2012 R2, you must first ask yourself these important questions: What type of server do I need? Will the server be a domain controller? What roles do I need to install on this server?

Once you have figured out what you need the server to do, you can make a game plan for the installation. So, let's start by looking at some of the server roles and technologies that can be installed on a Windows Server 2012 R2 computer.

Server Roles in Windows Server 2012 R2

When you install Windows Server 2012 R2, you have to decide which roles and features are going to be installed onto that server. This is an important decision in the computer world. Many administrators not only overuse a server but also underutilize servers in their organization.

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

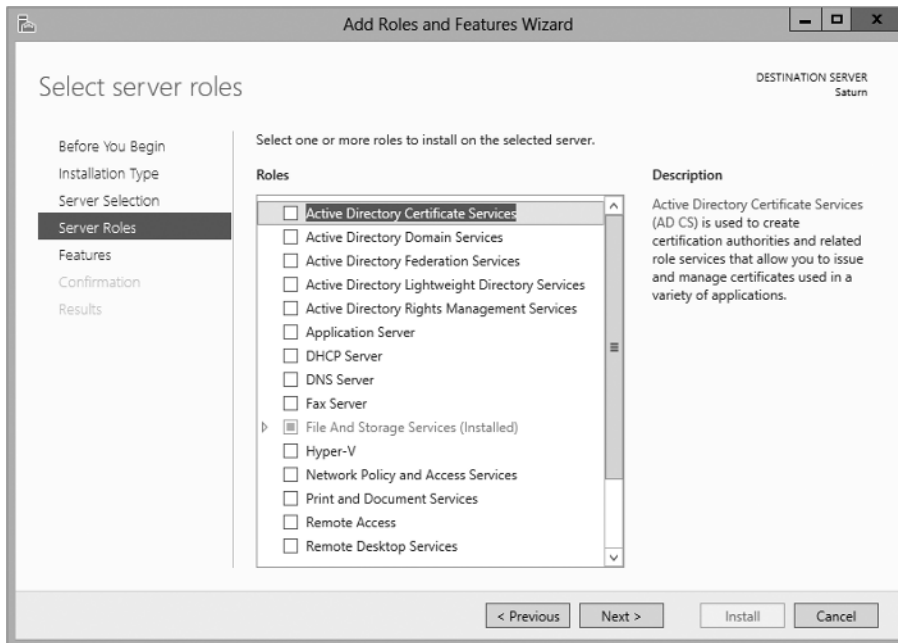
Now let's take a look at some of the roles and features you can install onto a Windows Server 2012 R2 machine. Knowing the different roles and features you can install will help you to design, deploy, manage, and troubleshoot technologies in Windows Server 2012 R2. Figure 1.1 shows the Add Roles And Features Wizard in Server Manager. It shows you just some of the roles that can be installed on a Windows Server 2012 R2 machine.

Roles and Features

Many of these features were discussed in the section "Features and Advantages of Windows Server 2012 and Server 2012 R2." I include them here again because they are also *roles* that can also be installed on Windows Server 2012 R2.

The following roles are available in Windows Server 2012 R2:

Active Directory Certificate Services The AD CS server role in Windows Server 2012 R2 allows you to build a PKI and provide public key cryptography, digital certificates, and digital signature capabilities for your organization.

FIGURE 1.1 Available roles in Windows Server 2012 R2

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

Role AD CS in Windows Server 2012 R2 is the server role that allows you to build a PKI and provide public key cryptography, digital certificates, and digital signature capabilities for your organization.

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

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

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

Active Directory Rights Management Services Active Directory Rights Management Services (AD RMS) in Windows Server 2012 R2 is the server role that provides you with management and development tools that work with industry security technologies including encryption, certificates, and authentication to help organizations create reliable information protection solutions.

Application Server *Application Server* provides an integrated environment for deploying and running custom, server-based business applications.

Failover Clustering The Failover Clustering feature provides a way to create, configure, and manage failover clusters for up to 4,000 virtual machines or up to 64 physical nodes.

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

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

Hyper-V The Hyper-V role allows administrators to create and manage a virtualized environment by taking advantage of the technology built into the Windows Server 2012 R2 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).

Networking This feature allows administrators to design, deploy, and maintain a Windows Server 2012 R2 network. The networking features include 802.1X authenticated wired and wireless access, BranchCache, Data Center Bridging, low-latency workload technologies, and many more.

Network Load Balancing The *Network Load Balancing (NLB)* feature dispenses traffic across multiple servers by using the TCP/IP networking protocol. By combining two or more computers that are running applications in Windows Server 2012 R2 into a single virtual cluster, NLB provides reliability and performance for mission-critical servers.

Network Policy and Access Services Use the *Network Policy and Access Services* server role to install and configure *Network Access Protection (NAP)*, secure wired and wireless access points, and RADIUS servers and proxies.

Print and Document Services *Print and Document Services* allows an administrator to centralize print server and network printer tasks. This role also allows you to receive scanned documents from network scanners and route the documents to a shared network resource, Windows SharePoint Services site, or email addresses. Print and Document

Services also provides fax servers with the ability to send and receive faxes while also giving the administrator the ability to manage fax resources such as jobs, settings, reports, and fax devices on the fax server.

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

Security and Protection Windows Server 2012 R2 has many new and improved security features for your organization. These security features include Access Control, AppLocker, BitLocker, Credential Locker, Kerberos, NTLM, passwords, security auditing, smart cards, and Windows Biometric Framework (WBF).

Telemetry The *Telemetry* service allows the Windows Feedback Forwarder to send feedback to Microsoft automatically by deploying a Group Policy setting to one or more organizational units. Windows Feedback Forwarder is available on all editions of Windows Server 2012 R2, including Server Core.

Volume Activation Windows Server 2012 R2 *Volume Activation* will help your organization benefit from using this service to deploy and manage volume licenses for a medium to large number of computers.

Web Server (IIS) The *Web Server (IIS)* role in Windows Server 2012 R2 allows an administrator to set up a secure, easy-to-manage, modular, and extensible platform for reliably hosting websites, services, and applications.

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

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

Windows Server Update Services *Windows Server Update Services (WSUS)* allows administrators to deploy application and operating system updates. By deploying WSUS, administrators have the ability to manage updates that are released through Microsoft Update to computers in their network. This feature is integrated with the operating system as a server role on a Windows Server 2012 R2 system.

Migrating Roles and Features to Windows Server 2012 R2

Once you decide on which roles and features you are going to install onto your Windows Server 2012 R2 system, then you either have to install those roles and features from scratch or migrate them from a previous version of Windows server.

Windows Server 2012 R2 includes a set of migration tools that administrators can use to help ease the process of migrating server roles, features, operating system settings, and data. Administrators can migrate this data from an existing server that is running Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, or Windows Server 2012 R2 to a computer that is running Windows Server 2012 R2.

Using Windows Server Migration Tools to migrate roles, role services, and features can simplify the deployment of new servers. You can migrate roles and features on servers running the Server Core installation option of Windows Server 2012 R2 and virtual servers. By using Windows Server Migration Tools, an administrator can reduce migration downtime, increase the accuracy of the migration process, and help eliminate conflicts that could otherwise occur during the migration process.

One advantage of using the migration tools is that most of them support cross-architecture migrations (x86-based to x64-based computing platforms), migrations between physical and virtual environments, and migrations between both the full and Server Core installation options of the Windows Server operating system. In Windows Server 2012 R2, Windows Server Migration Tools also supports cross-subnet migrations.

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

1. Installing Windows Server Migration Tools on destination servers that run Windows Server 2012 R2
2. Creating deployment folders on destination servers that run Windows Server 2012 R2 for copying to source servers
3. Copying deployment folders from destination servers to source servers
4. Registering Windows Server Migration Tools on source servers

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

Administrators can install Windows Server Migration Tools 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 2012 R2, you would complete the following steps:

1. Open a Windows PowerShell session by typing **powershell.exe** in the current command prompt session and then pressing Enter.
2. In the Windows PowerShell session, install Windows Server Migration Tools by using the Windows PowerShell `Install-WindowsFeature` cmdlet for Server Manager. In the Windows PowerShell session, type the following, and then press Enter. (Omit the `ComputerName` parameter if you are installing the Windows Server Migration Tools on the local server.)

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

Roles and Features That Have Been Reduced in Windows Server 2012 R2

One thing that we want to look at is which Roles and Features are being deprecated or removed from Windows Server 2012 and Windows Server 2012 R2. Table 1.1 was taken directly from Microsoft's website (<http://technet.microsoft.com/en-us/library/dn303411.aspx>), and this table may change at any time. Thus I would recommend that you go out to Microsoft's website to see the current list of Roles and Features.

Table 1.1 lists the features and functionalities in Windows Server 2012 and Windows Server 2012 R2 that either have been removed from the product in the current release or are planned for potential removal in subsequent releases (shown as *deprecated*).

TABLE 1.1 Roles and Features Updates

	Windows Server 2012		Windows Server 2012 R2	
	Removed	Deprecated	Removed	Deprecated
AD FS v1 Web Agent			X	
AD FS in-place upgrade from AD FS 1.0 or "out-of-the-box" AD FS 2.0	X			
AD FS support for "Resource Group"	X			
AD FS support for NT Token mode	X			
AD FS support for using AD LDS as an authentication store	X			
AD RMS license revocation				X
AD RMS SDK				X
Application Server role				X
Built-in drivers for tape drives				X
Cluster Automation Server COM API	X (Optional)		X (Optional)	
Cluster.exe command-line interface	X (Optional)		X (Optional)	

CertObj COM and InetInfo inter- faces of the Web Server role			X
Dcpromo.exe		X	
Dfscmd.exe			X
Drivers for Jet Red RDBMS and ODBC		X	X
File Replication Service			X
Internet Information Service (IIS) 6.0 Manager			X
Layered Service Providers		X	X
LPR/LPD protocol		X	X
Namespace for version 1.0 of WMI; WMIC (in WMI)		X	X
NDIS version 5.0, 5.1, and 5.2 APIs		X	X
Net DMA	X		
Network Access Protection (NAP)			X
Network Information Service (NIS) and Tools (in RSAT)			X
Nfsshare.exe			X
NFSv2 support			X
Ocllist.exe	X		
ODBC support for 16- and 32-bit applications and drivers		X	X
ODBC/OLEDB support for Microsoft Oracle		X	
ODBC/OLEDB support for SQL beyond SQL Server 7 and SQL 2000		X	X

TABLE 1.1 Roles and Features Updates (*continued*)

	Windows Server 2012		Windows Server 2012 R2	
	Removed	Deprecated	Removed	Deprecated
Providers for SNMP, Win32_ServerFeature API, Active Directory, MSCluster WMI1.0 (in WMI)		X		X
Recovery disk creation			X	
Remote Data Service		X		
Role Collector (Ceiprole.exe) and associated API	X			
SCSIport host-bus adapter	X			
Servermanagercmd.exe		X	X	
SIS Limited API				X
SImgr.vbs options			X	
SMB 1.0				X
SMB.sys	X			
SMTP and associated management tools		X		X
SQLXMLX		X		X
Storage Explorer snap-in for MMC	X			
Storage Manager for SANs snap-in for MMC	X			
Subsystem for UNIX-based applications		X	X	
Support for 32-bit cluster resource DLLs	X			
Support for hardware drivers for XDDM	X			

Support for Microsoft SQL Server prior to 7.0	X		
Support for native VGA via the PC/AT BIOS or UEFI CSM	X		
Support for Static VMQ		X	
Support for Token Rings		X	
Support for Visual Studio Analyzer 2003 over ODBC, OLEDB, and ADO	X		
System Image Backup ("Windows 7 File Recovery")			X
Telnet server			X
VM Chimney (also called TCP Offload) in Hyper-V	X		
Windows Server 2003 domain and functional levels of Active Directory			X
Windows Authorization Manager (AzMan)		X	X
Windows Help executable (WinHlp32.exe)	X		
Windows Identity Foundation 3.5			X
Windows Server Resource Manager		X	X
Winsock Direct		X	X
WMI root/virtualization namespace v1 (in Hyper-V)		X	X
XDR schema elements, XSI pattern feature of MSXML3 (in XML)		X	X

Deciding Which Windows Server 2012 R2 Versions to Use

You may be wondering which version of Windows Server 2012 R2 is best for your organization. After all, Microsoft offers the following four versions of Windows Server 2012 R2.

Windows Server 2012 R2 Datacenter This version is designed for organizations that are looking to migrate to a highly virtualized, private cloud environment. Windows Server 2012 R2 Datacenter has full Windows Server functionality with unlimited virtual instances.

Windows Server 2012 R2 Standard This version is designed for organizations with physical or minimally virtualized environments. Windows Server 2012 R2 Standard has full Windows Server functionality with two virtual instances.

Windows Server 2012 R2 Essentials This version is ideal for small businesses that have as many as 25 users and 50 devices. Windows Server 2012 R2 Essentials has a simpler interface and preconfigured connectivity to cloud-based services but no virtualization rights.

Windows Server 2012 R2 Foundation This version is designed for smaller companies that need a Windows Server experience for as few as 15 users. Windows Server 2012 R2 Foundation is a general-purpose server with basic functionality but no virtualization rights.

Once you choose what roles are going on your server, you must then decide how you're going to install Windows Server 2012 R2. There are two ways to install Windows Server 2012 R2. You can upgrade a Windows Server 2008 R2 with SP1 or Windows Server 2012 machine to Windows Server 2012 R2, or you can do a clean install of Windows Server 2012 R2. If you decide that you are going to upgrade, there are specific upgrade paths you must follow.

Your choice of Windows Server 2012 R2 version is dictated by how your current network is designed. If you are building a network from scratch, then it's pretty straightforward. Just choose the Windows Server 2012 R2 version based on your server's tasks. However, if you already have a version of Windows Server 2008 installed, you should follow the recommendations in Table 1.2, which briefly summarize the supported upgrade paths to Windows Server 2012 R2.



If your version of Microsoft Windows Server is not listed in the left column, upgrading to Windows Server 2012 R2 is not supported. If there is more than one edition listed in the right column, you can then choose either edition.

TABLE 1.2 Supported Windows Server 2012 R2 upgrade path recommendations

Current System	Upgraded System
Windows Server 2008 R2 Datacenter with SP1	Windows Server 2012 R2 Datacenter
Windows Server 2008 R2 Enterprise with SP1	Windows Server 2012 R2 Standard or Windows Server 2012 R2 Datacenter

Windows Server 2008 R2 Standard with SP1	Windows Server 2012 R2 Standard or Windows Server 2012 R2 Datacenter
Windows Web Server 2008 R2 with SP1	Windows Server 2012 R2 Standard
Windows Server 2012 Datacenter	Windows Server 2012 R2 Datacenter
Windows Server 2012 Standard	Windows Server 2012 R2 Standard or Windows Server 2012 R2 Datacenter
Hyper-V Server 2012	Hyper-V Server 2012 R2
Windows Storage Server 2012 Standard	Windows Storage Server 2012 R2 Standard
Windows Storage Server 2012 Workgroup	Windows Storage Server 2012 R2 Workgroup

Deciding on the Type of Installation

One of the final choices you must make before installing Windows Server 2012 R2 is what type of installation you want. There are three ways to install Windows Server 2012 R2.

Windows Server 2012 R2 with the Graphical User Interface (GUI) This is the version with which most administrators are familiar. This is the version that uses *Microsoft Management Console (MMC)* windows, and it is the version that allows the use of a mouse to navigate through the installation.

Windows Server 2012 R2 Server Core This is a bare-bones installation of Windows Server 2012 R2. You can think of it this way: If Windows Server 2012 R2 is a top-of-the-line luxury car, then Windows Server 2012 R2 Server Core is the stripped-down model with no air-conditioning, manual windows, and cloth seats. It might not be pretty to look at, but it gets the job done.

Windows Server 2012 R2 MinShell This is the best of both installation types mentioned previously. Minimum Shell (MinShell) gives you the advantage of using the GUI management tools, but MinShell does not actually install the GUI. It gives administrators the ability to use tools with which they are familiar but still provides a small attack surface and the advantages of Server Core.

In Windows Server 2012 R2, an administrator has the ability to remove the GUI shell after a GUI shell install has been completed. This removes Internet Explorer 10, Windows Explorer, the desktop, and the Start screen. Microsoft Management Console (MMC), Server Manager, and a subset of Control Panel are still present, giving you a MinShell installation plus PowerShell.



Real World Scenario

Server Core

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

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

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

Well, Windows Server 2012 R2 with the GUI is like regular hockey with a net, and Windows Server 2012 R2 Server Core is the Plexiglas version.

Server Core supports a limited number of roles.

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

- Volume Activation Services
- Web Server (IIS)
- Windows Deployment Services
- Windows Server Update Services
- .NET Framework 3.5 Features
- .NET Framework 4.5 Features
- Streaming Media Services
- Failover Clustering
- iSCSI
- Network Load Balancing
- MPIO
- qWave
- Telnet Server/Client
- Windows Server Migration Tools
- Windows PowerShell 4.0

Server Core does not have the normal Windows interface or GUI. Almost everything has to be configured via the command line or, in some cases, using the Remote Server Administration Tools from a full version of Windows Server 2012 R2. While this might scare off some administrators, it has the following benefits:

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

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

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

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

The prerequisites for Server Core are basic. It requires the Windows Server 2012 R2 installation media, a product key, and the hardware on which to install it.

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

One of the new things to keep in mind is that you can upgrade or downgrade to Server Core or MinShell. In Windows Server 2008 R2 and Windows Server 2008, if you wanted to switch your Windows Server GUI to Server Core, or vice versa, there was no way to convert to a full Windows Server installation or a Server Core installation without reinstalling the operating system. In Windows Server 2012 R2, the Server Core or GUI installation options are no longer an irreversible selection made during setup. An administrator now has the ability to convert between a Server Core installation and a full installation as needed.



Real World Scenario

Better Security

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

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

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

This is where Windows Server 2012 R2 Server Core can come into play. Since it is a slimmed-down version of Windows and there is no GUI, it makes it harder for anyone in the office to hack into the system. Also, Microsoft introduced a new domain controller in Windows Server 2008 called a *read-only domain controller (RODC)*. As its name suggests, it is a read-only version of a domain controller (explained in detail later in this book).

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

If you have a server that is running Server Core, there may be a situation in which you need to use the graphical user interfaces available only in Windows Server 2012 R2 with a GUI mode. Windows Server 2012 and Windows Server 2012 R2 allow you to switch the Server Core system to a Server with a GUI mode, or vice versa.

To convert from a Windows 2012 or Windows Server 2012 R2 Server Core system to Server with a GUI mode, run this code snippet (a restart is required):

```
Install-WindowsFeature Server-Gui-Mgmt-Infra,Server-Gui-Shell -Restart
```

To convert from Server Core mode to Server with a GUI mode, follow these steps when the server is initially installed in Server Core mode:

1. Determine the index number for a server with a GUI image (for example, SERVERDATA-CENTER, not SERVERDATACENTERCORE) using this cmdlet:

```
Get-WindowsImage -ImagePath path to wim\install.wim
```

2. Run this line of code:

```
Install-WindowsFeature Server-Gui-Mgmt-Infra,Server-Gui-Shell -Restart  
-Source wim: path to wim\install.wim: Index # from step 1
```

3. Alternatively, if you want to use Windows Update as the source instead of a WIM file, use this Windows PowerShell cmdlet:

```
Install-WindowsFeature Server-Gui-Mgmt-Infra,Server-Gui-Shell -Restart
```

After you have completed the management tasks, you can switch the server back to Server Core mode whenever it is convenient (a restart is required) with this Windows PowerShell cmdlet:

```
Uninstall-WindowsFeature Server-Gui-Mgmt-Infra -restart
```

NIC Teaming

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

To be able to use NIC Teaming, the computer system must have at least one Ethernet adapter. If you want to provide fault protection, an administrator must have a minimum of two Ethernet adapters. One advantage of Windows Server 2012 R2 is that an administrator can setup 32 network adapters in a NIC Team.

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

NIC Teaming gives an administrator the ability to allow a virtual machine to use virtual network adapters in Hyper-V. The advantage of using NIC Teaming in Hyper-V is that the administrator can use it to connect to more than one Hyper-V switch. This allows Hyper-V to maintain connectivity even if the network adapter under the Hyper-V switch gets disconnected.

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

Installing Windows Server 2012 R2

In the following sections, I am going to walk you through two different types of installs. I will show you how to do a full install of Windows 2012 Server with the GUI, and then I will show you how to install the Server Core version of the same software.



For these labs, I am using the full release of Windows Server 2012 R2 Datacenter, but you can use Windows Server 2012 R2 Standard.

Installing with the GUI

In Exercise 1.1, I will show you how to install Windows Server 2012 R2 Datacenter with the GUI. The GUI represents the Windows applications on the Desktop and the operating system functions that you can control and navigate with a mouse. The Server Core version is a command-line version only—you cannot use a mouse with Server Core unless you are going to use the mouse wheel for scrolling.

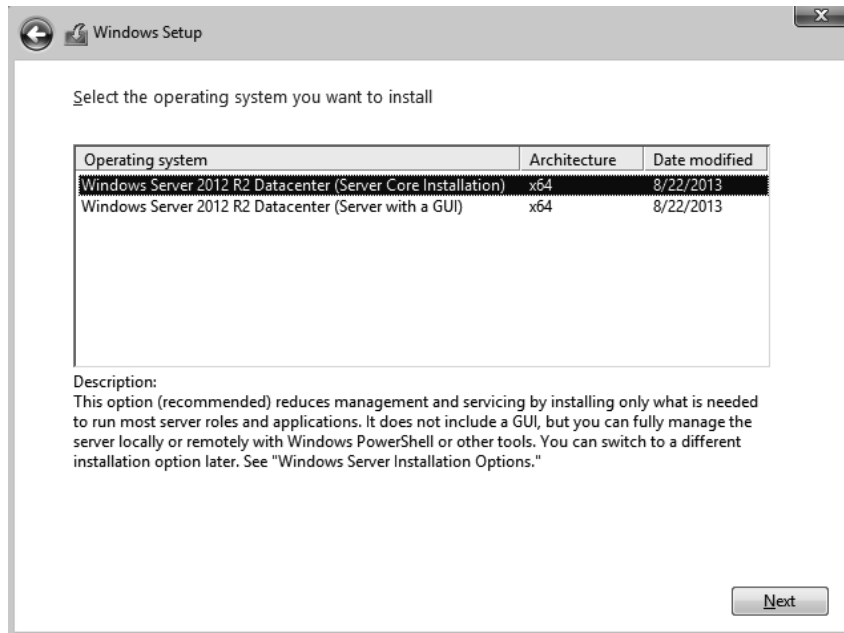
Windows Installation

At the time of this writing, I used the first full release of Windows Server 2012 R2 Datacenter. For this reason, there may be screens that have changed somewhat since this book was published.

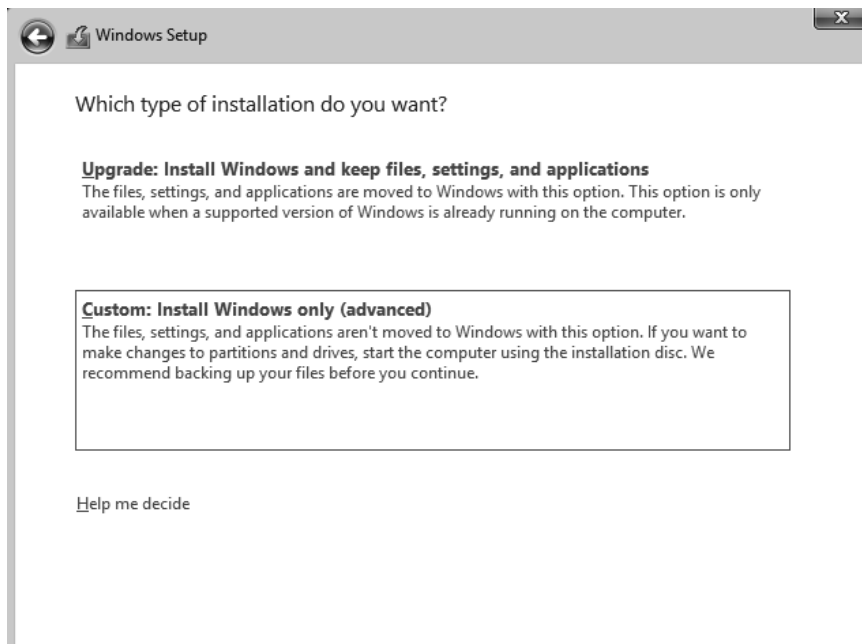
EXERCISE 1.1

Installing Windows Server 2012 R2 with the GUI

1. Insert the Windows Server 2012 R2 installation DVD, and restart the machine from the installation media.
2. At the first screen, Windows Server 2012 R2 will ask you to configure your language, time and currency, and keyboard. Make your selections, and click Next.
3. At the next screen, click Install Now.
4. Depending on what version of Windows Server 2012 R2 you have (MSDN, TechNet, and so on), you may be asked to enter a product key. If this screen appears, enter your product key and click Next. If this screen does not appear, just go to step 5.
5. The Select The Operating System That You Want To Install screen then appears. Choose the Windows Server 2012 R2 Datacenter (Server With A GUI) selection and click Next.



6. The license terms screen appears. After reading the Windows Server 2012 R2 license agreement, check the I Accept The License Terms check box and click Next.
7. On the Which Type Of Installation Do You Want? screen, choose Custom: Install Windows Only (Advanced).



EXERCISE 1.1 (continued)

8. The next screen will ask you where you want to install Windows. If your hard disk is already formatted as NTFS, click the drive and then click Next. If the hard disk is not yet set up or formatted, choose the New link and create a partition. After creating the partition, click the Format link. Once the format is done, make sure you choose the new partition and click Next.
 9. The Installing Windows screen will appear next. This is where the files from your media will be installed onto the system. The machine will reboot during this installation.
 10. After the machine is finished rebooting, a screen requesting the administrator password will appear. Type in your password. (**P@ssword** is used in this exercise.) Your password must meet the password complexity requirements (one capitalized letter, one number, and/or one special character). Click Finish.
 11. Next, log into the system. Press Ctrl+Alt+Del, and type in the administrator password. The machine will set up the properties of the administrator account.
 12. Notice that the Server Manager dashboard automatically appears. Your Windows Server 2012 R2 installation is now complete.
 13. Close Server Manager.
-

After you have logged into the Windows Server 2012 R2 Datacenter system, you will notice some big changes. The first is that the Start button in the lower-left corner of the screen has changed its look. Also, you can get to a Start button by clicking the Windows key (see Figure 1.2).

FIGURE 1.2 Windows key on a standard keyboard



Installing Windows Server 2012 R2 Server Core

In Exercise 1.2, you will learn how to install Windows Server 2012 R2 Server Core. You'll notice that the steps are similar to the ones in Exercise 1.1, with a couple of exceptions. As mentioned earlier, Server Core is a command-line configuration of Windows Server 2012 R2.

EXERCISE 1.2**Installing Windows Server 2012 R2 Using Server Core**

1. Insert the Windows Server 2012 R2 installation DVD, and restart the machine from the installation media.
 2. At the first screen, Windows Server 2012 R2 will prompt you to configure your language, time and currency, and keyboard. Make your selections, and click Next.
 3. At the next screen, click Install Now.
 4. Depending on what version of Windows Server 2012 R2 you have (MSDN, TechNet, and so on), you may be asked to enter a product key. If this screen appears, enter your product key and click Next. If this screen does not appear, just go to step 5.
 5. The Select The Operating System That You Want To Install screen then appears. Choose the Windows Server 2012 R2 Datacenter (Server Core Installation) selection and click Next.
 6. The license terms screen appears. After reading the Windows Server 2012 R2 license agreement, check the I Accept The License Terms check box and click Next.
 7. At the Which Type Of Installation Do You Want? screen, choose Custom: Install Windows Only (Advanced).
 8. The next screen will ask you where you want to install Windows. If your hard disk is already formatted as NTFS, click the drive and then click Next. If the hard disk is not set up or formatted, choose the New link and create a partition. After creating the partition, click the Format link. Once the format is done, make sure you choose the new partition and click Next.
 9. The Installing Windows screen will appear next. This is where the files from your media will be installed onto the system. The machine will reboot during this installation.
 10. After the machine is finished rebooting, a screen requesting the administrator password will appear. Type in your password. (**P@ssword** is used in this exercise.) Your password must meet the password complexity requirements (one capitalized letter, one number, and/or one special character).
 11. Log into the system. Press Ctrl+Alt+Del, and type in the administrator password. The machine will set up the properties of the administrator account.
 12. You will notice that the command prompt will automatically appear. Your Windows Server 2012 R2 Server Core installation is now complete.
 13. To log out or turn off the machine, press Ctrl+Alt+Del and then click Sign Out.
-

After Windows Server 2012 R2 server is installed, you need to look at how to manage and configure the server. In the next section, you will learn how to manage a server remotely and with Windows PowerShell.

Using Windows Deployment Services

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

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

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

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

1. The WDS client initiates a special boot process through the PXE network adapter (and the computer's BIOS configured for a network boot). On a PXE client, the user presses F12 to start the PXE boot process and to indicate that they want to perform a WDS installation.
2. A list of available Windows PE boot images is displayed. The user should select the appropriate Windows PE boot image from the boot menu.
3. The Windows Welcome screen is displayed. The user should click the Next button.
4. The WDS user is prompted to enter credentials for accessing and installing images from the WDS server.
5. A list of available operating system images is displayed. The user should select the appropriate image file to install.
6. The WDS user is prompted to enter the product key for the selected image.
7. The Partition And Configure The Disk screen is displayed. This screen provides the ability to install a mass storage device driver, if needed, by pressing F6.
8. The image copy process is initiated, and the selected image is copied to the WDS client computer.

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

Preparing the WDS Server

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

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

1. Make sure that the server meets the requirements for running WDS.
2. Install WDS.
3. Configure and start WDS.
4. Configure the WDS server to respond to client computers (if this was not configured when WDS was installed).

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

WDS Server Requirements

The WDS server must meet these requirements:

- The computer must be a domain controller or a member of an Active Directory domain.
- At least one partition on the server must be formatted as NTFS.
- WDS must be installed on the server.
- The operating system must be Windows Server 2003, Windows Server 2008/2008 R2, Windows Server 2012, or Windows Server 2012 R2.
- A network adapter must be installed.

Network Services

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

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

Installing the WDS Server Components

You can configure WDS on a Windows Server 2003/2008/2008 R2, Windows Server 2012, or Windows Server 2012 R2 computer by using the Windows Deployment Services Configuration Wizard or by using the WDSUTIL command-line utility. Table 1.3 describes the WDSUTIL command-line options.

TABLE 1.3 WDSUTIL command-line options

WDSUTIL Option	Description
/initialize-server	Initializes the configuration of the WDS server
/uninitialized-server	Undoes any changes made during the initialization of the WDS server
/add	Adds images and devices to the WDS server
/convert-ripimage	Converts Remote Installation Preparation (RIPrep) images to WIM images
/remove	Removes images from the server
/set	Sets information in images, image groups, WDS servers, and WDS devices
/get	Gets information from images, image groups, WDS servers, and WDS devices
/new	Creates new capture images or discover images
/copy- image	Copies images from the image store
/export-image	Exports to WIM files images contained within the image store
/start	Starts WDS services
/stop	Stops WDS services
/disable	Disables WDS services
/enable	Enables WDS services
/approve-autoadddevices	Approves Auto-Add devices
/reject-autoadddevices	Rejects Auto-Add devices
/delete-autoadddevices	Deletes records from the Auto-Add database
/update	Uses a known good resource to update a server resource

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

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

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

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

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

Preparing the WDS Client

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

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

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

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

1. Start the computer. When prompted, press F12 for a network service boot. The Windows PE appears.
2. The Windows Welcome screen appears. Click the Next button to start the installation process.
3. Enter the username and password of an account that has permissions to access and install images from the WDS server.
4. A list of available operating system images stored on the WDS server appears. Select the image to install and click Next.
5. Enter the product key for the selected Windows 7/8 image and click Next.
6. The Partition And Configure The Disk screen appears. Select the desired disk-partitioning options, or click OK to use the default options.
7. Click Next to initiate the image-copying process. The Windows Setup process will begin after the image is copied to the WDS client computer.

Understanding Features On Demand

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

Features On Demand in Windows Server 2012 R2 solves this issue because not only can administrators disable a role or feature, they can also completely remove the role or feature's files.

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

If you want to remove a role or feature completely from the system, use `-Remove` with the `Uninstall-WindowsFeature` cmdlet of Windows PowerShell. For example, if you want to remove Windows Explorer, Internet Explorer, and all dependent components completely, run the following Windows PowerShell command:

```
Uninstall-WindowsFeature Server-Gui-Shell -Remove
```

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

When you're using the Features On Demand configuration, if feature files are not available on the server computer and the installation requires those feature files, Windows Server 2012 R2 can be directed to get those files from a side-by-side feature store, which is a shared folder that contains feature files. It is available to the server on the network, from Windows Update, or from installation media. This can be overwritten using the `-Source` option in the Windows PowerShell utility.

Source Files for Roles or Features

Offline virtual hard disks (VHDs) cannot be used as a source for installing roles or features that have been completely removed. Only sources for the same version of Windows Server 2012 R2 are supported.

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

1. Run the following command:

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

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

2. Run the following command:

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

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

To add or remove a role or feature, you must have administrative rights to the Windows Server 2012 R2 machine.

Storage in Windows Server 2012 R2

As an IT administrator, you'll need to ask many questions before you start setting up a server. What type of disks should be used? What type of RAID sets should be made? What type of hardware platform should be purchased? These are all questions you must ask when planning for storage in a Windows Server 2012 R2 server. In the following sections, I will answer these questions so that you can make the best decisions for storage in your network's environment.

Initializing Disks

To begin, I must first discuss how to add disk drives to a server. Once a disk drive has been physically installed, it must be initialized by selecting the type of partition. Different types of partition styles are used to initialize disks: *Master Boot Record (MBR)* and *GUID Partition Table (GPT)*.

MBR has a partition table that indicates where the partitions are located on the disk drive, and with this particular partition style, only volumes up to 2TB (2,048GB) are supported. An MBR drive can have up to four primary partitions or can have three primary partitions and one extended partition that can be divided into unlimited logical drives.

Windows Server 2012 R2 can only boot off an MBR disk unless it is based on the Extensible Firmware Interface (EFI); then it can boot from GPT. An Itanium server is an example of an EFI-based system. GPT is not constrained by the same limitations as MBR. In fact, a GPT disk drive can support volumes of up to 18EB (18,874,368 million terabytes) and 128 partitions. As a result, GPT is recommended for disks larger than 2TB or disks used on Itanium-based computers. Exercise 1.3 demonstrates the process of initializing additional disk drives to an active computer running Windows Server 2012 R2. If you're not adding a new drive, then stop after step 4. I am completing this exercise using Computer Management, but you also can do this exercise using Server Manager.

EXERCISE 1.3**Initializing Disk Drives**

1. Open Computer Management under Administrative Tools.
2. Select Disk Management.
3. After disk drives have been installed, right-click Disk Management and select Rescan Disks.
4. A pop-up box appears indicating that the server is scanning for new disks. If you did not add a new disk, go to step 9.
5. After the server has completed the scan, the new disk appears as Unknown.
6. Right-click the Unknown disk, and select Initialize Disk.
7. A pop-up box appears asking for the partition style. For this exercise, choose MBR.
8. Click OK.
9. Close Computer Management.

The disk will now appear online as a basic disk with unallocated space.

Configuring Basic and Dynamic Disks

Windows Server 2012 R2 supports two types of disk configurations: basic and dynamic. Basic disks are divided into partitions and can be used with previous versions of Windows. Dynamic disks are divided into volumes and can be used with Windows 2000 Server and newer releases.

When a disk is initialized, it is automatically created as a basic disk, but when a new fault-tolerant (RAID) volume set is created, the disks in the set are converted to dynamic disks. Fault-tolerance features and the ability to modify disks without having to reboot the server are what distinguish dynamic disks from basic disks.



Fault tolerance (RAID) is discussed in detail later in this chapter in the “Redundant Array of Independent Disks” section.

A basic disk can simply be converted to a dynamic disk without loss of data. When a basic disk is converted, the partitions are automatically changed to the appropriate volumes. However, converting a dynamic disk back to a basic disk is not as simple. First, all the data on the dynamic disk must be backed up or moved. Then, all the volumes on the dynamic disk have to be deleted. The dynamic disk can then be converted to a basic disk. Partitions and logical drives can be created, and the data can be restored.

The following are actions that can be performed on basic disks:

- Formatting partitions
- Marking partitions as active
- Creating and deleting primary and extended partitions
- Creating and deleting logical drives
- Converting from a basic disk to a dynamic disk

The following are actions that can be performed on dynamic disks:

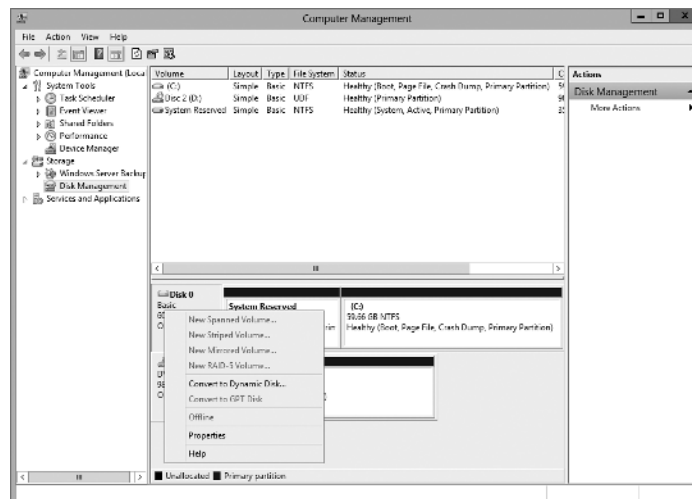
- Creating and deleting simple, striped, spanned, mirrored, or RAID-5 volumes
- Removing or breaking a mirrored volume
- Extending simple or spanned volumes
- Repairing mirrored or RAID-5 volumes
- Converting from a dynamic disk to a basic disk after deleting all volumes

In Exercise 1.4, you'll convert a basic disk to a dynamic disk.

EXERCISE 1.4

Converting a Basic Disk to a Dynamic Disk

1. Open Computer Management under Administrative Tools.
2. Select Disk Management.
3. Right-click a basic disk that you want to convert and select Convert To Dynamic Disk.



EXERCISE 1.4 (continued)

4. The Convert To Dynamic Disk dialog box appears. From here, select all of the disks that you want to convert to dynamic disks. In this exercise, only one disk will be converted.
5. Click OK.
6. The Convert To Dynamic Disk dialog box changes to the Disks To Convert dialog box and shows the disk/disks that will be converted to dynamic disks.
7. Click Convert.
8. Disk Management will warn that if you convert the disk to dynamic, you will not be able to start the installed operating system from any volume on the disk (except the current boot volume). Click Yes.
9. Close Computer Management.

The converted disk will now show as Dynamic in Disk Management.

Managing Volumes

A *volume set* is created from volumes that span multiple drives by using the free space from those drives to construct what will appear to be a single drive. The following list includes the various types of volume sets and their definitions:

- *Simple volume* uses only one disk or a portion of a disk.
- *Spanned volume* is a simple volume that spans multiple disks, with a maximum of 32. Use a spanned volume if the volume needs are too great for a single disk.
- *Striped volume* stores data in stripes across two or more disks. A striped volume gives you fast access to data but is not fault tolerant, nor can it be extended or mirrored. If one disk in the striped set fails, the entire volume fails.
- *Mirrored volume* duplicates data across two disks. This type of volume is fault tolerant because if one drive fails, the data on the other disk is unaffected.
- *RAID-5 volume* stores data in stripes across three or more disks. This type of volume is fault tolerant because if a drive fails, the data can be re-created from the parity off of the remaining disk drives. Operating system files and boot files cannot reside on the RAID-5 disks.

Exercise 1.5 illustrates the procedure for creating a volume set.

EXERCISE 1.5

Creating a Volume Set

1. Open Computer Management under Administrative Tools.
2. Select Disk Management.

3. Select and right-click a disk that has unallocated space. If there are no disk drives available for a particular volume set, that volume set will be grayed out as a selectable option. In this exercise, you'll choose a spanned volume set, but the process after the volume set selection is the same regardless of which kind you choose. The only thing that differs is the number of disk drives chosen.
4. The Welcome page of the New Spanned Volume Wizard appears and explains the type of volume set chosen. Click Next.
5. The Select Disks page appears. Select the disk that will be included with the volume set and click Add. Repeat this process until all of the desired disks have been added. Click Next.
6. The Assign Drive Letter Or Path page appears. From here you can select the desired drive letter for the volume, mount the volume in an empty NTFS folder, or choose not to assign a drive letter. The new volume is labeled as E. Click Next.
7. The Format Volume page appears. Choose to format the new volume. Click Next.
8. Click Finish.
9. If the disks have not been converted to dynamic, you will be asked to convert the disks. Click Yes.

The new volume will appear as a healthy spanned dynamic volume with the new available disk space of the new volume set.

Storage Spaces in Windows Server 2012 R2

Windows Server 2012 R2 includes a technology called *Storage Spaces*. Windows Server 2012 R2 allows an administrator to virtualize storage by grouping disks into storage pools. These storage pools can then be turned into virtual disks called *storage spaces*.

The Storage Spaces technology allows an administrator to have a highly available, scalable, low-cost, and flexible solution for both physical and virtual installations. Storage Spaces allows you to set up this advantage on either a single server or in scalable multinode mode. So, before going any further, let's look at these two terms that you must understand.

Storage Pools *Storage pools* are a group of physical disks that allows an administrator to delegate administration, expand disk sizes, and group disks together.

Storage Spaces *Storage spaces* allow an administrator to take free space from storage pools and create virtual disks called storage spaces. Storage spaces give administrators the ability to have precise control, resiliency, and storage tiers.

Storage spaces and storage pools can be managed by an administrator through the use of the Windows Storage Management API, Server Manager, or Windows PowerShell.

One of the advantages of using the Storage Spaces technology is the ability to set up resiliency. There are three types of Storage Space resiliency: mirror, parity, and simple (no resiliency).



Fault tolerance (RAID) is discussed in detail in the “Redundant Array of Independent Disks” section.

Now that you understand what storage spaces and storage pools do, let’s take a look at some of the other advantages of using these features in Windows Server 2012 R2.

Availability One advantage to the Storage Spaces technology is the ability to fully integrate the storage space with failover clustering. This advantage allows administrators to achieve service deployments that are continuously available. Administrators have the ability to set up storage pools to be clustered across multiple nodes within a single cluster.

Tiered Storage The Storage Spaces technology allows virtual disks to be created with a two-tier storage setup. For data that is used often, you have an SSD tier; for data that is not used often, you use an HDD tier. The Storage Spaces technology will automatically transfer data at a subfile level between the two different tiers based on how often the data is used. Because of tiered storage, performance is greatly increased for data that is used most often, and data that is not used often still gets the advantage of being stored on a low-cost storage option.

Delegation One advantage of using storage pools is that administrators have the ability to control access by using access control lists (ACLs). What is nice about this advantage is that each storage pool can have its own unique access control lists. Storage pools are fully integrated with Active Directory Domain Services.

Redundant Array of Independent Disks

The ability to support drive sets and arrays using *Redundant Array of Independent Disks (RAID)* technology is built into Windows Server 2012 R2. RAID can be used to enhance data performance, or it can be used to provide fault tolerance to maintain data integrity in case of a hard disk failure. Windows Server 2012 R2 supports three types of RAID technologies: RAID-0, RAID-1, and RAID-5.

RAID-0 (Disk Striping) *Disk striping* is using two or more volumes on independent disks created as a single striped set. There can be a maximum of 32 disks. In a striped set, data is divided into blocks that are distributed sequentially across all of the drives in the set. With RAID-0 disk striping, you get very fast read and write performance because multiple blocks of data can be accessed from multiple drives simultaneously. However, RAID-0 does not offer the ability to maintain data integrity during a single disk failure. In other words, RAID-0 is not fault tolerant; a single disk event will cause the entire striped set to be lost, and it will have to be re-created through some type of recovery process, such as a tape backup.

RAID-1 (Disk Mirroring) *Disk mirroring* is two logical volumes on two separate identical disks created as a duplicate disk set. Data is written on two disks at the same time; that way, in the event of a disk failure, data integrity is maintained and available. Although this fault tolerance gives administrators data redundancy, it comes with a price because it

diminishes the amount of available storage space by half. For example, if an administrator wants to create a 300GB mirrored set, they would have to install two 300GB hard drives into the server, thus doubling the cost for the same available space.

RAID-5 Volume (Disk Striping with Parity) With a RAID-5 volume, you have the ability to use a minimum of three disks and a maximum of 32 disks. RAID-5 volumes allow data to be striped across all of the disks with an additional block of error-correction called parity. *Parity* is used to reconstruct the data in the event of a disk failure. RAID-5 has slower write performance than the other RAID types because the OS must calculate the parity information for each stripe that is written, but the read performance is equivalent to a stripe set, RAID-0, because the parity information is not read. Like RAID-1, RAID-5 comes with additional cost considerations. For every RAID-5 set, roughly an entire hard disk is consumed for storing the parity information. For example, a minimum RAID-5 set requires three hard disks, and if those disks are 300GB each, approximately 600GB of disk space is available to the OS and 300GB is consumed by parity information, which equates to 33.3 percent of the available space. Similarly, in a five-disk RAID-5 set of 300GB disks, approximately 1,200GB of disk space is available to the OS, which means that 20 percent of the total available space is consumed by the parity information. The words *roughly* and *approximately* are used when calculating disk space because a 300GB disk will really be only about 279GB of space. This is because vendors define a gigabyte as 1 billion bytes, but the OS defines it as 2^{30} (1,073,741,824) bytes. Also, remember that file systems and volume managers have overhead as well.



Software RAID is a nice option for a small company, but hardware RAID is definitely a better option if the money is available.

Table 1.4 breaks down the various aspects of the supported RAID types in Window Server 2012 R2.

TABLE 1.4 Supported RAID-level properties in Windows Server 2012 R2

RAID Level	RAID Type	Fault Tolerant	Advantages	Minimum Number of Disks	Maximum Number of Disks
0	Disk striping	No	Fast reads and writes	2	32
1	Disk mirroring	Yes	Data redundancy and faster writes than RAID-5	2	2
5	Disk striping with parity	Yes	Data redundancy with less overhead and faster reads than RAID-1	3	32

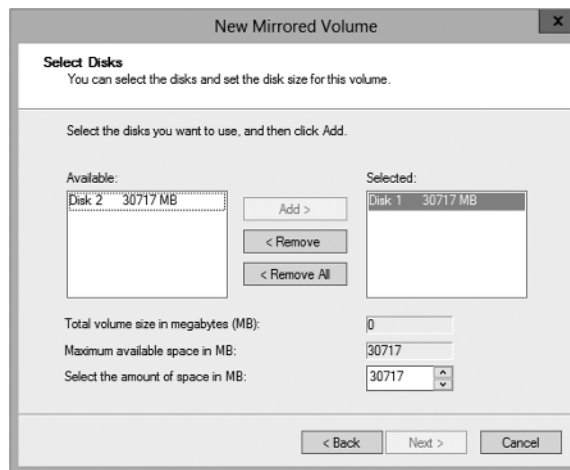
Creating RAID Sets

Now that you understand the concepts of RAID and how to use it, you can look at the creation of RAID sets in Windows Server 2012 R2. The process of creating a RAID set is the same as the process for creating a simple or spanned volume set, except for the minimum disk requirements associated with each RAID type.

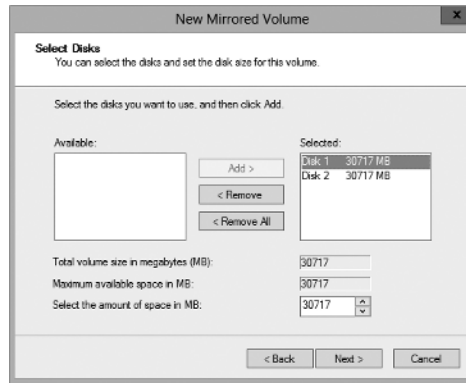
Creating a mirrored volume set is basically the same as creating a volume set, as shown in Exercise 1.6, except that you will select New Mirrored Volume. It is after the disk select wizard appears that you'll begin to see the difference. Since a new mirrored volume is being created, the volume requires two disks.

During the disk select process, if only one disk is selected, the Next button will be unavailable because the disk minimum has not been met. Refer to Figure 1.3 to view the Select Disks page of the New Mirrored Volume Wizard during the creation of a new mirrored volume, and notice that the Next button is not available.

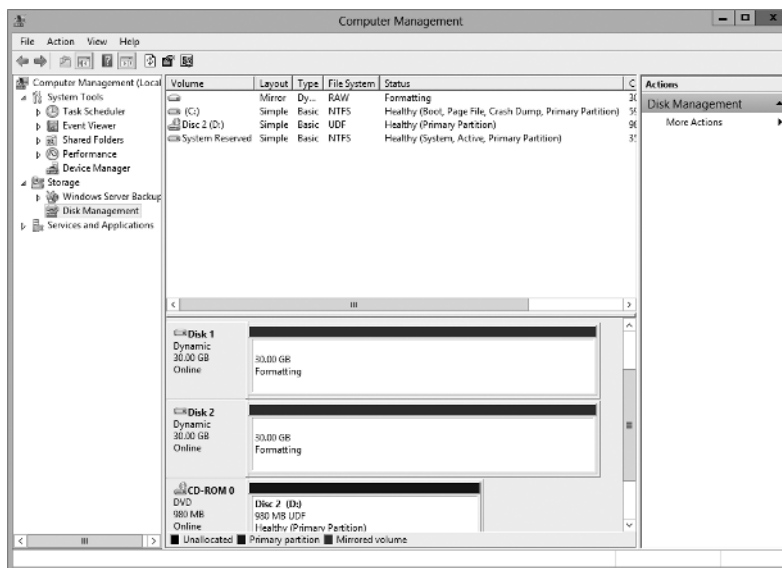
FIGURE 1.3 Select Disks page of the New Mirrored Volume Wizard



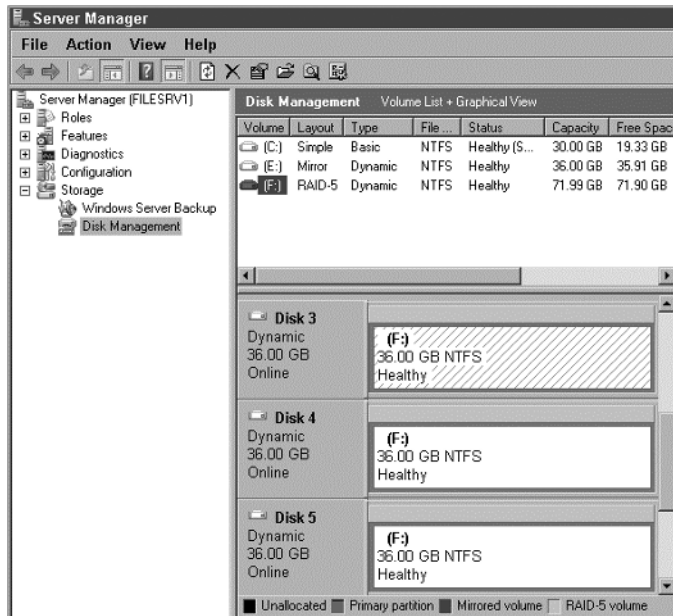
To complete the process, you must select a second disk by highlighting the appropriate disk and adding it to the volume set. Once the second disk has been added, the Add button becomes unavailable, and the Next button is available to complete the mirrored volume set creation (see Figure 1.4).

FIGURE 1.4 Adding the second disk to complete a mirrored volume set

After you click Next, the creation of the mirrored volume set is again just like the rest of the steps in Exercise 1.5. A drive letter will have to be assigned, and the volume will need to be formatted. The new mirrored volume set will appear in Disk Management. In Figure 1.5, notice that the capacity of the volume equals one disk even though two disks have been selected.

FIGURE 1.5 Newly created mirrored volume set

To create a RAID-5 volume set, you use the same process that you use to create a mirrored volume set. The only difference is that a RAID-5 volume set requires that a minimum of three disks be selected to complete the volume creation. The process is simple: Select New RAID-5 Volume, select the three disks that will be used in the volume set, assign a drive letter, and format the volume. Figure 1.6 shows a newly created RAID-5 volume set in Disk Management.

FIGURE 1.6 Newly created RAID-5 volume set

Mount Points

With the ever-increasing demands of storage, mount points are used to surpass the limitation of 26 drive letters and to join two volumes into a folder on a separate physical disk drive. A *mount point* allows you to configure a volume to be accessed from a folder on another existing disk.

Through Disk Management, a mount point folder can be assigned to a drive instead of using a drive letter, and it can be used on basic or dynamic volumes that are formatted with NTFS. However, mount point folders can be created only on empty folders within a volume. Additionally, mount point folder paths cannot be modified; they can be removed only once they have been created. Exercise 1.6 shows the steps to create a mount point.

EXERCISE 1.6

Creating Mount Points

1. Open Server Manager.
2. Click and then expand Storage.
3. Select Disk Management.

4. Right-click the volume where the mount point folder will be assigned, and select Change Drive Letter And Paths.
5. Click Add.
6. Either type the path to an empty folder on an NTFS volume or click Browse to select or make a new folder for the mount point.

When you explore the drive, you'll see the new folder created. Notice that the icon indicates that it is a mount point.

Microsoft MPIO

Multipath I/O (MPIO) is associated with high availability because a computer will be able to use a solution with redundant physical paths connected to a storage device. Thus, if one path fails, an application will continue to run because it can access the data across the other path.

The MPIO software provides the functionality needed for the computer to take advantage of the redundant storage paths. MPIO solutions can also load-balance data traffic across both paths to the storage device, virtually eliminating bandwidth bottlenecks to the computer. What allows MPIO to provide this functionality is the new native *Microsoft Device Specific Module (Microsoft DSM)*. The Microsoft DSM is a driver that communicates with storage devices—iSCSI, Fibre Channel, or SAS—and it provides the chosen load-balancing policies. Windows Server 2012 R2 supports the following load-balancing policies:

Failover In a failover configuration, there is no load balancing. There is a primary path that is established for all requests and subsequent standby paths. If the primary path fails, one of the standby paths will be used.

Failback This is similar to failover in that it has primary and standby paths. However, with failback you designate a preferred path that will handle all process requests until it fails, after which the standby path will become active until the primary reestablishes a connection and automatically regains control.

Round Robin In a round-robin configuration, all available paths will be active and will be used to distribute I/O in a balanced round-robin fashion.

Round Robin with a Subset of Paths In this configuration, a specific set of paths will be designated as a primary set and another as standby paths. All I/O will use the primary set of paths in a round-robin fashion until all of the sets fail. Only at this time will the standby paths become active.

Dynamic Least Queue Depth In a dynamic least queue depth configuration, I/O will route to the path with the least number of outstanding requests.

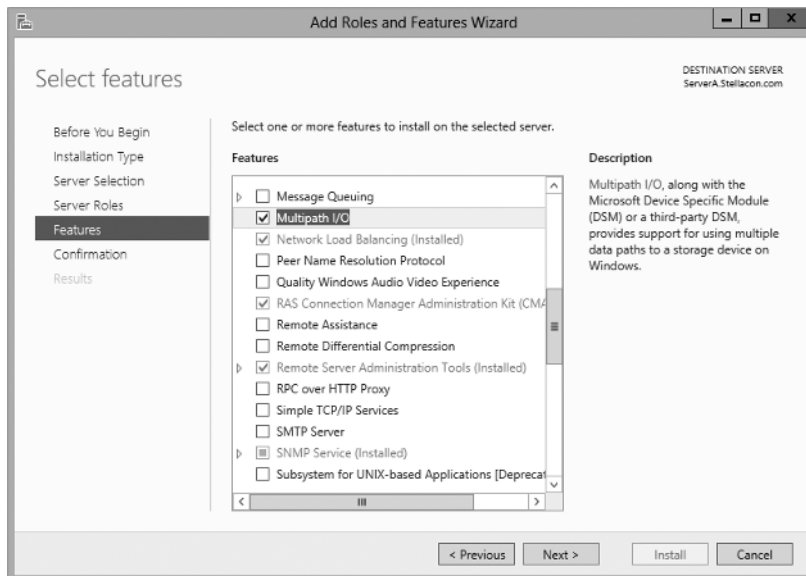
Weighted Path In a weighted path configuration, paths are assigned a numbered weight. I/O requests will use the path with the least weight—the higher the number, the lower the priority.

Exercise 1.7 demonstrates the process of installing the Microsoft MPIO feature for Windows Server 2012 R2.

EXERCISE 1.7

Installing Microsoft MPIO

1. Choose Server Manager by clicking the Server Manager icon on the Taskbar.
2. Click number 2, Add Roles And Features.
3. Choose role-based or feature-based installation and click Next.
4. Choose your server and click Next.
5. Click Next on the Roles screen.
6. On the Select Features screen, choose the Multipath I/O check box. Click Next.

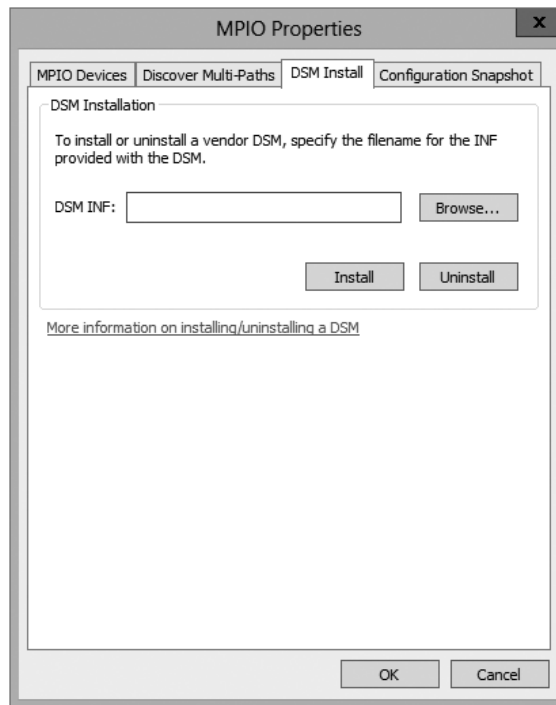


7. On the Confirm Installation Selections page, verify that Multipath I/O is the feature that will be installed. Click Install.
8. After the installation completes, the Installation Results page appears stating that the server must be rebooted to finish the installation process.
9. Click Close.
10. Restart the system.

Typically, most storage arrays work with the Microsoft DSM. However, some hardware vendors require DSM software that is specific to their products. Third-party DSM software is installed through the MPIO utility as follows:

1. Open Administrative Tools > MPIO.
2. Select the DSM Install tab (see Figure 1.7).

FIGURE 1.7 The DSM Install tab in the MPIO Properties dialog box



3. Add the path of the INF file and click Install.

iSCSI

Internet Small Computer System Interface (iSCSI) is an interconnect protocol used to establish and manage a connection between a computer (initiator) and a storage device (target). It does this by using a connection through TCP port 3260, which allows it to be used over a LAN, a WAN, or the Internet. Each initiator is identified by its iSCSI Qualified Name (iqn), and it is used to establish its connection to an iSCSI target.

iSCSI was developed to allow block-level access to a storage device over a network. This is different from using a network attached storage (NAS) device that connects through the use of Common Internet File System (CIFS) or Network File System (NFS).

Block-level access is important to many applications that require direct access to storage. Microsoft Exchange and Microsoft SQL are examples of applications that require direct access to storage.

By being able to leverage the existing network infrastructure, iSCSI was also developed as an alternative to Fibre Channel storage by alleviating the additional hardware costs associated with a Fibre Channel storage solution.

iSCSI also has another advantage over Fibre Channel in that it can provide security for the storage devices. iSCSI can use Challenge Handshake Authentication Protocol (CHAP or MS-CHAP) for authentication and Internet Protocol Security (IPsec) for encryption. Windows Server 2012 R2 is able to connect an iSCSI storage device out of the box with no additional software needing to be installed. This is because the Microsoft iSCSI initiator is built into the operating system.

Windows Server 2012 R2 supports two different ways to initiate an iSCSI session.

- Through the native Microsoft iSCSI software initiator that resides on Windows Server 2012 R2
- Using a hardware iSCSI host bus adapter (HBA) that is installed in the computer

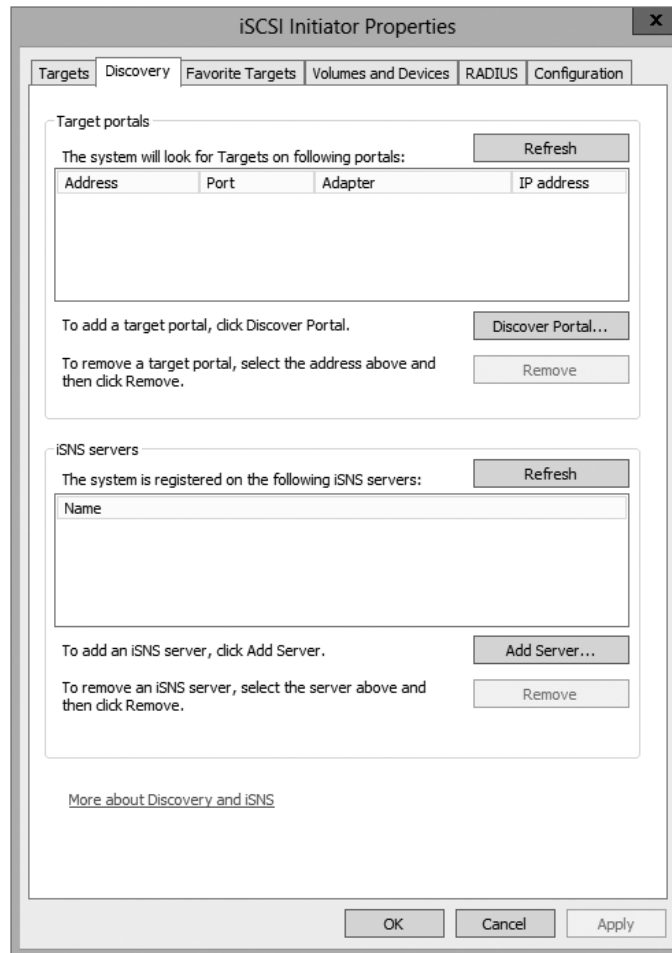
Both the Microsoft iSCSI software initiator and iSCSI HBA present an iSCSI qualified name that identifies the host initiator. When the Microsoft iSCSI software initiator is used, the CPU utilization may be as much as 30 percent higher than on a computer with a hardware iSCSI HBA. This is because all of the iSCSI process requests are handled within the operating system. Using a hardware iSCSI HBA, process requests can be offloaded to the adapter, thus freeing the CPU overhead associated with the Microsoft iSCSI software initiator. However, iSCSI HBAs can be expensive, whereas the Microsoft iSCSI software initiator is free.

It is worthwhile to install the Microsoft iSCSI software initiator and perform load testing to see how much overhead the computer will have prior to purchasing an iSCSI HBA or HBAs, depending on the redundancy level. Exercise 1.8 explains how to install and configure an iSCSI connection.

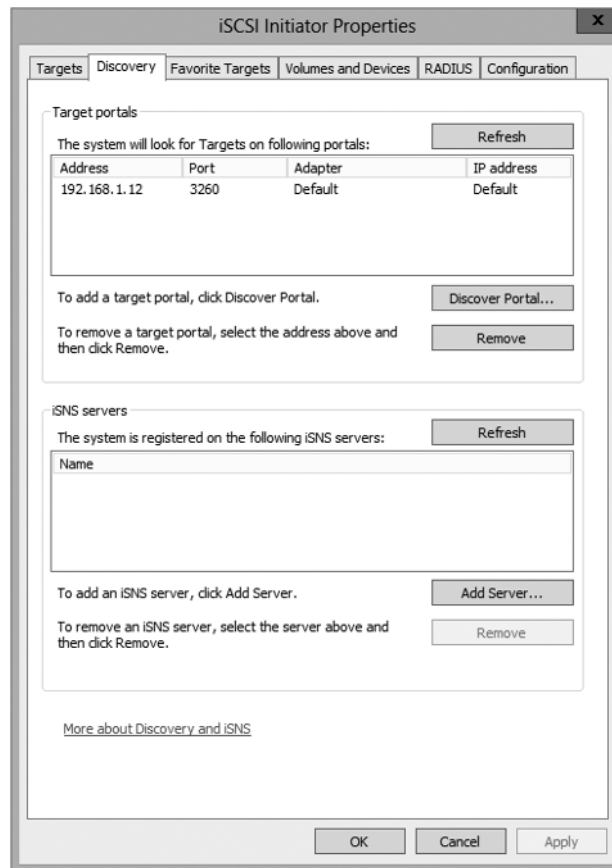
EXERCISE 1.8

Configuring iSCSI Storage Connection

1. Click the Windows key or Start button in the left-hand corner > Administrative Tools > iSCSI Initiator.
2. If a dialog box appears, click Yes to start the service.
3. Click the Discovery tab.



4. In the Target Portals portion of the page, click Discover Portal.
5. Enter the IP address of the target portal and click OK.

EXERCISE 1.8 (continued)

6. The IP address of the target portal appears in the Target Portals box.

7. Click OK.

To use the storage that has now been presented to the server, you must create a volume on it and format the space. Refer to Exercise 1.3 to review this process.

Internet Storage Name Service

Internet Storage Name Service (iSNS) allows for central registration of an iSCSI environment because it automatically discovers available targets on the network. The purpose of iSNS is to help find available targets on a large iSCSI network.

The Microsoft iSCSI initiator includes an iSNS client that is used to register with the iSNS. The iSNS feature maintains a database of clients that it has registered either through DHCP discovery or through manual registration. iSNS DHCP is available after the

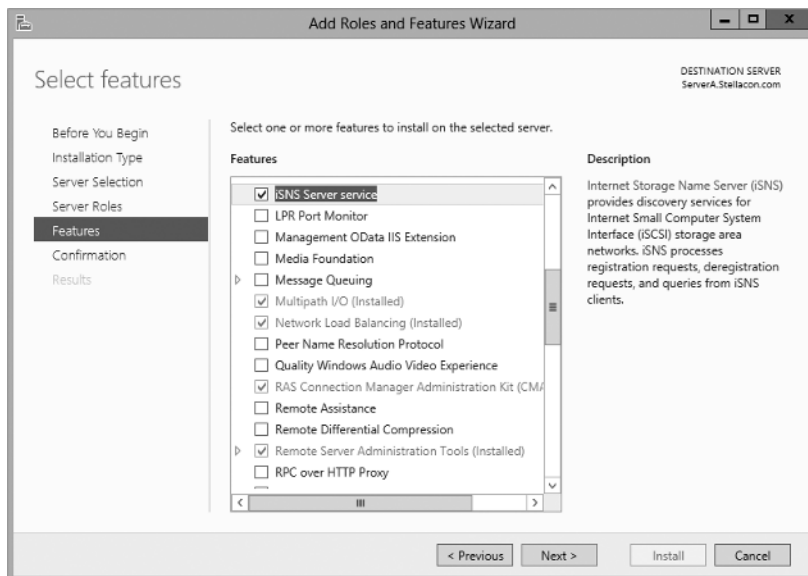
installation of the service, and it is used to allow iSNS clients to discover the location of the iSNS. However, if iSNS DHCP is not configured, iSNS clients must be registered manually with the `iscsicli` command.

To execute the command, launch a command prompt on a computer hosting the Microsoft iSCSI and type `iscsicli addisnsserver server_name`, where `server_name` is the name of the computer hosting iSNS. Exercise 1.9 walks you through the steps required to install the iSNS feature on Windows Server 2012 R2, and then it explains the different tabs in iSNS.

EXERCISE 1.9

Installing the iSNS Feature on Windows Server 2012 R2

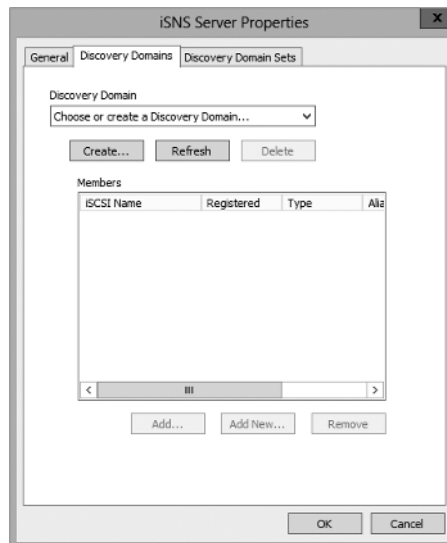
1. Choose Server Manager by clicking the Server Manager icon on the Taskbar.
2. Click number 2 > Add Roles And Features.
3. Choose role-based or featured-based installation and click Next.
4. Choose your server and click Next.
5. Click Next on the Roles screen.
6. On the Select Features screen, choose the iSNS Server Service check box. Click Next.



7. On the Confirmation screen, click the Install button.
8. Click the Close button. Close Server Manager and reboot.
9. Log in and open the iSNS server under Administrative Tools.

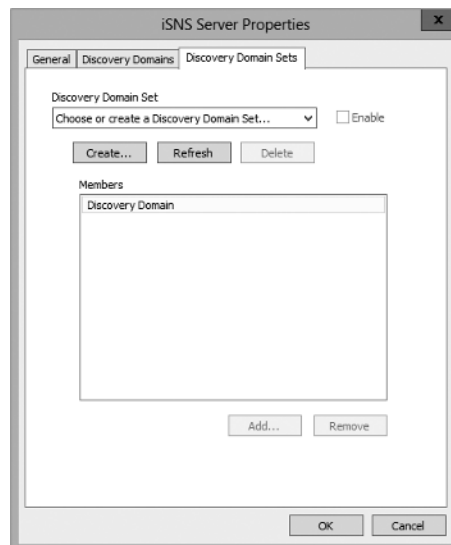
EXERCISE 1.9 (continued)

10. Click the General tab. This tab displays the list of registered initiators and targets. In addition to their iSCSI qualified name, it lists storage node type (Target or Initiator), alias string, and entity identifier (the Fully Qualified Domain Name [FQDN] of the machine hosting the iSNS client).
11. Click the Discovery Domains tab. The purpose of Discovery Domains is to provide a way to separate and group nodes. This is similar to zoning in Fibre Channel. The following options are available on the Discovery Domains tab:
 - *Create* is used to create a new discovery domain.
 - *Refresh* is used to repopulate the Discovery Domain drop-down list.
 - *Delete* is used to delete the currently selected discovery domain.
 - *Add* is used to add nodes that are already registered in iSNS to the currently selected discovery domain.
 - *Add New* is used to add nodes by entering the iSCSI Qualified Name (iQN) of the node. These nodes do not have to be currently registered.
 - *Remove Used* is used to remove selected nodes from the discovery domain.



12. Click the Discovery Domain Sets tab. The purpose of discovery domain sets is to separate further discovery domains. Discovery domains can be enabled or disabled, giving administrators the ability to restrict further the visibility of all initiators and targets. The options on the Discovery Domain Sets tab are as follows:

- The *Enable* check box is used to indicate the status of the discovery domain sets and to turn them off and on.
- *Create* is used to create new discovery domain sets.
- *Refresh* is used to repopulate the Discovery Domain Sets drop-down list.
- *Delete* is used to delete the currently selected discovery domain set.
- *Add* is used to add discovery domains to the currently selected discovery domain set.
- *Remove* is used to remove selected nodes from the discovery domain sets.



13. Close the iSNS server.

Fibre Channel

Fibre Channel storage devices are similar to iSCSI storage devices in that they both allow block-level access to their data sets and can provide MPIO policies with the proper hardware configurations. However, Fibre Channel requires a Fibre Channel HBA, fiber-optic cables, and Fibre Channel switches to connect to a storage device.

A *World Wide Name (WWN)* from the Fibre Channel HBA is used from the host and device so that they can communicate directly with each other, similar to using a NIC's MAC address. In other words, a logical unit number (LUN) is presented from a Fibre

Channel storage device to the WWN of the host's HBA. Fibre Channel has been the preferred method of storage because of the available connection bandwidth between the storage and the host.

Fibre Channel devices support 1Gb/s, 2Gb/s, and 4Gb/s connections, and they soon will support 8Gb/s connections, but now that 10Gb/s Ethernet networks are becoming more prevalent in many datacenters, iSCSI can be a suitable alternative. It is important to consider that 10Gb/s network switches can be more expensive than comparable Fibre Channel switches.

N-Port Identification Virtualization (NPIV) is a Fibre Channel facility allowing multiple n-port IDs to share a single physical N-Port. This allows multiple Fibre Channel initiators to occupy a single physical port. By using a single port, this eases hardware requirements in storage area network (SAN) design.

Network Attached Storage

The concept of a *network attached storage (NAS)* solution is that it is a low-cost device for storing data and serving files through the use of an Ethernet LAN connection. A NAS device accesses data at the file level via a communication protocol such as NFS, CIFS, or even HTTP, which is different from iSCSI or FC Fibre Channel storage devices that access the data at the block level. NAS devices are best used in file-storing applications, and they do not require a storage expert to install and maintain the device. In most cases, the only setup that is required is an IP address and an Ethernet connection.

Virtual Disk Service

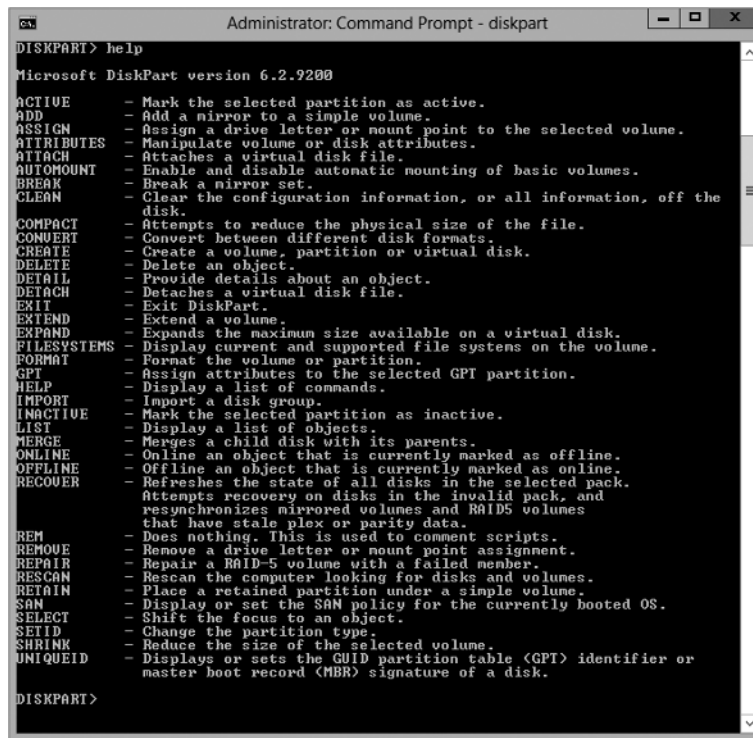
Virtual Disk Service (VDS) was created to ease the administrative efforts involved in managing all of the various types of storage devices. Many storage hardware providers used their own applications for installation and management, and this made administering all of these various devices very cumbersome.

VDS is a set of application programming interfaces (APIs) that provides a centralized interface for managing all of the various storage devices. The native VDS API enables the management of disks and volumes at an OS level, and hardware vendor-supplied APIs manage the storage devices at a RAID level. These are known as software and hardware providers.

A *software provider* is host based, and it interacts with Plug and Play Manager because each disk is discovered and operates on volumes, disks, and disk partitions. VDS includes two software providers: basic and dynamic. The basic software provider manages basic disks with no fault tolerance, whereas the dynamic software providers manage dynamic disks with fault management. A hardware provider translates the VDS APIs into instructions specific to the storage hardware. This is how storage management applications are able to communicate with the storage hardware to create LUNs or Fibre Channel HBAs to view the WWN. The following are Windows Server 2012 R2 storage management applications that use VDS:

- The *Disk Management snap-in* is an application that allows you to configure and manage the disk drives on the host computer. You have already seen this application in use when you initialized disks and created volume sets.
- DiskPart is a command-line utility that configures and manages disks, volumes, and partitions on the host computer. It can also be used to script many of the storage management commands. DiskPart is a robust tool that you should study on your own because it is beyond the scope of this book. Figure 1.8 shows the various commands and their function in the DiskPart utility.

FIGURE 1.8 DiskPart commands



```

Administrator: Command Prompt - diskpart
DISKPART> help
Microsoft DiskPart version 6.2.9200

ACTIVE          - Mark the selected partition as active.
ADD             - Add a mirror to a simple volume.
ASSIGN         - Assign a drive letter or mount point to the selected volume.
ATTRIBUTES     - Manipulate volume or disk attributes.
ATTACH         - Attaches a virtual disk file.
AUTOMOUNT      - Enable and disable automatic mounting of basic volumes.
BREAK          - Break a mirror set.
CLEAN          - Clear the configuration information, or all information, off the
               - disk.
COMPACT        - Attempts to reduce the physical size of the file.
CONVERT        - Convert between different disk formats.
CREATE         - Create a volume, partition or virtual disk.
DELETE        - Delete an object.
DETAIL        - Provide details about an object.
DETACH        - Detaches a virtual disk file.
EXIT          - Exit DiskPart.
EXTEND        - Extend a volume.
EXPAND        - Expands the maximum size available on a virtual disk.
FILESYSTEMS   - Display current and supported file systems on the volume.
FORMAT        - Format the volume or partition.
GPT           - Assign attributes to the selected GPT partition.
HELP         - Display a list of commands.
IMPORT        - Import a disk group.
INACTIVE      - Mark the selected partition as inactive.
LIST         - Display a list of objects.
MERGE        - Merges a child disk with its parents.
ONLINE       - Online an object that is currently marked as offline.
OFFLINE      - Offline an object that is currently marked as online.
RECOVER     - Refreshes the state of all disks in the selected pack,
               - Attempts recovery on disks in the invalid pack, and
               - resynchronizes mirrored volumes and RAID5 volumes
               - that have stale plex or parity data.
REM         - Does nothing. This is used to comment scripts.
REMOVE     - Remove a drive letter or mount point assignment.
REPAIR     - Repair a RAID-5 volume with a failed member.
RESCAN    - Rescan the computer looking for disks and volumes.
RETAIN    - Place a retained partition under a simple volume.
SAN       - Display or set the SAN policy for the currently booted OS.
SELECT   - Shift the focus to an object.
SETID    - Change the partition type.
SHRINK   - Reduce the size of the selected volume.
UNIQUEID - Displays or sets the GUID partition table (GPT) identifier or
               - master boot record (MBR) signature of a disk.

DISKPART>

```

- DiskRAID is also a scriptable command-line utility that configures and manages hardware RAID storage systems. However, at least one VDS hardware provider must be installed for DiskRAID to be functional. DiskRAID is another useful utility that you should study on your own because it's beyond the scope of this book.

Booting from a VHD

Once you have installed each operating system, you can choose the operating system that you will boot to during the boot process. You will see a boot selection screen that asks you to choose which operating system you want to boot.

The Boot Configuration Data (BCD) store contains boot information parameters that were previously found in `boot.ini` in older versions of Windows. To edit the boot options in the BCD store, use the `bcdedit` utility, which can be launched only from a command prompt. To open a command prompt window, do the following:

1. Launch `\Windows\system32\cmd.exe`.
2. Open the Run command by pressing the Windows key plus the R key and then entering `cmd`.
3. Type `cmd.exe` in the Search Programs And Files box and press Enter.

After the command prompt window is open, type `bcdedit` to launch the `bcdedit` utility. You can also type `bcdedit /?` to see all of the different `bcdedit` commands.



Virtualization is covered in greater detail in Chapter 9: “Use Virtualization in Windows Server 2012.”

Summary

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

I discussed the different upgrade paths that are available and which upgrades are best for your current network setup. You learned that another important issue to decide when installing Windows Server 2012 R2 is whether to use Server Core or the GUI installation.

You learned how to install Windows Server 2012 R2 Datacenter with GUI, and you installed the Windows Server 2012 R2 Server Core. Remember, Server Core is a slimmed-down version of Windows Server. With no GUI desktop available, it's a safer alternative to a normal Windows install. As discussed, a nice advantage of Windows Server 2012 R2 is that you can change from Server Core to the GUI version and back again.

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

You examined the various aspects of Windows Server 2012 R2 storage services as well as the various types of storage technologies and native Windows Server 2012 R2 storage

management tools. I started the chapter by discussing initializing disks and choosing a partition type: MBR or GPT. I then discussed the types of disk configurations, dynamic and basic, that are supported in Windows Server 2012 R2. You learned that various properties are associated with each type of configuration. Then I discussed the different types of RAID and the properties of each.

The next section explored storage technologies, namely, iSCSI, Fibre Channel, and NAS. I primarily focused on iSCSI because of the native support in Windows Server 2012 R2. You learned how to configure an iSCSI initiator and a connection to an iSCSI target. After that, you looked at its iSNS server and how to configure it.

The chapter concluded by looking at Storage Manager for SANs and Storage Explorer, which are built-in management tools in Windows Server 2012 R2 for storage devices and firewall settings.

Exam Essentials

Understand the upgrade paths. It's important to make sure you understand the different upgrade paths from Windows Server 2008 R2 with SP1 and Windows Server 2012 to Windows Server 2012 R2.

Understand Windows Server 2012 R2 server roles. Understand what the Windows Server 2012 R2 server roles do for an organization and its users.

Understand Windows Server 2012 R2 GUI vs. Server Core. Understand the difference between the Windows Server 2012 R2 GUI version and the Windows Server 2012 R2 Server Core version. Know the benefits of using Server Core, and know that you can convert between the two different versions.

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

Know disk types. Know how to initialize disks and the type of partitioning to choose. Also know the difference between dynamic and basic disks and when to use them.

Understand RAID. Know the various RAID types, the requirements for each, and when it is appropriate to use each type.

Know storage technologies. Understand how to use the storage technologies Fibre Channel, iSCSI, and NAS. Know how to configure an iSCSI initiator and how to establish a connection to a target. Know the various MPIO policies.

Understand how to manage storage. Know what type of administrative features are available for Storage Manager for SANs and Storage Explorer.

Review Questions

1. You are the administrator for the ABC Company. You are looking to install Windows Server 2012 R2, and you need to decide which version to install. You need to install a version of Windows that is just for logon authentication and nothing else. You want the most secure option and cost is not an issue. What should you install?
 - A. Windows Server 2012 R2 Datacenter with GUI
 - B. Windows Server 2012 R2 Datacenter Server Core
 - C. Windows Server 2012 R2 Standard with GUI
 - D. Windows Server 2012 R2 Web Server Core

2. You are the IT manager for a large organization. One of your co-workers installed a new Windows Server 2012 R2 Datacenter Server Core machine, but now the IT team has decided that it should be a Windows Server 2012 R2 Datacenter with GUI. What should you do?
 - A. Reinstall Windows Server 2012 R2 Datacenter Server Core on the same machine.
 - B. Install a new machine with Windows Server 2012 R2 Datacenter Server Core.
 - C. Convert the current Windows Server 2012 R2 Datacenter Server Core to the Windows Server 2012 R2 Datacenter with GUI version.
 - D. Dual-boot the machine with both Windows Server 2012 R2 Datacenter Server Core and Windows Server 2012 R2 Datacenter with GUI.

3. You are the administrator for your company, and you are looking at upgrading your Windows Server 2008 web server to Windows Server 2012 R2. Which version of Windows Server 2012 R2 does Microsoft recommend you use?
 - A. Windows Server 2012 R2 Datacenter
 - B. Windows Server 2012 R2 Standard
 - C. Windows Server 2012 R2 Essentials
 - D. Windows Server 2012 R2 Foundation

4. You are looking at upgrading your Windows Server 2008 R2 Enterprise with SP2 machine to Windows Server 2012 R2. Your organization is considering virtualizing its entire server room, which has 25 servers. To which version of Windows Server 2012 R2 would you upgrade?
 - A. Windows Server 2012 R2 Datacenter
 - B. Windows Server 2012 R2 Standard
 - C. Windows Server 2012 R2 Essentials
 - D. Windows Server 2012 R2 Foundation

5. You have been hired to help a small company set up its first Windows network. It has had the same 13 users for the entire two years it has been open, and the company has no plans to expand. What version of Windows Server 2012 R2 would you recommend?
 - A. Windows Server 2012 R2 Datacenter
 - B. Windows Server 2012 R2 Standard
 - C. Windows Server 2012 R2 Essentials
 - D. Windows Server 2012 R2 Foundation

6. You have been hired to help a small company set up its Windows network. It has 20 users, and it has no plans to expand. What version of Windows Server 2012 R2 would you recommend?
 - A. Windows Server 2012 R2 Datacenter
 - B. Windows Server 2012 R2 Standard
 - C. Windows Server 2012 R2 Essentials
 - D. Windows Server 2012 R2 Foundation

7. Which of the following are benefits of using Windows Server 2012 R2 Server Core? (Choose all that apply.)
 - A. Reduced management
 - B. Minimal maintenance
 - C. Smaller footprint
 - D. Tighter security

8. You are a server administrator, and you are trying to save hard drive space on your Windows Server 2012 R2 Datacenter machine. Which feature can help you save hard disk space?
 - A. HDSaver.exe
 - B. Features On Demand
 - C. ADDS
 - D. WinRM

9. You have a server named SRV1 that runs Windows Server 2012 R2. You want to remove Windows Explorer, Windows Internet Explorer, and all components and files from this machine. Which command should you run?
 - A. `msiexec.exe /uninstall iexplore.exe /x`
 - B. `msiexec.exe /uninstall explorer.exe /x`
 - C. `Uninstall-WindowsFeature Server-Gui-Mgmt-Infra Remove`
 - D. `Uninstall-WindowsFeature Server-Gui-Shell Remove`

10. What type of domain controller would you install into an area where physical security is a concern?
- A. Primary domain controller
 - B. Backup domain controller
 - C. Read-only domain controller
 - D. Locked-down domain controller