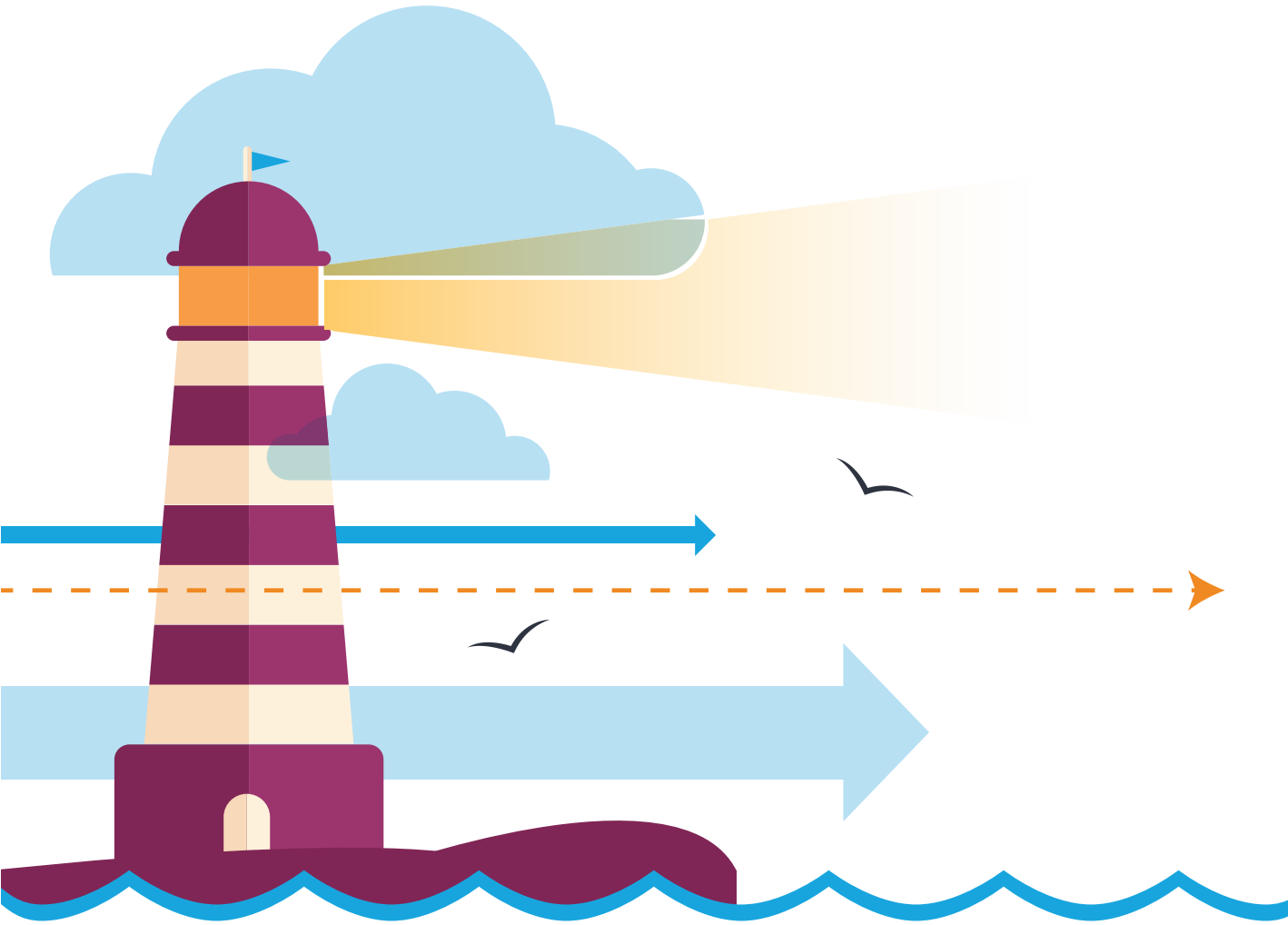


# WINDOWS SERVER® ADMINISTRATION FUNDAMENTALS

Crystal Panek

SYBEX®
A Wiley Brand

# Windows Server®

# Administration Fundamentals

Crystal Panek

SYBEX®
A Wiley Brand

Published simultaneously in Canada

ISBN: 978-1-119-65065-2
ISBN: 978-1-119-65775-0 (ebk.)
ISBN: 978-1-119-65068-3 (ebk.)

Manufactured in the United States of America



**Library of Congress Control Number:** 2019952299



10 9 8 7 6 5 4 3 2 1

*This book is dedicated to my loving husband, William Panek, and to my two wonderful daughters, Alexandria and Paige. Thank you all for your love and support. I love you all more than anything!*

# Acknowledgments

I would like to thank my husband and best friend, Will, because without him I would not be where I am today—thank you! I would also like to express my love to my two daughters, Alexandria and Paige, who have always shown nothing but love and support. Thank you all!

I would like to thank everyone on the Sybex team, especially my associate acquisitions editor, Devon Lewis, who helped make this the best book possible. I would like to thank Christine O'Connor, who was the production editor, and Kim Wimpsett for being the proofreader.

Finally, I also want to thank everyone behind the scenes who helped make this book possible. Thank you all for your hard work and dedication.

# About the Author

**Crystal Panek** holds the following certifications: MCP, MCP+I, MCSA, MCSA+ Security and Messaging, MCSE-NT (3.51 & 4.0), MCSE 2000, 2003, 2012/2012 R2, 2016, MCSE+Security and Messaging, MCDBA, MCTS, MCITP.

For many years she trained as a contract instructor teaching at such places as MicroC, Stellacon Corporation, and the University of New Hampshire. She then became the vice president for a large IT training company, and for 15 years she developed training materials and courseware to help thousands of students get through their certification exams. She currently works on a contract basis creating courseware for several large IT training facilities.

She currently resides in New Hampshire with her husband and two daughters. In her spare time, she likes to camp, hike, shoot trap and skeet, golf, bowl, and snowmobile.

# Contents at a Glance

# Contents

# Introduction

## What Does This Book Cover?

**Chapter 1: Server Overview** This chapter covers understanding server installation options, choosing the correct operating system version options, Server core vs. Desktop Experience, Nano Server installation, interactive installs, automated install using WDS, VHD/VHDX installation source, how to perform unattended installs, perform upgrades, clean installs, and migrations. This chapter also covers identifying application servers, mail servers, database servers, collaboration servers, monitoring servers, and threat management. You will learn to understand server virtualization, virtual memory, virtual networks, VHD and VHDX formats. This chapter delves into identifying major hardware components, memory, disk, processor, network, 32-bit and 64-bit architecture, removable drives, graphic cards, cooling, power usage, and ports. This chapter will also teach you how to work with updates, software, driver, operating systems, applications, Windows Update, and using Windows Server Update Service (WSUS).

**Chapter 2: Managing Windows Server 2016** This chapter covers understanding device drivers, installing, removing, disabling, update/upgrade, rollback, troubleshooting, Plug & Play, IRQ, interrupts, driver signing, and managing devices through Group Policy. This chapter will also teach you how to understand services. It also covers which statuses a service can be in, startup types, recovery options, delayed startup, Run As settings for a service, stopping or pausing a service, service accounts, and dependencies. This chapter will also delve into understanding remote access. Also covered are remote assistance, remote administration tools, Remote Desktop Services, multipoint services, licensing, RD Gateway, VPN, application virtualization, and multiple ports.

**Chapter 3: Managing Storage** This chapter covers identifying storage technologies and their typical usage scenarios, the advantages and disadvantages of different storage topologies, local storage, network storage, Fibre Channel, and iSCSI hardware. This chapter also introduces using RAID redundancy, RAID 0, RAID 1, RAID 5, RAID 10 and combinations, hardware and software RAID. This chapter will also discuss understanding disk types, such as Solid State Drive (SSD) and Hard Disk Drive (HDD) types and comparisons, ATA basic disk, dynamic disk, mount points, file systems, mounting a virtual hard disk, and distributed file systems.

**Chapter 4: Monitoring and Troubleshooting Servers** This chapter covers understanding performance monitoring, methodology, procedures, effect of network, CPU, memory and disk, creating a baseline, Performance Monitor, Resource Monitor, Task Manager, performance counters, and Data Collector Sets. You will also learn to understand logs and alerts, Event Viewer, performance logs, and alerts. This chapter will cover the steps of the startup

process, BIOS, UEFI, TPM, bootsector, bootloader, MBR, boot.ini, POST, and Safe Mode. Will delve into understanding business continuity, using backup and restore, disaster recovery planning, clustering, AD restore, folder redirection, data redundancy, uniterruptible power supply (UPS). You will also learn troubleshooting methodologies, processes, procedures, best practices, systematic vs. specific approach, Performance Monitor, Event Viewer, Resource Monitor, Information Technology Infrastructure Library, central logging, event filtering, and using default logs.

**Chapter 5: Essential Services** This chapter covers understanding accounts and groups, domain accounts, local accounts, user profiles, computer accounts, group types, default groups, group scopes, group nesting, and understanding AGDLP and AGUDLP processes to help implement nesting. You will learn about organizational units and containers, the purpose of OUs, purpose of containers, delegation, default containers, uses for different container objects, default hidden, and visible containers. This chapter will teach you about the Active Directory infrastructure, domain controllers, forests, child domains, operation master roles, domain vs. workgroup, trust relationships, functional levels, deprecated functional levels, namespace, sites, replication, schema, and Passport. This chapter will also delve into understanding group policies, group policy processing, Group Policy Management Console, computer policies, user and local policies.

**Chapter 6: File and Print Services** This chapter covers the file and print services. You will learn about local printers, network printers, printer pools, web printing, web management, driver deployment, file, folder, and share permissions vs. rights, auditing, and print job management.

**Chapter 7: Popular Windows Network Services and Applications** This chapter covers using Web services such as IIS, WWW, and FTP, installing from Server Manager, separate worker processes, adding components, sites, ports, SSL, and using certificates. You will also learn about server virtualization, including how to use snapshots and saved states, physical to virtual conversions, virtual to physical conversions, and nested virtualization.

# Interactive Online Learning Tools

Studying the material in *Windows Server Administration Fundamentals* is an important part of self-learning, but we provide additional tools to help you prepare.

To start using these tools to jump-start your self-study, go to `www.wiley.com/go/sybextestprep`.

Lesson

1

# Server Overview

Objective Domain Matrix

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

## Key Terms

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

### Real World Scenario

**Lesson 1 Case**

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

# Understanding What a Server Does

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

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

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

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


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

## Introducing Server Roles

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

**Certification Ready?**

Can you list and describe the basic server roles? 2.1

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

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

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

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

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

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

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

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

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

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

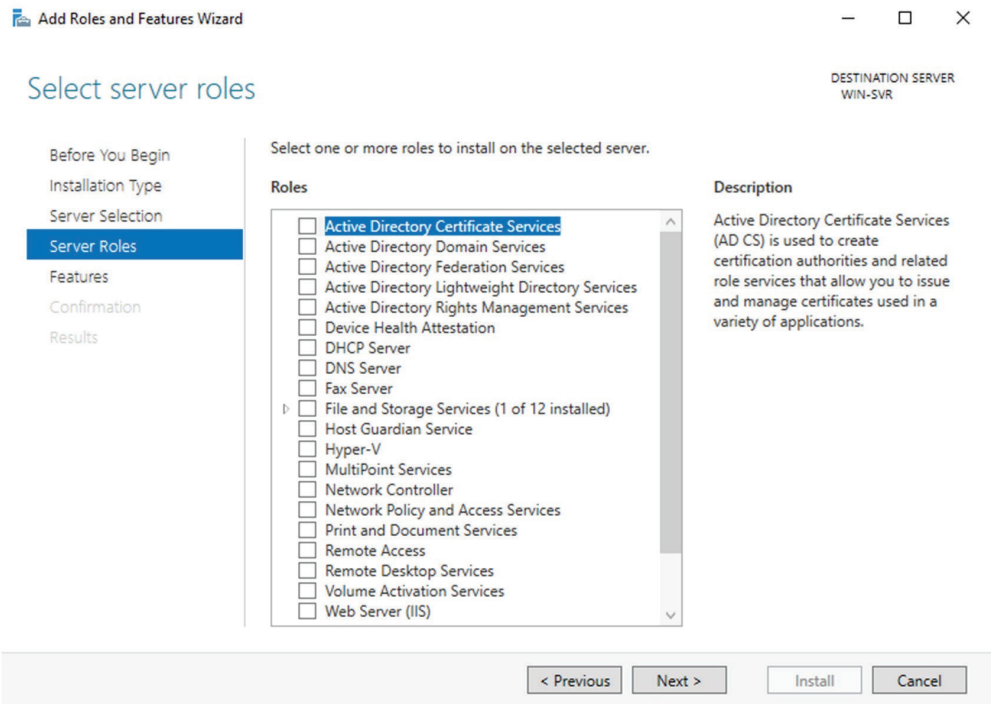
Another example of an application server is if you have a sales tracking application or inventory control applications. You would access this type of server on your company network by using a customized program or using your browser. You will then request information or input some data, which will then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

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

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

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

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




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

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

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

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

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

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

**Device Health Attestation** Helps protect a corporate network by verifying that client systems meet corporate policy. For example, an administrator can make sure that all computers connected to a network have their proper updates, antivirus, and proper configuration policies before connecting to the network.

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

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

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

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

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

**Hyper-V** Allows administrators to create and manage a virtualized environment by taking advantage of the technology built into the Windows Server 2016 operating system. When an administrator installs the Hyper-V role, all required virtualization components are installed. Some of the required components include the Windows hypervisor, Virtual Machine Management Service, the virtualization WMI provider, the virtual machine bus (VMbus), the virtualization service provider (VSP), and the virtual infrastructure driver (VID).

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

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

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

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

**Remote Access** Provides connectivity through DirectAccess, VPN, and Web Application Proxies. DirectAccess provides an Always On and Always Managed experience. Remote Access provides VPN access including site-to-site connectivity. Web Application Proxies enable web-based applications from a corporate network to client devices outside of the corporate network. Remote Access also includes routing capabilities, including Network Address Translation (NAT).

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

**Volume Activation Services** Helps an organization benefit from using this service to deploy and manage volume licenses for a medium to large number of computers.

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

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

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

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

## Configure Windows Server Security Settings

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

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

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

## Back Up Information and Systems

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

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

## Management and Monitoring Using Operations Management Suite

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

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

OMS offers the following capabilities and features:

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

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

## Protect Privileged Identities

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

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

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

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

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

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

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

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

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