Installing
—and—
Configuring Windows Server 2022

Learn the ins and outs of Windows Server 2022 administration

Bekim Dauti

bpb

Installing
—and—
Configuring Windows Server 2022

Learn the ins and outs of Windows Server 2022 administration

Bekim Dauti

bpb

Installing and Configuring Windows Server 2022

Learn the ins and outs of Windows Server 2022 administration

Bekim Dauti

www.bpbonline.com

Dedicated to

To all the children who dream of a better future.
May this book inspire
them to pursue their passions and achieve their
goals,
just as it has inspired me.

About the Author

Bekim Dauti is a qualified and experienced computer technology expert specializing in server administration, computer networking, and training, focusing on Cisco, CompTIA, and Microsoft technologies. He earned his bachelor's in informatics from the University of Tirana, a master's in information technology from UMGC Europe, and a doctorate in Computer Science from Aspen University.

Bekim has over 20 years of experience as a Cisco Certified Academy Instructor (CCAI) and over 15 years of experience as a Microsoft Certified Trainer (MCT). In addition, he holds several IT certifications from reputable vendors, including ECDL, Certiport, CompTIA, Cisco, Microsoft, and Sun Microsystems.

As a prolific writer, Bekim has contributed to nearly 20 books and published dozens of articles in renowned publications such as PC World Albanian and CIO Albanian. In addition, he founded InfoTech (Academy) and Dautti and is working as a Microsoft Certified Trainer at Elev8. Bekim's passion for technology extends to maintaining a blog called *Bekim Dauti's Blog*. Bekim is grateful for his parents' support.

Given the persistent extreme poverty in numerous countries worldwide, would it be more prudent to redirect the efforts currently devoted to building a global economy towards the primary goal of achieving global equality? Prioritizing global equality, in conjunction with the worldwide economy could

pave the way for numerous international initiatives to enhance the overall quality of life worldwide.

— Bekim Dauti

Acknowledgement

Preface

Windows Server 2022 is the server operating system developed by Microsoft as part of the Windows NT family of operating systems, developed concurrently with Windows 10 version 1809. This book is designed to get you started with Windows Server 2022. At the same time, this book aims to introduce you to the roles that Windows Server 2022 supports. In addition, the book teaches you how to install roles by using both Add Roles and Features Wizard and Windows PowerShell cmdlets. Furthermore, the book provides instructions for configuring client/server network services using the various Graphical User Interface (GUI) wizards, tools, and Windows PowerShell cmdlets.

The book begins with the introduction of computer networks and Windows Server 2022. Then, it continues with the installation and post-installation tasks of Windows Server 2022. You will then move on to a more advanced aspect of working with Windows Server 2022, such as installing roles and configuring client/server network services like AD DS, DNS, DHCP, WDS, PDS, WSUS, Web Server, Hyper-V, and other essential network services. Next, with the help of real-world examples, you will get to grips with the fundamentals of Windows Server 2022, which will help you solve complex tasks the easy way. Later, the book also shows you maintenance and troubleshooting tasks, where with the help of best practices, you can easily manage Windows Server 2022. By the end of this book, you will have the knowledge required to administer and manage Windows Server environments.

Chapter 1: Understanding Networks and their Components - This chapter is designed to introduce Windows Server in general. Besides introducing Windows Server, at the beginning of this chapter, there is a reminder of the basic concepts of computer network components. Definitions such as hosts, nodes, peer-to-peer, and clients/servers are covered in the Computer Network Overview section. In addition, the reader will learn about general concepts of clients, servers, NOS, hardware and software, and networking architectures.

Chapter 2: Introduction to Windows Server 2022 - This chapter is designed to introduce Windows Server 2022. Windows Server 2022 is the server's operating system developed by Microsoft as part of the Windows NT family of operating systems and developed concurrently with Windows 10 version 1809. The Windows Server Overview section uncovers the essentials of Windows Server 2022. The reader will learn Microsoft's new server OS, Windows Server 2022. In addition, the reader will learn Windows Server 2022 editions, compare Windows Server 2022 with Windows Server 2016, minimum and recommended system requirements, and download Windows Server 2022.

Chapter 3: Windows Server 2022 Installation - This chapter provides detailed instructions for installing Windows Server 2022. The step-by-step instructions, driven by easy-to-understand graphics, explain and show you how to master the installation of Windows Server 2022. In addition, the reader will learn about Windows Server 2022 installation options. For each option, a step-by-step approach will be presented.

Chapter 4: Initial Configuration of Windows Server 2022 - This chapter explains steps to take in Windows Server 2022 post-installation, including managing devices and device drivers, checking the registry and the status of

services, and taking care of the initial server configuration. The reader will learn about the server's device drivers and play with them by installing, upgrading, uninstalling, troubleshooting, etc. Additionally, the reader will learn about services and how to manage them in a server environment.

Chapter 5: Installing Roles Using Server Manager and PowerShell - This chapter provides step-by-step installation how-to instructions for roles in Windows Server 2022 using the Add Roles and Features Wizard from the Server Manager and cmdlets from Windows PowerShell. The reader will learn to use the Server Manager Add Roles and Feature Wizard and Windows PowerShell to add roles in Windows Server 2022. At the same time, the reader will get to know and learn each role's purpose.

Chapter 6: Service Management with GUI and PowerShell - This chapter provides step-by-step installation how-to instructions for configuring client/server network services in Windows Server 2022 by using various Graphical User Interfaces (GUI) and Windows PowerShell cmdlets. The reader will learn to use multiple Graphical User Interface (GUI) wizards and Windows PowerShell cmdlets to configure client/server network services in Windows Server 2022.

Chapter 7: Tuning Windows Server 2022 for Peak Performance - This chapter is designed to teach you the best practices and considerations for server hardware. By understanding the importance of a server's role in a computer network and possessing knowledge of each server component, a sys admin can be vigilant when selecting server hardware. In addition, this chapter teaches server performance monitoring methodologies and procedures. The reader will learn how to tune the performance of Windows Server 2022. The reader will also become familiar with the

maintenance process and understand the maintenance techniques.

Chapter 8: Maintaining and Resolving Issues in Windows Server 2022 - This chapter teaches the most challenging part of working with servers. Thus, understanding the importance of troubleshooting, updating, and maintaining servers increases the potential to have a high business continuity standard. Also, this chapter teaches the server startup process, advanced boot options and Safe Mode, backup and restore disaster recovery plan, and updating the OS, hardware, and software. The Event Viewer is also included, which helps you monitor different logs on your system, thus allowing you to troubleshoot and solve the problem. The reader will become familiar with the importance of keeping Windows Server 2022 up-to-date while learning the options available for updating Windows Server 2022. Additionally, the reader will understand troubleshooting and be able to troubleshoot errors and problems in Windows Server 2022, too.

Chapter 9: Getting Ready for Microsoft Certifications - This chapter comprehensively introduces Microsoft certifications, encompassing insights into the competencies evaluated within the examination. Moreover, it outlines the significance of Microsoft certifications aligned with specific roles and elucidates the procedure for exam enrollment. Furthermore, you will uncover invaluable sources to aid you in accumulating extensive insights about the examination in a broader context, discern the requisites for its successful completion, and, in the process, embark on a prosperous professional journey.

Chapter 10: Answers to Chapter Questions - This chapter provides responses to the inquiries posed in the chapter. Furthermore, numerous queries are presented alongside each chapter to assist you in solidifying your

grasp of the concepts and definitions. This supplementary section empowers you to verify your solutions to those queries.

Coloured Images

Please follow the link to download the
Coloured Images of the book:

https://rebrand.ly/1gnuzf5

We have code bundles from our rich catalogue of books and videos available at **https://github.com/bpbpublications**. Check them out!

Errata

We take immense pride in our work at BPB Publications and follow best practices to ensure the accuracy of our content to provide with an indulging reading experience to our subscribers. Our readers are our mirrors, and we use their inputs to reflect and improve upon human errors, if any, that may have occurred during the publishing processes involved. To let us maintain the quality and help us reach out to any readers who might be having difficulties due to any unforeseen errors, please write to us at :

errata@bpbonline.com

Your support, suggestions and feedbacks are highly appreciated by the BPB Publications' Family.

business@bpbonline.com for more details.

At www.bpbonline.com, you can also read a collection of free technical articles, sign up for a range of free newsletters, and receive exclusive discounts and offers on BPB books and eBooks.

Piracy

If you come across any illegal copies of our works in any form on the internet, we would be grateful if you would provide us with the location address or website name. Please contact us at business@bpbonline.com with a link to the material.

If you are interested in becoming an author

If there is a topic that you have expertise in, and you are interested in either writing or contributing to a book, please visit www.bpbonline.com. We have worked with thousands of developers and tech professionals, just like you, to help them share their insights with the global tech community. You can make a general application, apply for a specific hot topic that we are recruiting an author for, or submit your own idea.

Reviews

Please leave a review. Once you have read and used this book, why not leave a review on the site that you purchased it from? Potential readers can then see and use your unbiased opinion to make purchase decisions. We at BPB can understand what you think about our products, and our authors can see your feedback on their book. Thank you!

For more information about BPB, please visit www.bpbonline.com.

Join our book's Discord space

Join the book's Discord Workspace for Latest updates, Offers, Tech happenings around the world, New Release and Sessions with the Authors:

https://discord.bpbonline.com

Table of Contents

Q3: How many types of network components can you name?

Q4: List three differences between IPv4 and IPv6 addressing technologies.

Q5: In your own words, define a Network Operating System.

Answers to Chapter 2 questions

Q1: What are the server's four hardware key components, and what is their function?

Q2: Can you name each era of the Windows Server and list the corresponding versions?

Q3: What do you mean by minimum system requirements?

Q4: List three new features in Windows Server 2022.

Q5: What do you like most about Windows Server 2022?

Answers to Chapter 3 questions

Q1: What are the two primary partition schemes typically used in computers and servers?

Q2: What is the boot option?

Q3: Can you provide the names of installation methods?

Q4: What installation options should be considered before installing Windows Server 2022?

Q5: What is the purpose of a virtual switch in Hyper-V?

Answers to Chapter 4 questions

Q1: What are device drivers?

Q2: What is Windows Registry?

Q3: What are Windows services?

Q4: Why is initial configuration essential for Windows Server?

Understanding Networks and their Components

Introduction

The most recent version of Microsoft's server operating system and part of the Windows NT series, Windows Server 2022 boasts improved security, versatility, and stability. Moreover, it supports hybrid deployments through a specially developed edition of Windows Server 2022 Datacenter Azure. All these new features and capabilities of Windows Server 2022 show that anyone interested in learning how to use a **Network Operating System** (**NOS**) must have a basic understanding of the computer network, especially the essential network components. Therefore, this chapter introduces the network and its features. Definitions such as computer networks, network components, hosts, nodes, clients and servers, network architectures, IP address and subnet mask, and the NOS itself are discussed in this chapter. These concepts will help you understand networks' essentials and their components. Finally, you can configure the Hyper-V client in Windows 10/11 with the help of this chapter's exercise.

Structure

In this chapter, we will cover the following topics:

- Birth of the internet

- Computer networks
- Network components
- Network architectures
- Network topologies
- Internet Protocol addresses and subnets
- Network operating system
- Technology trends

Objectives

This chapter aims to supply a basic introduction to networking. It will also discuss the details of essential networking components. This chapter begins with the most fundamental concepts about computer network types and networks to delve into a detailed explanation of network components. Finally, we will conclude the chapter with a first-hand example of configuring Hyper-V in Windows 11 Pro using settings and Windows PowerShell.

Birth of the internet

The internet itself is the ultimate authority when explaining its history. It all began with the US government's initiative to create a reliable and resilient communication network called the **Defense Advanced Research Projects Agency** (**DARPA**). Through the involvement of research centers and academic institutions, this endeavor gradually transformed into two distinct projects: the ARPANET and the **Military Network** (**MILNET**). MILNET focused on meeting operational requirements, whereas ARPANET was primarily developed to cater to research needs. By 1985, the internet had already established its identity, thereby signifying the formal conclusion of ARPANET's prosperous era. This progression can be summarized with the phrase, "Every new beginning is some beginning's end."

As stated on **internetsociety.org**, the **Federal Networking Council** (**FNC**) adopted a resolution on October 24, 1995, after consulting with internet community members and considering

intellectual property rights. This resolution aimed to define the term "internet." According to the resolution, the internet refers to a global information system that possesses the following characteristics:

- It is logically connected by a globally unique address space established on the **Internet Protocol** (**IP**) or its subsequent updates.

- It can support communication through the TCP/IP protocol suite or its subsequent updates, along with other compatible protocols.

- It provides, utilizes, and grants accessibility, whether publicly or privately, to high-level layered services on the communications and related Infrastructure outlined in the document previously mentioned.

In essence, this resolution serves as a comprehensive definition of the internet, outlining its interconnectedness, communication protocols, and the provision of accessible services.

As computer network technologies progressed, a growing demand emerged to effectively connect and interconnect an increasing number of computers across various geographical locations. Consequently, the necessity arose for precise terminology and concepts to describe the field of computer networking. That resulted in the development of distinct types of computer networks, diverse network topologies, varied network architectures, and an array of network components.

Undoubtedly, computer networks stand as one of humanity's most significant inventions in communication. Merely mentioning the internet demonstrates the tremendous advantages that computer networks bring to society.

Note: To learn more about the history of the internet, visit the following URL: **https://www.internetsociety.org/internet/history-internet/**. It directs to a Web page hosted by the Internet Society, providing a concise and comprehensive overview of the history of the internet. From its origins to its evolution, the Web page covers significant milestones, developments, and contributions of various individuals and organizations, offering valuable insights into the remarkable journey of the internet and its impact on the world.

Computer networks

The intention of this section is not to engage in a comparison of computer networks and network components. Instead, its primary objective is to define a computer network and expound upon its components. Hence, without delving into intricate academic or professional explanations, a computer network can connect two or more computers for resource sharing. From this fundamental definition, we deduce that a pair of computers is the minimum requirement for constructing a network. Moreover, factors such as network coverage, accessibility of services, and the purpose of network servers is to determine the different types of computer networks. Therefore, various networks can be classified as follows:

- A **Personal Area Network** (**PAN**) refers to a computer network designed to establish connections between devices and enable the transmission and reception of data within an individual's workspace. An excellent illustration of a PAN is the **Wireless Personal Area Network** (**WPAN**), which uses Bluetooth technology for interconnecting devices.

- On the other hand, a **Local Area Network** *(LAN)* is a computer network that connects devices and facilitates data exchange within a specific area, such as a floor or a building. A **Wireless Local Area Network** (**WLAN**) is a prime example of a LAN that uses radio waves for interconnection. The most prevalent radio wave technology used in WLANs is Wi-Fi, commonly called Wireless Fidelity, which typically operates at 2.4 GHz and, more recently, at 5 GHz.

- A **Campus Area Network** (**CAN**) is a computer network that interconnects LANs and enables data transmission within a limited geographical area. An extended LAN illustrates a CAN, facilitating network connectivity across multiple buildings or campuses.

- A **Metropolitan Area Network** (**MAN**) is a computer network that connects LANs and allows data exchange

within a town, city, or metropolitan area. It encompasses a larger geographical area compared to a CAN.

- Furthermore, a **Wide Area Network** (**WAN**) is a computer network that extends across a vast geographical expanse and facilitates data transfer between MANs. The internet is a well-known example of a WAN, connecting networks worldwide and enabling global communication and information exchange.

Network components

Once we have clearly understood what constitutes a computer network, it becomes easier to identify its different elements. These elements encompass computers, the medium used for networking, networking devices, and the resources used within the network, as mentioned earlier in this chapter and represented in *Figure 1.1*.

In this context, the computers within the network are interconnected with a network device, specifically a switch, through the networking medium. In our case, the medium used is a twisted pair cable. Furthermore, these computers can share various resources their operating system facilitates, such as Windows 10 or 11. For instance, a resource in this context could be a file or a printer.

Refer to *Figure 1.1:*
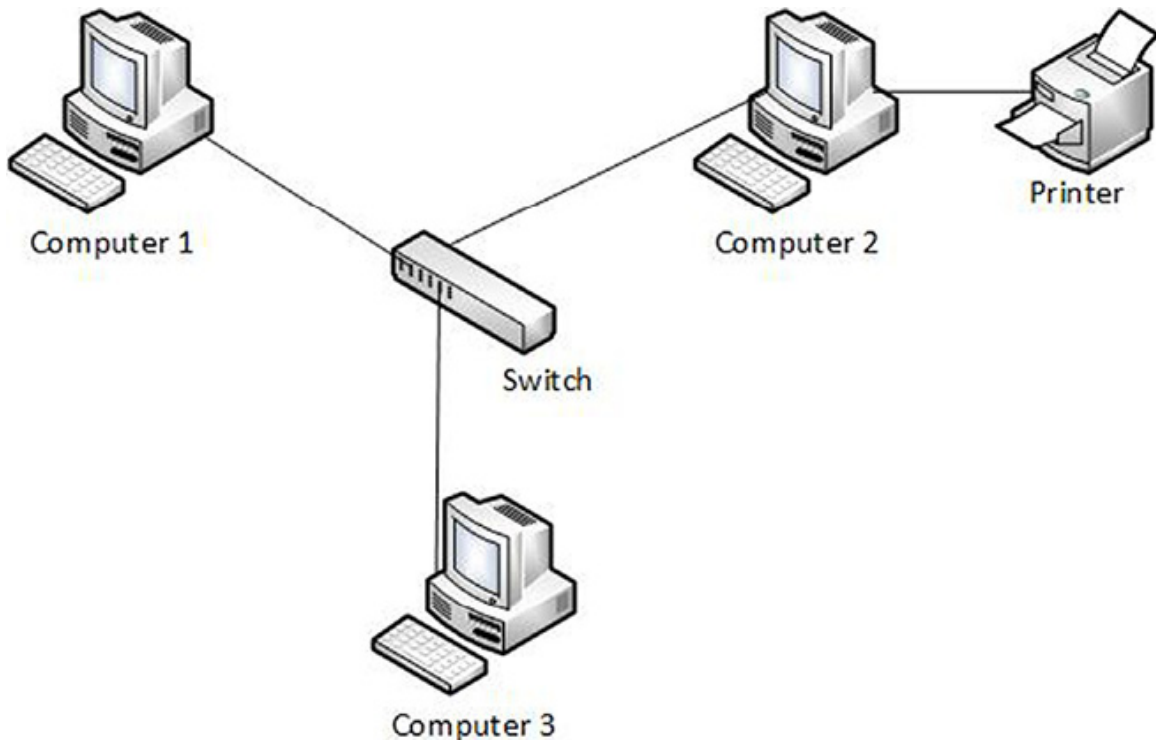
Figure 1.1: *The computer network and network components*

The subsequent sections will delve into the critical components of computer networks and provide a comprehensive understanding of their functionality and importance.

Hosts and nodes

By examining the computer network shown in *Figure 1.1*, we can identify computers 1–3 as hosts, the switch as a node, and the printer as a peripheral device. Although you may have understood this description, the question remains: What are hosts and nodes?

At first glance, hosts and nodes might appear interchangeable but have different meanings. In computer networks, the term *node* is generally used in a broader sense to refer to any device connected to the network. However, a node lacks a network interface with an assigned IP address, which is crucial for locating the node within the network, enabling data transmission, and granting access to network services. This specific attribute is found only in hosts. A *host* is a device with a network interface with an assigned IP address. It uses this address to communicate

with other devices and utilize network services. Therefore, it can be said that all hosts can be considered nodes, but not all nodes are hosts.

To further illustrate this distinction, consider *Figure 1.2*, which depicts a network with clients, servers, and a router identified as hosts. In contrast, the switch is classified as a node within the same network. Please refer to the following figure:
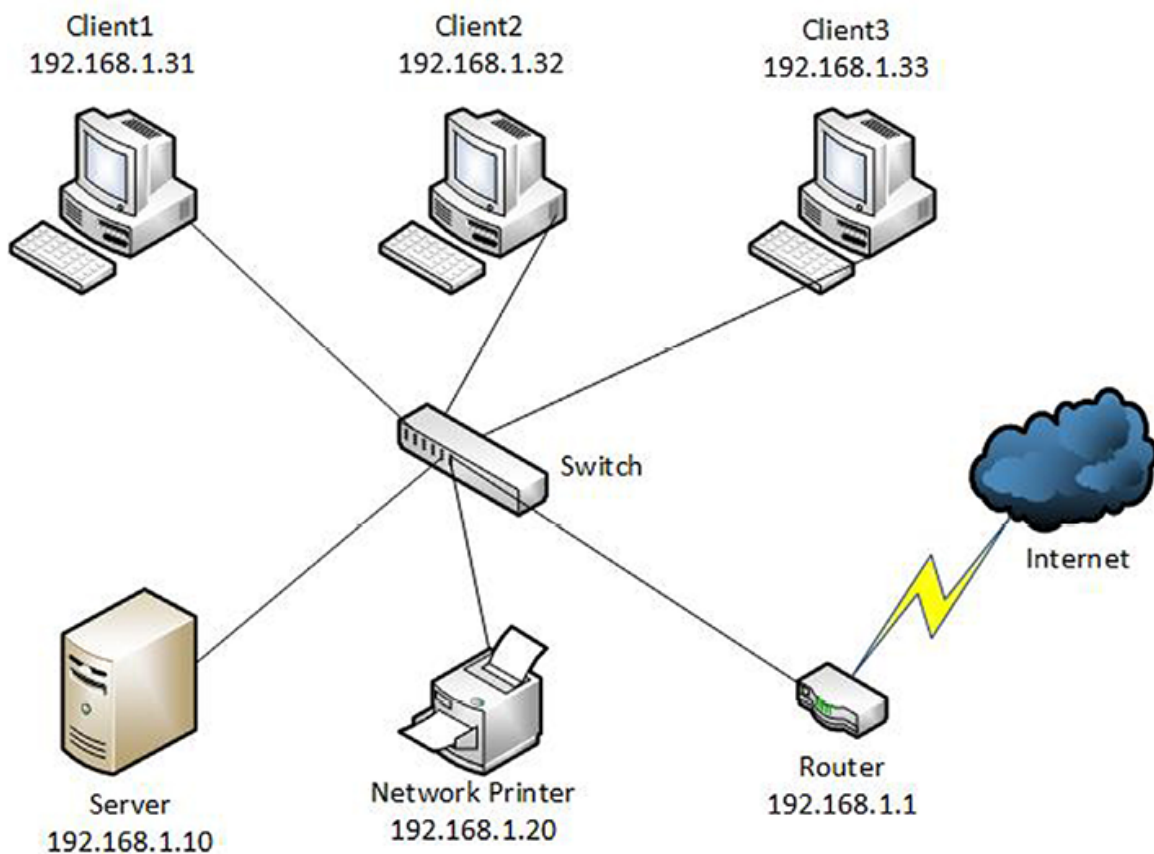
Figure 1.2: *The hosts and nodes in a computer network*

Note: It is important to note that hosts and nodes are two different terms in computer networking. While all hosts can be considered nodes, not all nodes have the essential attributes of hosts, such as a network interface with an assigned IP address. However, network nodes have network interfaces with assigned IP addresses, but these addresses are solely used for management purposes.

Clients and servers

Within the computer network illustrated in *Figure 1.2*, the computers labeled 1–3 are categorized as clients, while the server represents the central server entity. On the other hand, the switch and the router function as nodes, and the network printer serves as a peripheral device. The information provided shows that *clients* are responsible for initiating requests to access resources in computer networks, whereas *servers* are designed to provide services. More precisely, servers respond to access requests by delivering the services themselves. Hence, the term *server* is assumed to originate from its role in serving the needs of its clients by providing the required services.

This distinction between clients and servers highlights their roles and responsibilities within a computer network. Clients actively seek resources or services, whereas servers fulfill those requests and deliver the requested services. It is essential to understand this differentiation to grasp the functioning and dynamics of computer networks effectively.

Network interface

As shown in *Figure 1.3*, a network interface refers to hardware components such as a network card or LAN port on various network devices. Its primary function is facilitating the connection and communication between clients, servers, peripheral devices, and other network equipment. The network interface plays a dual role in the computer network, acting as both a passive and active component. In its passive role, the network interface serves as a connector, allowing devices to connect to the network physically. It provides the necessary ports and connectors to establish a link between the device and the network infrastructure. This passive function enables the transmission of data packets to and from the connected device. Please refer to the following figure:

Figure 1.3. *USB-based network interface*

In its active role, the network interface takes on a more dynamic and manageable role, particularly in the case of network equipment such as switches or routers. These functional network interfaces include additional features and capabilities that enable the device to actively manage network traffic, perform routing functions, and enforce network policies. Active network interfaces can be configured, monitored, and controlled to optimize network performance, security, and reliability.

Peripheral devices

Peripheral devices encompass hardware components, such as printers, scanners, and storage, which offer client resources via a **Local Area Network** (**LAN**) or as shared devices on a network. These devices serve both passive and active roles within the computer network. In their passive role, peripheral devices provide resources or services to clients without actively participating in network management or control. For example, a printer may accept print jobs from client devices and produce physical copies without actively managing network traffic. However, specific peripheral devices, such as **Storage Area Networks** (**SANs**) and **Network-Attached Storage** (**NAS**), are active in the network. SANs and NAS systems actively manage and control data storage and retrieval operations within the network, offering centralized and efficient storage solutions.

Shared apps and data

Shared applications and data are virtual network components representing the presence of applications and shared files within the network. Typically, servers host these components. While applications and shared data primarily play a passive role in the computer network, the server responsible for hosting these services assumes an active role. In their passive role, applications and shared data are resources available to network users. Users can access these applications and share files without directly participating in network management or control.

On the other hand, as said above, the server hosting these services assumes an active role in the computer network. The server controls the availability, delivery, and security of applications and shared data. It handles client requests, processes data, and ensures the efficient functioning of its network services.

Hubs and switches

Hubs and switches are essential components in Ethernet communication technology that serve as central points in a computer network. They facilitate the interconnection and communication between clients, servers, and peripheral devices. Hubs are generally passive devices, whereas switches actively participate in the operation of the computer network. Hubs function as essential connectivity devices that allow multiple devices to connect and share the same network segment. However, they do not actively manage or control network traffic. Instead, they replicate incoming data packets and broadcast them to all connected devices, regardless of the intended recipient. That can lead to network congestion and inefficient data transmission.

In contrast, *switches* (depicted in *Figure 1.4*) are active devices that manage and control network traffic. They make intelligent forwarding decisions based on the destination MAC addresses of the data packets. By maintaining a table of MAC addresses and associated port connections, switches can selectively forward packets to the appropriate devices, improving network efficiency and reducing congestion. Please refer to the following figure:

Figure 1.4. Cisco switch

Routers

Routers, shown in *Figure 1.5*, are essential components in computer networks that facilitate the transfer of data packets between a **Local Area Network** (**LAN**) and the internet in both directions. Routers play an active role in the overall functioning of the computer network. Routers are responsible for efficiently directing data packets from their source to their destination across different networks. They analyze the network addresses within the packets and determine the most optimal path for forwarding the data. This process, known as routing, involves making intelligent decisions based on network topology and routing protocols. Please refer to the following figure:

Figure 1.5. Cisco routers

Routers ensure data is delivered accurately and efficiently to intended recipients by actively managing network traffic. They maintain routing tables and exchange information with neighboring routers to update and adapt to network changes dynamically. Routers connect LANs to the internet and provide network segmentation by separating networks into smaller subnets. This segmentation helps enhance security, performance, and network management by controlling the flow of data and improving network efficiency.

Firewall

A *firewall* (see *Figure 1.6*) serves as a crucial network component responsible for ensuring the security of the network infrastructure. It achieves this by regulating and monitoring incoming and outgoing network traffic according to preconfigured security rules. In essence, a firewall can be likened to a security officer stationed at the main gate of an organization. Like how a security officer scrutinizes individuals entering or leaving premises, a firewall examines and controls network traffic flow as a barrier against unauthorized access and potential threats. By enforcing security rules, a firewall helps safeguard the network from malicious activities, such as unauthorized access attempts, data breaches, and network attacks. It acts as a crucial line of defense, preventing unwanted or potentially harmful traffic from entering the network while allowing legitimate and authorized communication to flow smoothly. Please refer to the following figure:
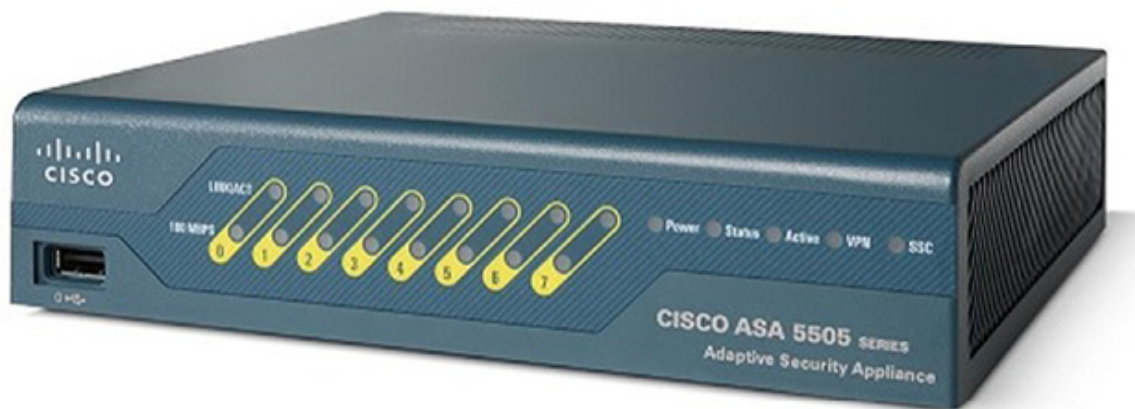
Figure 1.6. *Cisco firewall*

Networking mediums

Various networking mediums are used for data transfer and communication depending on whether physical (cable-based) or wave-based (wireless) communications. The following are the primary mediums used:

- **Metallic-based mediums**: Copper wires in twisted pairs and coaxial cables transmit electrical impulses. These mediums use the conductive properties of metal to carry electrical signals.

- **Glass-based mediums**: Fiber optic cables transmit pulses of light. These cables consist of glass fibers that transmit data through the reflection and refraction of light signals.

- **Air-based mediums**: Wave-based communication relies on transmitting signals through the air using different frequencies within the electromagnetic spectrum. That includes wireless communication technologies that use radio waves, microwaves, or other frequencies to share data without needing physical cables.

These networking mediums serve as the foundation for data transfer and communication, each with their characteristics and advantages. Metallic mediums provide reliable and cost-effective wired connections, whereas glass mediums offer high-speed and long-distance transmission capabilities through fiber optics. Air mediums enable wireless communication, providing flexibility and mobility in data transfer.

Network architectures

Although different types of computer networks classify networks based on geographical coverage, computer network architectures focus on the designs that enable communication among the various components within a network. Therefore, computer network architecture encompasses several elements, including physical and logical topology, network components, communication protocols, and the principles and procedures that govern its operation. Two widely recognized network architectures are **Peer-To-Peer** (**P2P**) and client/server, which are explained as follows:

- In a P2P architecture, a computer network operates on a distributed framework. In this type of network, the traditional concept of dedicated servers is eliminated, and communication occurs directly between peer computers

that function as both clients and servers. In a P2P network, all peer computers are considered equal, with equal permissions and responsibilities. *Figure 1.1* serves as a prime example of a P2P network architecture.

- On the other hand, *client/server* architecture revolves around the client/server relationship, where the client requests services from the server. This architecture involves establishing a centralized network that facilitates sharing network services between the server and the client. Typically, a client sends requests to a server using a defined protocol, seeking specific information or requesting an action, and the server responds accordingly. *Figure 1.2* provides an exemplary depiction of a client/server network architecture.

Understanding network architectures is crucial for comprehending network design, communication, and service provision between devices. P2P and client/server architectures are fundamental models in computer networking. However, network designs often incorporate elements from both paradigms, adopting a hybrid approach to meet specific requirements and enhance overall performance. It is important to note that P2P and client/server architectures are not mutually exclusive; they can be combined or customized based on a network's unique needs.

Various factors, including scalability, influence the choice of architecture, security considerations, and the types of services and resources used within the network. Scalability involves assessing the network's ability to handle increased demands and expand its capacity effectively. Security considerations revolve around protecting the network from unauthorized access, data breaches, and other threats. The nature of services and resources accessed within the network also plays a significant role in determining the most suitable architecture. Specific applications may be better suited to a P2P model, whereas others may require the centralized control and management provided by the client/server approach. Therefore, carefully evaluating

these factors is necessary to select the appropriate architecture that aligns with the network's requirements.

Peer-to-peer applications

The primary objective of **Peer-to-Peer** (**P2P**) networking is facilitating online file sharing. This functionality is made possible through peer applications, commonly called **P**eer-to-Peer **Applications** (**P2P apps**). Let us consider an illustrative scenario: when you use a P2P app to download a file from the internet, the file is acquired in fragments or chunks from multiple other peer computers connected to the same P2P network through the app. Simultaneously, the file stored on your computer is being uploaded to other peer computers currently downloading the same file. As a result, the network established by the P2P app enables two-way communication, allowing files to be exchanged and shared among peers in a decentralized manner.

P2P networking revolutionizes file sharing by leveraging participating peers' collective resources and bandwidth. Rather than relying on a central server for file distribution, P2P enables a distributed network where each peer contributes to downloading and uploading tasks. This approach enhances efficiency and resilience as the network becomes more robust with increased participation. However, it is essential to note that P2P networks can raise concerns regarding copyright infringement and the illegal sharing of copyrighted materials, which must be addressed and regulated to ensure responsible and lawful usage.

Network topologies

In addition to the different types of computer networks, another way to classify them is based on their topology, which defines the structural layout and interconnections of network components. There are two primary types of network topologies: physical topology and logical topology, each serving distinct purposes:

- *Physical topology* refers to the arrangement and placement of network components within a computer network. That includes positioning computers, peripheral devices, data transmission cables, and network devices. As the name suggests, physical topology focuses on the tangible and physical structure of the network. Common physical topologies include bus, ring, star, extended star, hierarchical, and mesh configurations, each with characteristics and advantages.

- Conversely, *logical topology* pertains to the communication pathways between network components. It describes how data accesses the transmission medium and how packets are transmitted within the network. Vital elements of logical topology include hostnames, IP addresses, and communication protocols that govern data flow. Logical topology concerns the logical connections and relationships between network devices, regardless of their physical arrangement.

Understanding a computer network's physical and logical topologies provides insights into how network components are physically organized and how data flows and communicates within the network. These categorizations assist in network design, troubleshooting, and optimizing network performance.

By examining the physical topology, one can determine the physical layout of devices, the distance between them, and the type of connections used. This knowledge aids in identifying potential points of failure and optimizing the network's physical Infrastructure.

On the other hand, understanding the logical topology reveals how devices communicate with each other, the paths data takes through the network, and the protocols used for data transmission. This information is crucial for troubleshooting network issues, ensuring efficient data flow, and implementing security measures.

Note: Combining physical and logical topologies allows a comprehensive understanding of a computer network's structure and functionality. Network administrators can effectively design and manage networks by considering both

aspects, leading to smooth operation and optimal performance. This holistic approach ensures the network is structured and configured to meet the organization's needs, facilitates efficient communication between devices, and maximizes resource utilization.

Types of physical topologies

As previously stated, the physical topology of a computer network refers to its physical arrangement or structure. This arrangement is commonly visualized using various shapes, including the bus, ring, star, extended star, hierarchical, and mesh topologies.

- In the *bus topology*, computers, peripheral devices, and network devices are interconnected using a shared communication channel called the *bus*. This bus is primarily constructed using a coaxial cable. In this topology, all devices are connected to the same cable, forming a linear structure. Each device taps into the bus to send or receive data. When a device transmits data, it is broadcast to all other devices on the bus, and each device checks if the data is intended for it. It is worth noting that the bus topology requires termination at both ends of the cable to prevent signal reflections. The entire network may also be affected if the cable breaks or fails.

- The *ring topology* involves arranging computers, peripherals, and network devices in a closed cycle, creating a *ring* network where each device is connected to its neighboring devices. Previously, coaxial cable was commonly used for this topology, but in modern dual-ring networks, optical fiber is used. In a ring network, data is transmitted unidirectionally, traveling from one device to the next until it reaches the intended destination. Each device on the ring receives the data and checks if it is the intended recipient. If not, it passes the data to the next device in the ring until it reaches the intended recipient. Dual-ring networks, which use optical fiber, offer increased reliability and performance compared to traditional coaxial cable rings. Two rings are established in these networks,

usually in opposite directions, allowing redundancy and fault tolerance. If a break or failure occurs in one ring, the data can be rerouted through the other ring, ensuring uninterrupted connectivity.

- The *star topology* independently connects computers, peripheral devices, and network devices to a central device. Each device directly links to the primary device in this configuration, forming a *star-like* structure. Typically, a twisted pair cable is the primary medium for this type of topology. In a star network, all communication between devices is routed through the central device, often called a hub or a switch. When a device wants to send data, it transmits it to the central device, which then forwards it to the intended recipient. This centralized communication pattern offers several advantages, such as easier management and fault isolation, as a failure in one device does not affect the operation of other devices in the network. The twisted pair cable, commonly used in star topologies, consists of pairs of insulated wires twisted together to reduce electromagnetic interference. This cable type is cost-effective and widely available, making it a popular choice for LANs and small-scale network deployments.

- The *extended star topology* combines elements of both *star* and *bus* topologies. This configuration connects computers, peripheral devices, and network devices in multiple star topology networks. These star networks are interconnected through a bus using central components such as switches. A twisted pair cable is primarily used to establish the star topology within the extended star. This cable type is commonly employed for its cost-effectiveness and availability. On the other hand, the bus topology within the extended star uses optical fiber. Optical fiber offers higher bandwidth and longer transmission distances, making it suitable for interconnecting the central components. In the extended star topology, data flows from individual devices to the main switches within their respective star networks.

The switches then route the data through the interconnected bus, allowing communication between machines across different star networks. By combining the star and bus topologies, the extended star topology provides scalability and flexibility. It allows for the expansion of the network by adding more star networks and interconnecting them through the bus. This design also enables fault tolerance, as the failure of a one-star network does not disrupt the entire network.

- The *hierarchical topology* is a combination of *star* and *bus* topologies. It is characterized by a hierarchical structure consisting of at least three levels. This topology uses multiple star topologies, where each star connects one or more nodes to a central primary node. All of these star topologies are then connected to the main trunk of the hierarchical structure, forming a tree-like configuration. Like the extended star topology, the hierarchical topology uses twisted pair cables for the star topologies. These cables are commonly used due to their cost-effectiveness and widespread availability. Additionally, optical fiber is employed within the hierarchical topology, likely for connecting the main trunk of the hierarchical structure. Optical fiber offers high bandwidth and long-distance transmission capabilities, making it suitable. The hierarchical topology enables efficient management and organization of network resources. The primary node at the top of the hierarchy is a central control point, facilitating communication and coordination between the star topologies and their connected nodes. Data can flow from the nodes to the main primary node and vice versa, allowing for the effective distribution of information. The hierarchical topology provides a scalable and structured approach to network design. It allows for the expansion of the network by adding more star topologies at different levels of the hierarchy. Additionally, this topology offers fault tolerance, as the failure of one-star topology or node does not affect the operation of other network parts.

- The *mesh topology* is characterized by a network configuration where each computer is directly connected to every other computer, forming a fully interconnected network. Mesh topologies are commonly used in WANs to connect LANs. In a mesh topology, each computer has a dedicated point-to-point connection with every other computer in the network. That means data can be directly transmitted from one computer to another without passing through intermediate devices. This direct connectivity offers high reliability and robustness, providing multiple paths for data to travel. Using mesh topologies in WANs allows for efficient interconnection of geographically dispersed LANs. The mesh topology enables seamless communication and data exchange across the entire network by establishing direct connections between computers in different LANs. It is worth noting that implementing a fully connected mesh topology can be resource-intensive and expensive, significantly as the number of computers in the network increases.

Internet Protocol addresses and subnets

For a computer to communicate within a computer network, it needs an **Internet Protocol** (**IP**) address. This address is typically assigned to the computer's **Network Interface Card** (**NIC**), which allows it to be identified on the network. In computer networking, two well-known IP addressing technologies are IPv4 and IPv6. While IPv6 is gaining popularity, it still plays a secondary role in the internet landscape, with IPv4 being the dominant and widely adopted technology.

Internet Protocol version 4

In the context of IPv4, **IPv4** stands for **Internet Protocol version 4**, commonly known as an IP address. IPv4 is the fourth version of IP addressing, as defined in the **Internet Engineering Task Force** (**IETF**) publication RFC 791. An IPv4 address or IP address is a 32-bit logical component within a computer network. It allows for approximately 4,294,967,296 unique IP addresses,

calculated as 2^32. The IP address is divided into four segments called octets, each consisting of 8 bits and decimal points separate these octets for more straightforward interpretation (for example, 192.168.1.1). *Figure 1.7* shows a manually assigned IPv4 address on a Windows Server 2022.

It is important to note that IPv4 addresses are limited in number, and as the demand for IP addresses continues to grow, the transition to IPv6 becomes crucial. IPv6 offers a significantly larger address space, providing an abundance of unique addresses and ensuring the scalability and future growth of the internet. However, due to the widespread adoption and compatibility challenges, IPv4 continues to dominate the current internet infrastructure.
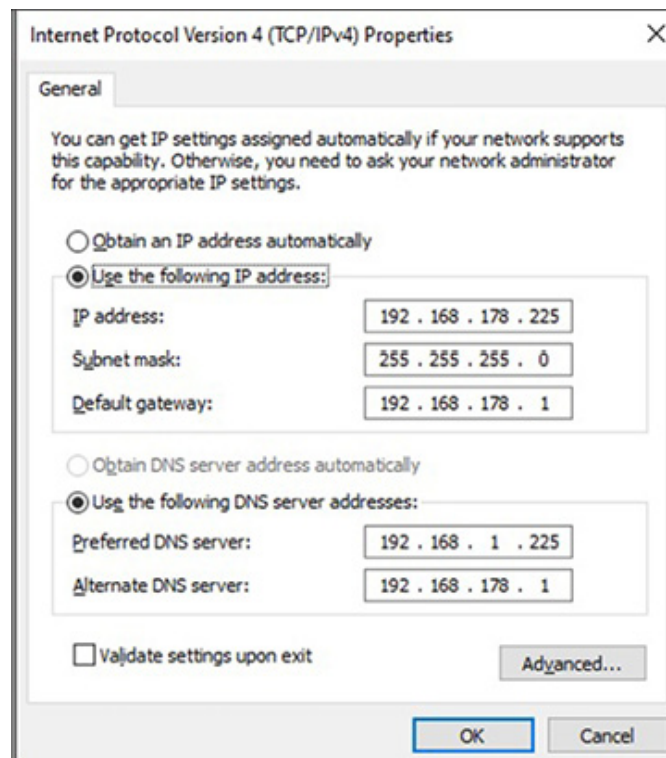
Figure 1.7: *The manually assigned IPv4 address in Windows Server 2022*

Internet Protocol version 6

The term **IPv6** in the network address refers to **Internet Protocol version 6**, the sixth iteration of IP addressing technology. It is defined in the IETF publication RFC 2460. Unlike

IPv4, IPv6 utilizes a 128-bit address structure divided into eight hextets, each consisting of 16 bits. The hextets are separated by colons for more straightforward interpretation (for example, 2001:0DB8:85A3:0000:0000:8A2E:0370: 7334). Due to its 128-bit structure, IPv6 can accommodate approximately 340 undecillion addresses, representing many available IPv6 addresses. *Figure 1.8* shows a manually assigned IPv6 address on a Windows Server 2022:
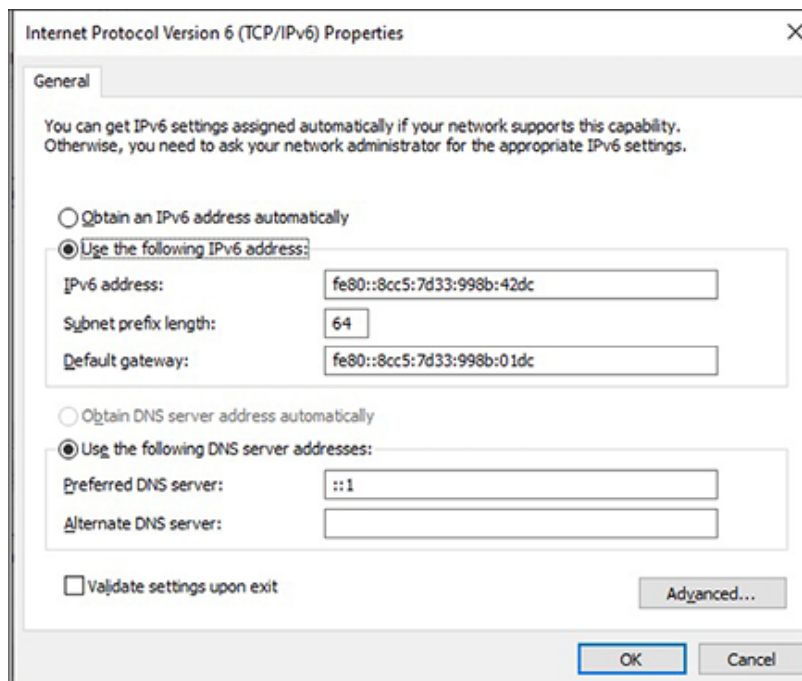
Figure 1.8: The manually assigned IPv6 address in Windows Server 2022

Subnets

In computer networks, subnets are commonly used with IP addresses to identify specific networks within a more extensive network. Subnetting involves dividing a larger network into smaller, logically separated networks. The subnet mask plays a crucial role in identifying the network and determining its size by combining it with the IPv4 address. That allows for the designation of a network's network address, host address, and broadcast address.

The Internet Engineering Task Force's RFC 791 document categorizes IP addresses into 8-bit, 16-bit, or 24-bit prefixes, forming the classful addressing system that classifies IP addresses into classes A, B, C, D, and E. Classes A, B, and C are commonly used in everyday operations. Class D is reserved for multicasting, and Class E is designated for research and experimentation. The classful addressing system divides the IP address into the network and host portions based on its specific class. *Table 1.1* provides the default subnet masks for each class of IPv4 addresses, following the concept of classful subnetting:

Classes of IPv4	Default subnet masks
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Table 1.1: *The IPv4 default subnet masks*

Note: For more in-depth information regarding IPv4 addressing technology, the depletion of address space, and the categorization of networks based on their address space, refer to **https://blogs.igalia.com/dpino/2017/05/25/ipv4-exhaustion/**.

Network operating system

Similar to a computer, a server operates using an **Operating System** (**OS**) that enables it to deliver network services. Specifically, a **Network Operating System** (**NOS**) is software designed to manage, maintain, and provision resources within a network. In addition to resource management, an NOS can facilitate file and application sharing, provide Web services, control resource access, manage users and computers, offer configuration tools, and perform other tasks related to network resources. The presence of a NOS is essential for effectively managing computer network resources.

In recent years, versions of Windows Server, Linux Server, and macOS Server have been recognized as NOS due to their ability to offer network services. However, recent advancements in

client device operating systems, such as Windows 10/11, Linux Ubuntu, and macOS, have made them equally capable of providing network services. Consequently, these client OS versions can also be considered NOS. This expanded scope of NOS capabilities is depicted in the following points.

Windows server

Windows Server (as shown in *Figure 1.9*), developed by Microsoft, debuted in the early 1990s with Windows NT 3.5 and has seen subsequent releases. Initially, it was a **Graphical User Interface** (**GUI**) based system, similar to most Windows operating systems. However, with the introduction of Windows Server 2008, Microsoft also offered a Server Core edition, a **Command Line Interface** (**CLI**) based operating system. From Windows Server 2003 to Windows Server 2008, the architecture supported both 32-bit and 64-bit versions. However, starting from the Windows Server 2012, it has exclusively been a 64-bit operating system.

The native file system used in Windows Server is the **New Technology File System** (**NTFS**). However, with the release of Windows Server 2012, the **Resilient File System** (**ReFS**) was introduced, primarily designed for network-intensive applications. This addition expanded the capabilities of Windows servers to cater to a broader range of network needs.

Windows server is widely used in on-premises environments to provide network services for Windows and non-Windows systems. However, it has also become famous for running **Virtual Machines** (**VMs**) in the **Infrastructure as a Service** (**IaaS**) cloud environment. That demonstrates the adaptability and versatility of Windows Server in meeting the evolving demands of modern computing environments. Please refer to the following figure:

Figure 1.9: *The Windows Server 2022 Datacenter edition*

Note: You can find a comprehensive overview of ReFS at the following link: **https://docs.microsoft.com/en-us/windows-server/storage/refs/refs-overview**.

Linux server

The Linux server (see *Figure 1.10*) has its roots in the desire to enhance the functionality of an existing operating system called MINIX. However, instead of improving MINIX, Linus Torvalds took the initiative to create a new operating system in the early 1990s, which he named Linux. The GNU GPL project then took charge of licensing the new OS. Over time, the Linux penguin became the iconic mascot of the operating system. Various events and activities, such as the publication of the first Linux booklet and the creation of Linux-themed magazines, contributed to the formation of the Linux community, which has become one of the largest volunteer communities worldwide.

Today, Linux servers are widely used due to their emphasis on security and open-source nature. Linux powers a significant number of Web servers and supercomputers globally. The robust security features and the collaborative nature of open-source development have contributed to its popularity and widespread adoption. As a result, Linux has become a go-to choice for server applications, offering stability, flexibility, and the ability to be

customized based on specific needs. Please refer to the following figure:

Figure 1.10: *The Ubuntu Server distro*

Note: Linux is a widely recognized and widespread family of operating systems that has garnered numerous volunteers and contributors. Its impact on the world of operating systems is unparalleled, with no other technological initiative attracting such a significant level of participation. If you want to learn how to operate Linux distributions on Windows Server 2019, you can find detailed instructions at **https://docs.microsoft.com/en-us/windows/wsl/install-on-server**.

Mac OS X Server

Although Mac OS X Server may have a smaller market share than Windows Server and Linux Server operating systems, its notable strength lies in its reliability. Built upon a modified Unix OS foundation, the Mac OS X Server maintains the familiar Apple **Graphical User Interface** (**GUI**) that Mac users are accustomed to. Like Windows and Linux, macOS Server is available in 32-bit and 64-bit versions. However, due to Apple's adoption of Intel processors for their computers and servers, macOS Server is exclusively distributed in a 64-bit format. That ensures compatibility and optimized performance on Apple's hardware architecture. Please refer to the following figure:

Figure 1.11: *The Mac OS X Server version*

Note: Years ago, Apple discontinued the Mac OS X Server and started offering the macOS Server instead through the App Store. However, as of April 2022, even macOS Server has been discontinued. Despite this, customers with macOS servers can still download and use the software on macOS Monterey. To gather further information about macOS servers, visit **https://support.apple.com/guide/server/welcome/mac**.

Technology trends

We are currently experiencing the **Internet of Things** (**IoT**) era, where the Internet significantly impacts our daily lives and work. This transformation has turned what was once science fiction into reality. The rapid advancement of technology has created a constantly evolving environment, necessitating everyone to adapt to this new reality. In the realm of computer networks, several current trends are worth noting:

- Improved security has become the utmost priority for enterprise networks. The increasing number of users and the growing sophistication of cybercriminal attacks have heightened the need for enhanced security measures.

- Increased bandwidth ranks as the second priority for enterprises, right after security. The escalating demands for data traffic put significant pressure on networks, necessitating higher bandwidth to handle the increasing load.

- **Software-defined networks** (**SDNs**) are gaining popularity, particularly among enterprises. SDNs offer multiplexing capabilities, which enable better performance by efficiently using multiple physical links for data transmission.

- Video communication has revolutionized distance communication, making it more appealing and opening online collaboration and entertainment opportunities.

- Online collaboration, including video communication, brings people together for joint projects. Businesses, educational institutions, and individuals embrace this trend.

- **Bring Your Own Devices** (**BYOD**) is a network trend allowing users to use their personal devices to access business data. This approach gives users freedom, flexibility, and more opportunities while accessing resources.

- Cloud computing has transformed how we access and store data and reshape the internet. From businesses to individuals, cloud computing offers on-demand services securely and economically accessible from any device, anywhere in the world.

These trends reflect the ongoing evolution of computer networks, driven by the need for enhanced security, higher bandwidth, advanced communication methods, collaborative tools, and the flexibility provided by cloud computing. Adapting to and leveraging these trends can help organizations and individuals thrive in the ever-changing technological landscape.

Conclusion

In conclusion, this chapter provided an overview of computer networks and explored various types of networks, including PAN, LAN, CAN, MAN, and WAN. Additionally, the chapter introduced network components such as hosts, nodes, clients, and servers, along with discussing network architecture, topology, IP

addressing, subnetting, and NOS. The differences between peer-to-peer and client/server networks and physical and logical topologies were also covered. Furthermore, the chapter discussed IPv4 and IPv6 addressing technologies. It explained the different IPv4 classes from A to E. The chapter concluded with a practical exercise on enabling Hyper-V Client using Settings and Windows PowerShell, preparing you for the upcoming chapter focusing on server hardware and Windows Server 2022. This comprehensive coverage equips you with the foundational knowledge to delve into the subject of server hardware and explore the functionalities of Windows Server 2022.

Exercise 1.1—Enabling Hyper-V using settings

Windows 10/11 Pro includes a feature called Hyper-V Client that allows virtualization. Microsoft's Hyper-V was introduced in Windows Server 2008 and is a successor to Windows Virtual PC. Over time, Hyper-V has gained popularity among system administrators, becoming a strong contender against VMware in the virtualization platform market. Hyper-V offers various services for creating and managing **Virtual Machines** (**VMs**) and their resources. To enable the Hyper-V Client in Windows 11 Pro, follow the following steps within the settings menu.

1. Click on the **Start** button and then the **Settings** within the **All Apps** section of the **Start** menu.

2. In the Settings navigation menu, click on **Apps** and select the **Optional features** from the list.

3. Scroll to the bottom and select the **More Windows features** from the **Related settings** section**.**

4. The **Windows Features** window opens, allowing you to **Turn Windows features on or off**. Then, search for **Hyper-V** and click its check box. Ensure that both **Hyper-V Management Tools** and **Hyper-V Platform** are checked, as shown in *Figure 1.12*:
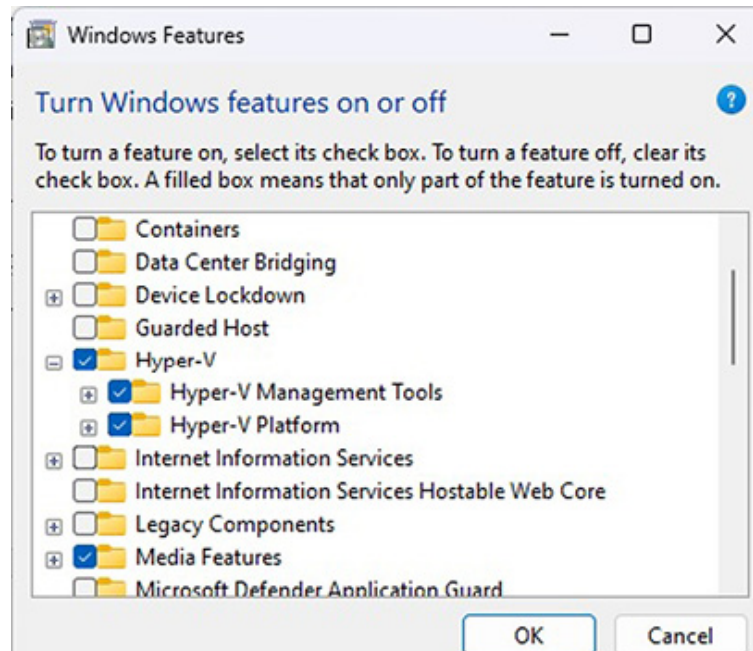
Figure 1.12: *Enabling Hyper-V Client using settings.*
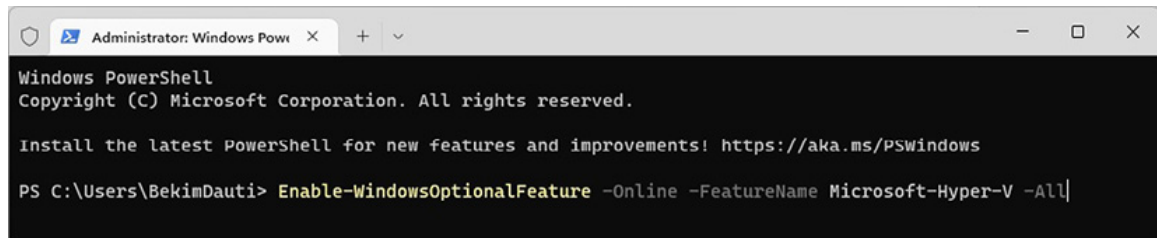
5. Click on the **OK** button. Shortly after that, the **Windows Features** will begin applying changes. Once completed, **Windows Features** displays the message **Windows completed the requested changes**.

6. Click on the **Restart Now** button to restart the computer.

Exercise 1.2—Enabling Hyper-V using PowerShell

This exercise involves enabling the Hyper-V Client feature on Windows 11 Pro using Windows PowerShell. To accomplish this, follow the provided instructions as follows:

1. Right-click the **Start** button, select Terminal (Admin) from the **administrator's menu**, and select **Terminal (Admin)**.

2. The **User Account Control** window opens to confirm whether **you want to allow that application to make changes to your device**. Click on the **Yes** button shortly after the **Windows PowerShell** window opens.

3. In **Windows PowerShell**, enter the following cmdlet and press **Enter**. Refer to *Figure 1.13*.

```
Enable-WindowsOptionalFeature -Online -FeatureName
Microsoft-Hyper-V -All
```


Figure 1.13: Installing Hyper-V Client using the Windows PowerShell

4. Shortly after the execution of the cmdlet, the installation of the **Hyper-V Client** will begin. Once completed, enter the following cmdlet to reboot the computer:

```
Restart-Computer -ComputerName ComputerName -Force
```

Questions

1. In your own words, define a computer network.
2. How many types of computer networks can you name?
3. How many types of network components can you name?
4. List three differences between IPv4 and IPv6 addressing technologies.
5. In your own words, define a Network Operating System (NOS).

CHAPTER 2
Introduction to Windows Server 2022

Introduction

This chapter will explore Windows Server 2022, Microsoft's latest server operating system. Before diving into the details of Windows Server 2022, it is essential to understand the hardware characteristics specific to servers, as this differentiation is crucial for businesses. This chapter will overview server hardware and software, distinguishing them from PC hardware and software. The chapter will then proceed to provide an overview of Windows Server 2022, including its release timeline, various editions available, and the introduction of the Azure edition, which integrates cloud computing capabilities. A comparison will be made between Windows Server 2022 and its predecessor, Windows Server 2019, to highlight the new features and enhancements introduced in the latest version. When deploying Windows Server 2022, administrators must be aware of the minimum and recommended system requirements to ensure optimal performance. These requirements will be discussed to assist administrators in making informed decisions during deployment. To conclude the chapter, a step-by-step guide will be provided for downloading Windows Server 2022 and Windows Admin Center. This exercise will offer practical guidance on acquiring the necessary software components for implementing Windows Server 2022 effectively.

Structure

In this chapter, we will cover the following topics:

- Server hardware and its specifics
- Overview of Windows Server 2022
- Editions of Windows Server 2022
- Comparing Windows Server versions
- System requirements
- New features in Windows Server 2022

Objectives

This chapter aims to provide you with knowledge about server hardware. You will gain an understanding of the critical components of server hardware, namely, the processor, memory, disk, and network interface. In addition to exploring server hardware, the chapter will introduce you to Windows Server 2022. This introduction will cover essential aspects such as the release timeline, different editions available, updated features, and the system requirements for Windows Server 2022. To conclude this chapter, you will have the opportunity to participate in an exercise where you will download Windows Server 2022 and Windows Admin Center from the internet. This exercise will allow you to apply the knowledge gained in the chapter practically.

Server hardware and its specifics

Servers, like personal computers, are composed of similar components, including hardware and software. These components represent the physical and logical aspects of a server. However, servers require more advanced hardware and software than personal computers because of their primary role in providing client network services. This distinction between PCs and servers at the hardware and software level is essential.

In a business environment, personal computers are typically used as workstations by users, whereas servers are responsible for

supplying network services accessed by those users through their computers. Consequently, server hardware must be robust and high-quality to support continuous network operations. For instance, a database server requires significant memory and storage capacity. Therefore, the performance and quality of the processor, memory, disk, and network interface are critical factors that influence the overall performance of a server.

Four critical hardware components

To ensure optimal server performance for both standard and demanding workloads, it is recommended to regularly assess and monitor the performance of these four key hardware components. By doing so, any potential bottlenecks or issues can be identified and addressed promptly, allowing the server to function at its best capacity.

- *The processor,* or the **Central Processing Unit** (**CPU**), is a chip on a server's motherboard (see *Figure 2.1*), similar to a **persoanl computer** (**PC**). Often referred to as the "brain" of the server, the processor is responsible for managing all data processing and computations. Popular processor manufacturers for both PCs and servers include Intel and AMD. Their latest processors are designed based on 64-bit architecture, which differs from older processors built on 32-bit architecture. In 64-bit architecture, each communication session between the processor and RAM involves the exchange of 64 bits of data. In contrast, 32-bit architecture exchanges only 32 bits of data per communication session between RAM and the processor. As a result, the data communicated through 32-bit architecture is halved compared to 64-bit architecture. Using 64-bit architecture allows for a more efficient and higher-capacity data exchange between the processor and RAM. This improved data processing capability contributes to enhanced performance and increased system responsiveness in server operations. Please refer to the following figure:
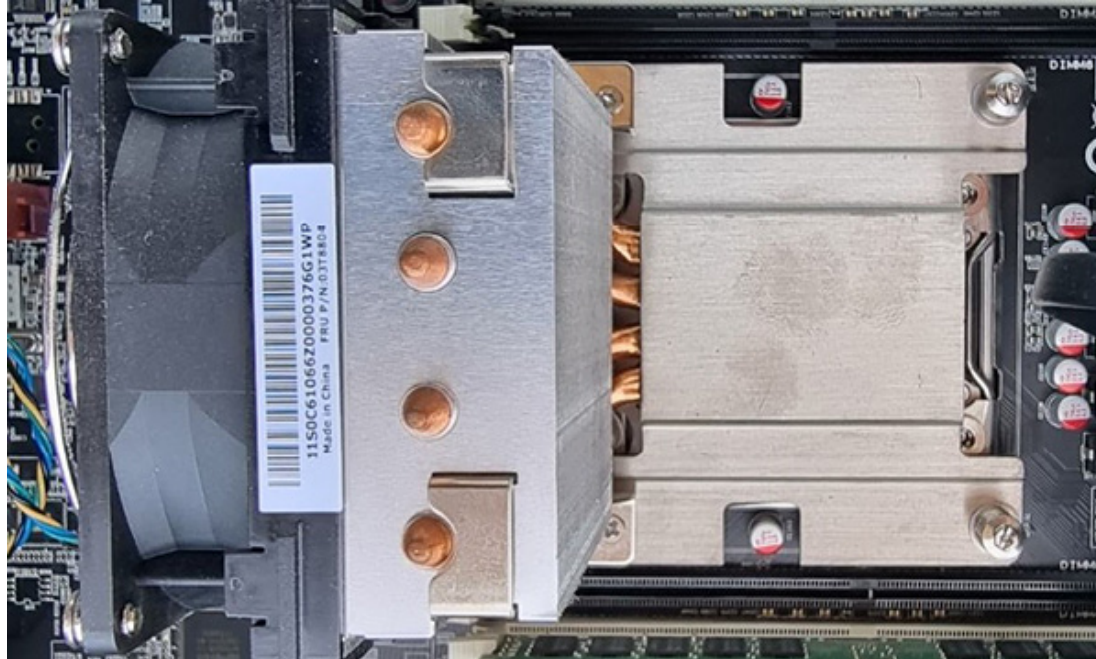
Figure 2.1: *A processor in a motherboard*

Note: When comparing the processing capabilities of Windows Server 2022, it is noteworthy that the 64-bit edition can handle double the amount of data compared to the 32-bit edition of the same operating system. That implies that, when installed on identical hardware, the 64-bit edition of Windows Server 2022 has the advantage of processing a significantly larger volume of data, offering improved performance and capacity in handling computational tasks.

- **Random Access Memory** (**RAM**), as shown in *Figure 2.2*, serves as the server's working memory, playing a crucial role in the smooth operation of Windows Server 2022 and its applications. Having an ample amount of RAM is essential for optimal performance. With increased RAM capacity, Windows Server 2022 can operate comfortably, and applications specifically designed for servers can run more smoothly. RAM is a hardware component heavily used by the server's operating system and applications. It serves as a temporary storage space for data actively being processed by the server. When RAM is available, the server can efficiently handle multiple tasks and accommodate the operating system's and applications' memory requirements. This results in improved responsiveness, reduced latency, and overall better performance. By increasing the RAM on a server, administrators can enhance their capability to

handle a more significant workload and accommodate resource-intensive applications. That ensures the server's performance remains optimal, even under demanding conditions. Please refer to the following figure:
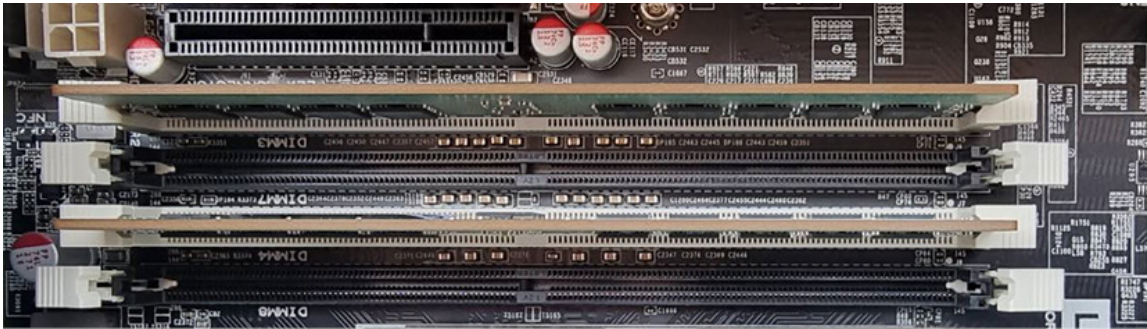
Figure 2.2: *RAM modules in a motherboard*

- The *disk* (see *Figure 2.3*) serves as the hardware component responsible for permanent data storage. In the context of a server, it typically consists of multiple disks, forming the server's disk subsystem. Just as the suitability of 64-bit architecture was established for the processor, and a larger RAM capacity was emphasized, it is essential to consider the read/write operations for the disk. Efficient read/write operations on the disk are crucial for optimal data transfer. Faster read/write speeds allow for more rapid and efficient reading and writing of data to and from the disk. That is significant as it enables the server to process more data within shorter time frames, ultimately enhancing overall performance. To ensure efficient disk operations, several factors should be considered. These include selecting disks with higher read/write speeds, utilizing disk configurations such as **Redundant Array of Independent Disks** (**RAID**) for improved performance and data redundancy, and enploying caching mechanisms to accelerate data access. By prioritizing fast read/write operations and implementing appropriate disk configurations, administrators can maximize the server's ability to read and write data efficiently. That facilitates smooth operations, faster data processing, and enhanced server performance. Please refer to the following figure:
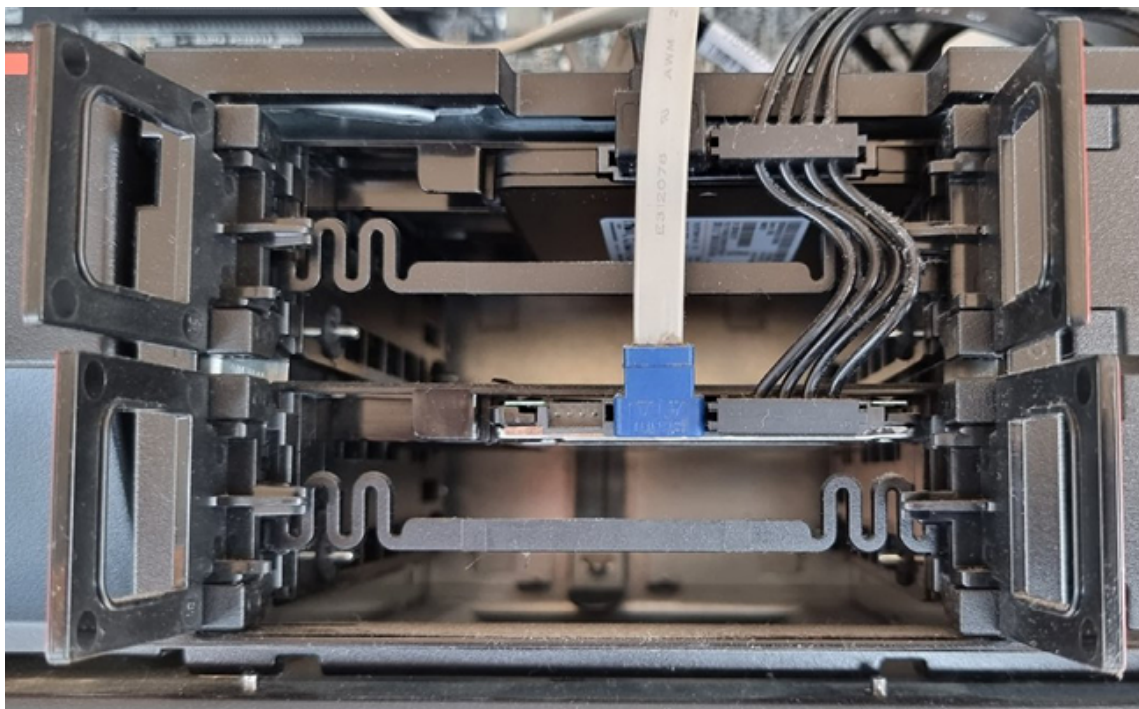
Figure 2.3: SSD disks on a tower server

- As mentioned in *Chapter 1, Understanding Networks and their Components,* the *network interface* allows the server to establish connections with an organization's **Local Area Network** (**LAN**) and the Internet. Typically, a server is equipped with multiple network interfaces, as shown in *Figure 2.4*. The speed of the server's network connection plays a crucial role in determining its data transfer capabilities. A faster network connection speed enables the server to efficiently send and receive data between the intranet (the organization's internal network) and the internet. A higher network connection speed translates to the server's ability to handle larger volumes of data and perform data transfers faster. That is particularly important for servers that deal with heavy network traffic or require swift access to external resources. By ensuring a fast network connection speed, the server can effectively meet the demands of users accessing network services and applications. It allows for smooth and uninterrupted communication between the server, the LAN, and the internet. Please refer to the following figure:

Figure 2.4: *Network interfaces on a server*

The server's size and form factor

Apart from those mentioned previously, four critical hardware components, a server's size, and form are equally important factors. The size of the server refers to the dimensions of its hardware components. At the same time, the form factor encompasses the overall appearance and structure of the server, including its size, configuration, and physical layout. Let us explore these considerations in more detail:

- As the name implies and depicted in *Figure 2.5*, a *rack-mountable server* is specifically designed to be installed and secured within a rack framework. This server type is commonly used in on-premises server rooms or data centers.

Figure 2.5: *A rack-mountable server*

- On the other hand, a *blade server* operates differently by using a compact module known as a blade inserted into a server chassis. This configuration allows space and power efficiency, as the blade server is designed to be mounted within a rack. Blade servers are commonly deployed in data centers and supercomputer facilities, where maximizing space and power utilization is paramount.

- Finally, depicted in *Figure 2.6*, the *tower server* is a standalone unit that stands vertically. This server type is commonly used for testing purposes or to provide local services in a **Small Office/Home Office** (**SOHO**) setting.

Figure 2.6: *The tower server under the desk*

Overview of Windows Server 2022

Throughout its 30-year history since the introduction of Windows NT, Microsoft has demonstrated a remarkable ability to adapt to evolving network service demands within its Windows Server operating systems. As a result, the timeline of Windows Server development showcases an exciting progression. *Table 2.1* illustrates the impressive evolution of Windows Server technology over time:

Server for the Masses era 1996-2000	Enterprise era 2000–2008	Datacenter era 2009–2013	Cloud for the Masses era 2016- present
• Windows NT Server 3.5 • Windows NT Server 4.0	• Windows 2000 Server • Windows Server 2003	• Windows Server 2008 • Windows Server 2012	• Windows Server 2016 • Windows Server 2022 • Windows Server 2022

Table 2.1: *Windows Server 2022 timeline*

Figure 2.7 illustrates the Start menu and desktop of *Windows Server 2022*, the latest iteration of Microsoft's server operating system belonging to the Windows NT family. The preview program for Windows Server 2022 commenced in March 2021, followed by its official release on August 18, 2021. The general availability of the operating system was announced on September 1, 2021, accompanied by a launch event as part of the Windows Server Summit on September 16, 2021. Like its predecessors, Windows Server 2016 and Windows Server 2019, Windows Server 2022 is built upon the codebase of Windows 10 and shares the version number of the Windows November 10, 2021, Update, 21H2.

Refer to *Figure 2.7:*
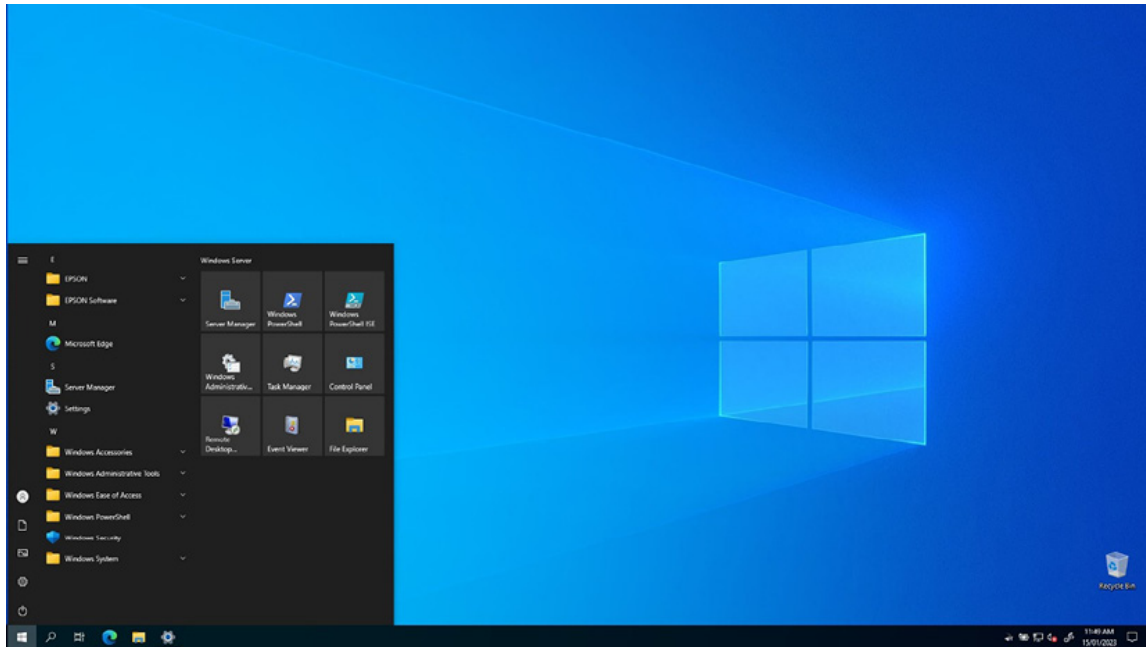
Figure 2.7: *Start menu and desktop in Windows Server 2022*

Cloud-oriented Windows Server

In the current era of cloud computing, a server operating system must be equipped to support cloud-based environments. When Microsoft released the Windows Server 2016, it was explicitly marketed as "Windows Server for the Cloud." As cloud computing has matured, Microsoft has introduced Windows Server 2022 to address the evolving needs of cloud-based infrastructure.

Windows Server 2022 is designed to be more secure, flexible, and robust, catering to modern cloud computing requirements. It supports hybrid deployments through a dedicated edition called Windows Server 2022 Datacenter Azure. Compared to its predecessor, Windows Server 2019, Windows Server 2022 introduces enhancements in several critical areas such as security, secure connectivity, Azure hybrid capabilities, application platform, and storage.

Furthermore, with the integration of Microsoft Azure, Windows Admin Center has transformed into a modern management platform. That allows businesses to efficiently manage, configure, and integrate workloads running on Windows Server 2022,

offering enhanced ease of use and seamless integration with cloud-based services.

Note: Besides Remote Server Administration Tools (RSAT), Microsoft has introduced Windows Admin Center, a new server management tool with an interface similar to Azure. This tool allows for the management of multiple servers. Once you have installed Windows Server 2022 and have access to the desktop, the Windows Admin Center dialog box will appear. It is free and can be downloaded from **https://www.microsoft.com/en-us/windows-server/windows-admin-center**.

Editions of Windows Server 2022

Like its predecessors, Windows Server 2016 and Windows Server 2019, Windows Server 2022 offers a range of editions tailored to different enterprise requirements. The available editions of Windows Server 2022 include the following:

- **Windows Server 2022 Datacenter Azure edition**: This new edition is specifically designed to enable enterprises to leverage the benefits of cloud computing through Azure Automanage. It provides enhanced integration and features for seamless integration with Azure services.

- **Windows Server 2022 Datacenter**: This edition is comprehensive and suitable for enterprises with highly virtualized data centers or those acting as cloud providers. It offers advanced capabilities and scalability for demanding server environments.

- **Windows Server 2022 Standard**: This edition is feature-rich and caters to medium-sized businesses with on-premises servers. It provides a comprehensive set of functionalities for their server infrastructure needs.

- **Windows Server 2022 Essentials**: This edition targets small businesses with a single server in their IT infrastructure. It offers essential features and is designed to meet the specific requirements of small-scale deployments.

- **Microsoft Hyper-V Server 2022**: This free product delivers enterprise-class virtualization capabilities for data centers and hybrid clouds. It allows organizations to

leverage the benefits of virtualization technology without additional licensing costs.

These different editions of Windows Server 2022 cater to a diverse range of enterprise needs, ensuring that organizations of various sizes and infrastructure requirements can choose the most suitable version for their specific use cases.

Comparing Windows Server versions

While Windows Server 2022 and Windows Server 2019 may appear similar initially, a closer analysis reveals significant enhancements and novel features in Windows Server 2022. This section outlines the key distinctions between these two operating systems, emphasizing the most noteworthy differences.

Windows Server 2022 introduces significant enhancements and new features, including hybrid cloud capabilities, security, Hyper-V Manager, platform flexibility, Windows Admin Center, and Kubernetes experience. These improvements contribute to an elevated user experience and enhanced performance. The following are the key highlights:

- **Hybrid cloud capabilities**: Windows Server 2022 enhances Azure Arc with enabled HTTPS and TLS 1.3, improving deployment and management of Storage Migration Services. The introduction of Azure Automanage unlocks additional capabilities for the Windows Server 2022 Datacenter Azure edition, including Hot Patch, **Server Message Block** (**SMB**) over **Quick UDP Internet Connections** (**QUIC**), and an extended network for Azure.

- **Improved security**: Windows Server 2022 offers advanced security features such as Hypervisor-based code integrity, Secured-core server, and Hardware-enforced stack protection. It also runs TLS 1.3 by default, ensuring secure communications.

- **Upgraded Hyper-V manager**: Windows Server 2022 enhances the Hyper-V Manager with features such as the Action bar, Live storage migration, Affinity and anti-affinity rules, VM clones, and a new partitioning tool. These

additions enhance the management and flexibility of virtualized environments.

- **Improved platform flexibility**: Windows Server 2022 introduces support for **Dynamic Source Routing** (**DSR**) and **Domain Joining for Group Managed Service Accounts** (**gMSA**). It also includes improvements in the virtualized time zone and reduces the uncompressed image size, contributing to enhanced platform flexibility.

- **Enhanced Windows Admin Center**: The Windows Admin Center in Windows Server 2022 offers automatic updates, automated extension lifecycle management, event workspace tracking, customizable columns for VM information, and a built-in detachable events overview screen. These improvements simplify management tasks and enhance the administrative experience.

- **Improved Kubernetes experience**: Windows Server 2022 provides an improved Kubernetes experience, featuring HostProcess containers and Multiple subnets. These enhancements enhance containerization capabilities and facilitate efficient networking within Kubernetes clusters.

Overall, Windows Server 2022 introduces notable advancements and features that enhance hybrid cloud capabilities, security, virtualization management, platform flexibility, administration, and Kubernetes experience. These improvements cater to the evolving needs of modern server environments and offer enhanced performance, security, and flexibility for organizations deploying Windows Server 2022.

System requirements

Before delving into the specifics of the minimum and recommended system requirements, it is crucial to understand their significance. The minimum standards pertain to the hardware necessary for installation, whereas the recommended requirements correspond to the hardware that ensures an optimal user experience. Familiarizing oneself with these requirements

enables IT professionals to select suitable hardware based on the intended services they aim to deploy.

According to the information provided by Microsoft, Windows Server 2022 shares the exact minimum hardware requirements as its predecessor, Windows Server 2019. That indicates that the hardware specifications needed for installation remain unchanged between these two versions.

Minimum system requirements

The following are the minimum system requirements for Windows Server 2022, along with some additional details:

- **Processor**: A 64-bit processor with a clock speed of 1.4 GHz.

- **RAM**: 512 MB of memory, although it is recommended to have 2 GB if choosing the Server with a desktop experience installation option.

- **Disk space**: At least 32 GB of available storage space.

- **Network**: An Ethernet adapter capable of achieving a minimum throughput of 1 Gbps.

- **Graphics Device and Monitor**: A graphics device and monitor can display a resolution of Super VGA (1,024 × 768) or higher.

- **Other hardware**: It is necessary to have a DVD drive if installing from DVD media. A keyboard, mouse (or compatible pointing device), **Trusted Platform Module** (**TPM**), and internet access are required.

These minimum system requirements outline the baseline specifications for running Windows Server 2022 on a system. It is essential to ensure that the hardware components meet or exceed these requirements to ensure proper installation and functionality of the operating system.

Recommended hardware requirements

The following are the recommended hardware requirements for Windows Server 2022, along with some additional details:

- **Processor**: A 64-bit processor with a clock speed of 2.0 GHz or higher.

- **RAM**: A recommended minimum of 32 GB of memory or higher for optimal performance.

- **Disk space**: It is recommended to have a 256 GB **Solid State Drive** (**SSD**) and a 1 TB **Hard Disk Drive** (**HDD**) for storage.

- **Network**: An Ethernet **Network Interface Card** (NIC) can achieve at least 1 Gbps throughput.

- **Graphics Device and Monitor**: A graphics device and monitor can display a resolution of Super VGA (1,024 × 768) or higher.

- **Other hardware**: It is necessary to have a DVD drive and a keyboard, mouse (or compatible pointing device) for input.

These recommended hardware requirements guide achieving optimal performance and capabilities when running Windows Server 2022. Meeting or exceeding these recommendations is advisable to ensure smooth operation and accommodate potential resource-intensive tasks or workloads.

New features in Windows Server 2022

While Windows Server 2022 shares standard features with its predecessor, Windows Server 2019, it also introduces significant innovations and enhancements. The notable advancements in Windows Server 2022 include the following.

Microsoft Edge

Figure 2.8 showcases Microsoft Edge, which uses Google's Chromium engine and benefits from Microsoft's commitment to security and innovation. In Windows Server 2022, Microsoft Edge (Chromium) is the default Web browser, replacing the previously retired internet Explorer. This updated browser is available for use

in the Desktop Experience installation option. Please refer to the following figure:
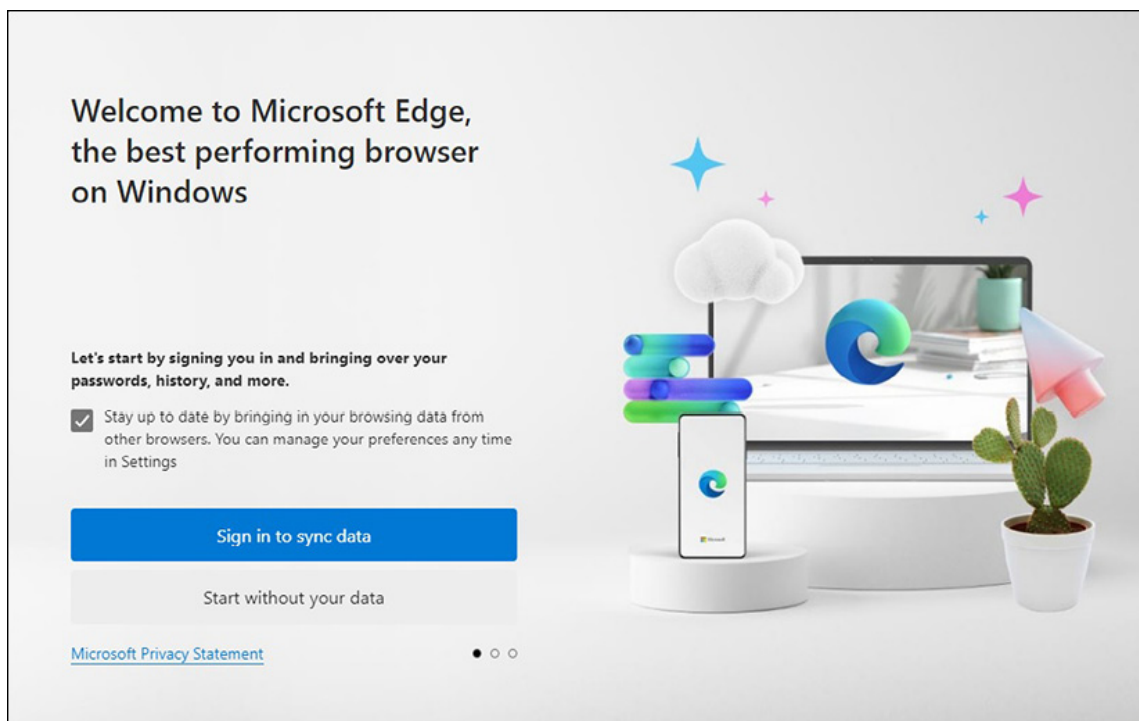

Figure 2.8: *Microsoft Edge in Windows Server 2022*

Azure Hybrid Center

Figure 2.9 depicts the *Azure Hybrid Center*, a centralized hub facilitating seamless access to a comprehensive range of integrated services within Azure. This hub enables enhanced connectivity between on-premises servers and cloud services. It provides access to various Azure offerings such as Azure Automanage, Azure Arc, Azure Backup, File Sync, Disaster Recovery, and other essential cloud services. The Azure Hybrid Center is vital in establishing efficient and integrated connections between on-premises infrastructure and the Azure cloud platform. Please refer to the following figure:
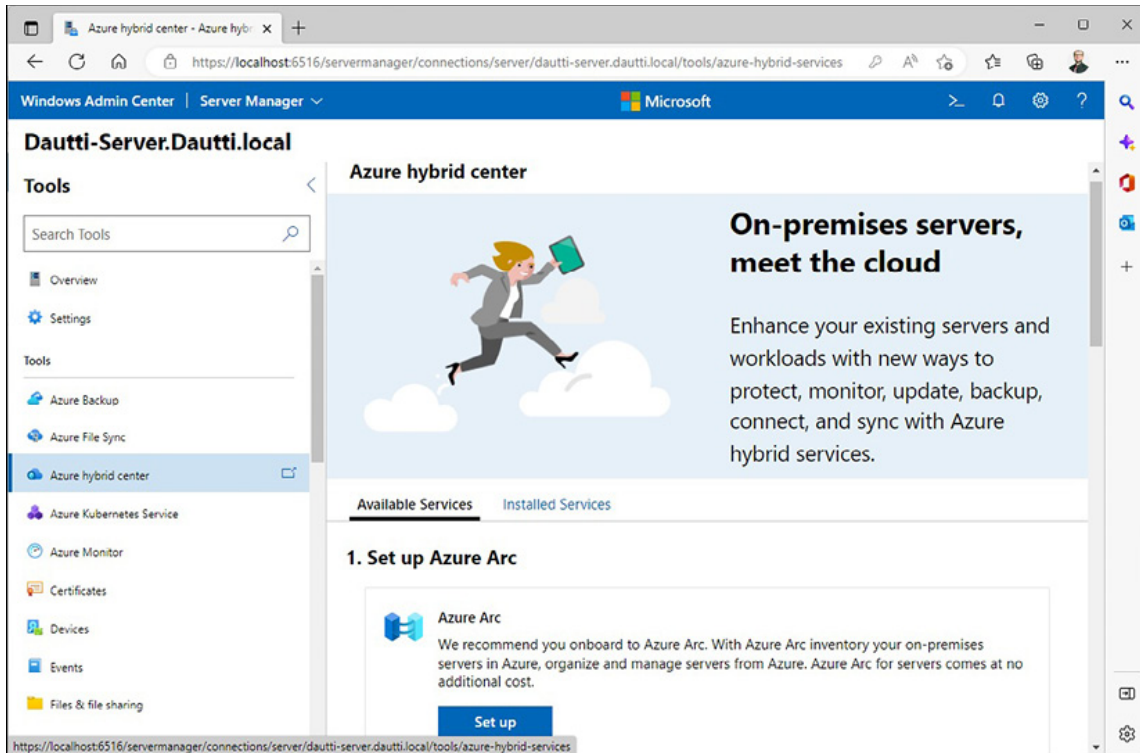
Figure 2.9: The Azure hybrid center in Windows Server 2022

Secured-core server

Figure 2.10 showcases the *secured-core server*, a newly introduced feature in Windows Server 2022 that offers robust protection against various threats by implementing multi-layered security measures across hardware, firmware, and the operating system. This innovative feature leverages technologies such as **Trusted Platform Module** (**TPM**) 2.0 and System Guard to ensure secure booting of Windows Server, significantly reducing the risks associated with firmware vulnerabilities and mitigating the potential disruptions caused by malicious threats. By incorporating the secured-core server feature, organizations can enhance their security posture and strengthen their defense against possible security breaches. Please refer to the following figure:
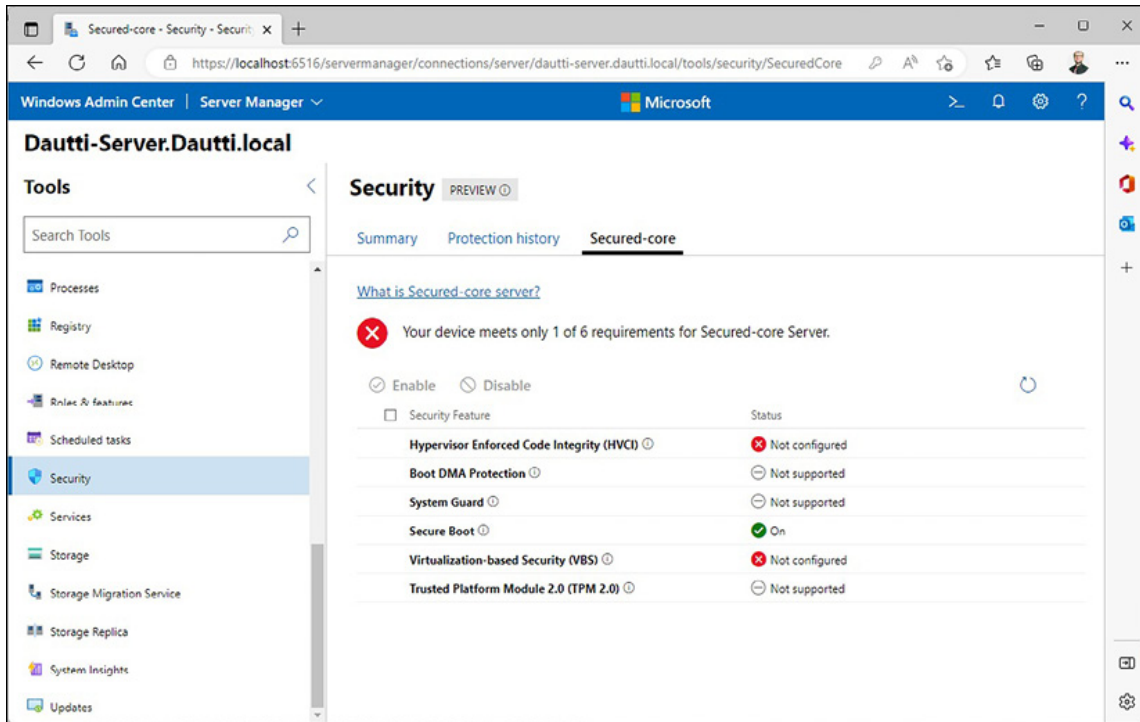
Figure 2.10: *Secured-core server in Windows Server 2022*

Conclusion

This chapter has presented comprehensive information on Windows Server 2022, the latest iteration of **Microsoft's Network Operating System** (**NOS**), which belongs to the Windows NT family. This chapter began by exploring server hardware's significance and various components, emphasizing their crucial role in achieving optimal server performance. Subsequently, an overview of Windows Server 2022, including its timeline, was provided, accompanied by a comparison between Windows Server 2019 and Windows Server 2022. Additionally, the chapter delved into the essential aspects of minimum and recommended system requirements, crucial considerations for system administrators when deploying Windows Server 2022.

Furthermore, this chapter introduced readers to a few new features in Windows Server 2022, such as the incorporation of Microsoft Edge (Chromium), the Azure hybrid center's presence, and the Secured-core server's introduction. These enhancements aim to enhance user experience, facilitate seamless integration

with cloud services, and fortify overall system security. Finally, an exercise was included in this chapter, guiding readers through downloading Windows Server 2022 and the Windows Admin Center, preparing them for the subsequent installation of Windows Server 2022 in the upcoming chapter.

Exercise 2.1—Downloading Windows Server 2022

This book is structured around a project, and the exercises in this chapter are a continuation of *Chapter 1, Understanding Network and their Components*. To download Windows Server 2022, follow the following steps:

1. Press the *Windows key + R* to open **Run**.

2. Enter **Microsoft-edge:** and press **Enter**.

3. Click on the address bar in *Microsoft Edge*, type **https://www.microsoft.com/en-us/evalcenter/**, and press *Enter*.

4. Click the **Evaluate Now link for the Windows Server 2022** tile before the **Evaluation Center** page.

5. On the **Windows Server 2022** page, click **Download the ISO** link within the **Get Started for Free** section.

6. Complete the **Register for your free trial** form shown in *Figure 2.11* today and click on **Download now**:
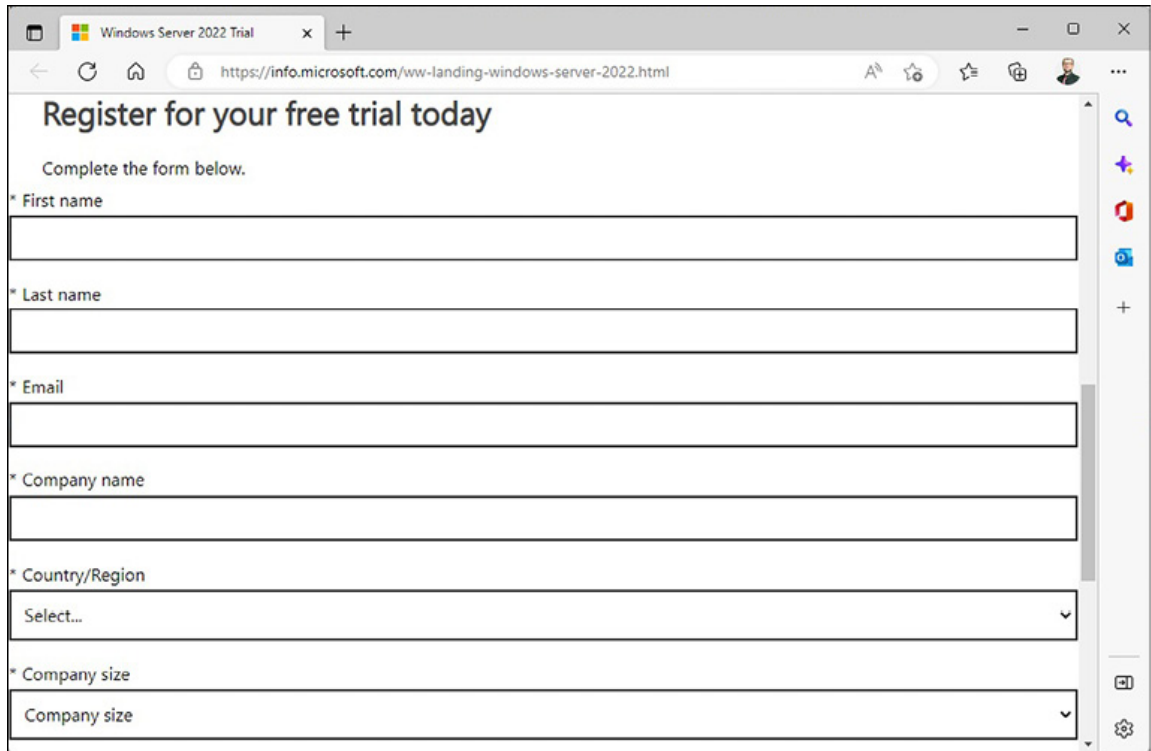
Figure 2.11: *Downloading for a free trial of Windows Server 2022*

7. **Please select your Windows Server 2022 download** page, select the preferred language, and click the link you choose.

8. Shortly after, the Windows Server 2022 download will begin.

Note: After downloading your Windows Server 2022, you must create a bootable USB drive by burning the ISO file. If you do not know how to do this, there are instructions at **https://www.lifewire.com/how-to-burn-an-iso-file-to-a-USB-drive-2619270**.

Exercise 2.2—Downloading Windows Admin Center

To obtain Windows Admin Center, follow the following steps:

1. Open *Microsoft Edge* and navigate to **https://www.microsoft.com/en-us/windows-server/windows-admin-center** page.

2. Click on the **Download Windows Admin Center** button on the **Windows Admin Center** page, as shown in *Figure 2.12*:
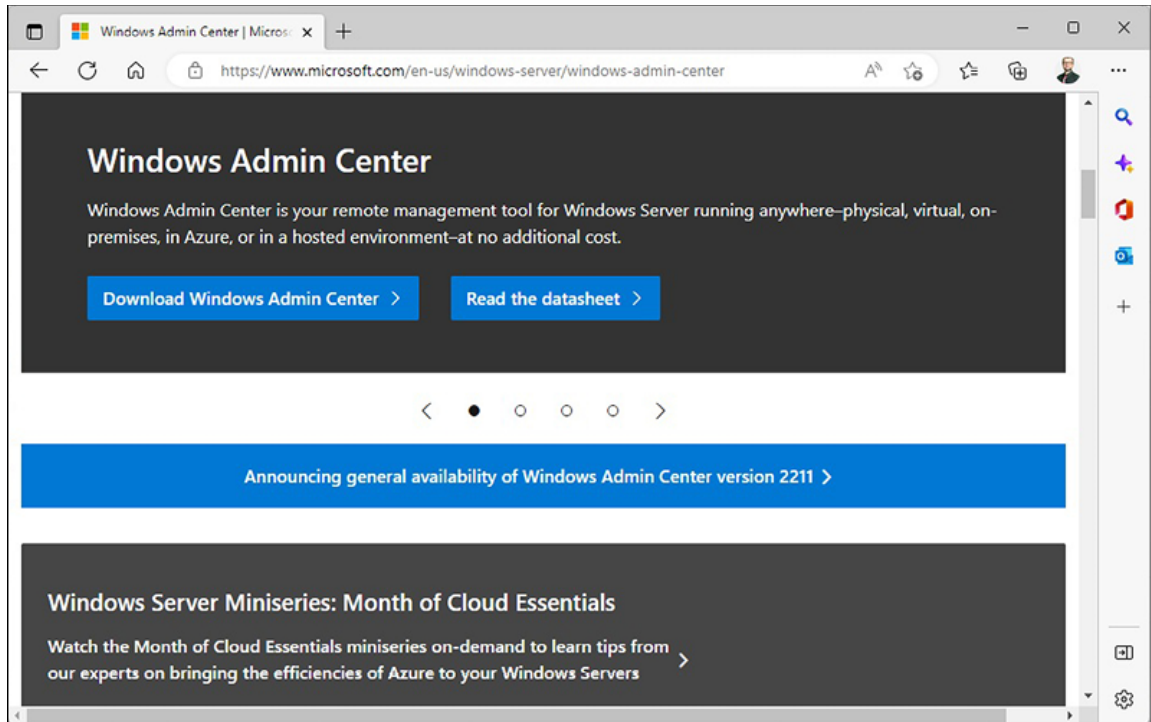
Figure 2.12: *Downloading Windows Admin Center*

3. Shortly after, you will be prompted to save the **Windows Admin Center** file you are about to download.

Questions

1. What are the server's four hardware key components, and what is their function?
2. Can you name each era of the Windows Server and list the corresponding versions?
3. What do you mean by minimum system requirements?
4. List three new features in Windows Server 2022.
5. What do you like most about Windows Server 2022?

Join our book's Discord space

Join the book's Discord Workspace for Latest updates, Offers, Tech happenings around the world, New Release and Sessions with the Authors:

https://discord.bpbonline.com

Windows Server 2022 Installation

Introduction

Until now, you have successfully covered the initial two chapters, which served as an introduction to various network elements, server hardware, and gaining access to Windows Server 2022. Furthermore, you have obtained and installed Windows Server 2022 and Windows Admin Center and configured the Hyper-V Client. At this point, it is crucial to enhance your involvement by familiarizing yourself with partition schemes, boot options, and installation choices while also understanding the detailed instructions for installing Windows Server 2022. This chapter is thoughtfully structured, providing step-by-step instructions and easily understandable visuals that facilitate a smooth installation process and efficient setup of Windows Server 2022. Additionally, it includes valuable tips for expeditious and effective installation. As before, practical exercises are included, but this time in greater quantity, allowing for more hands-on experience.

Structure

In this chapter, we will cover the following topics:

- Getting to know partition schemes
- The boot option

- Getting to know installation methods
- Getting to know installation options

Objectives

As you have been informed, you will learn how to install Windows Server 2022 in this chapter. However, you will be introduced to partition schemes, boot options, and installation options before installing. These concepts will give you a better understanding of how to install Windows Server 2022 smoothly. You will also set up the virtual switch and **Virtual Machine** (**VM**) in Hyper-V Client and use the ISO image you downloaded in *Chapter 2*, *Introduction to Windows Server 2022,* to install Windows Server 2022. These tasks are designed to be engaging and help you quickly learn how to install Windows Server 2022.

Getting to know partition schemes

A disk partition logically divides a disk so an operating system can manage its data. On the other hand, the partition scheme refers to the method used to separate the disk into sections. Typically, two types of partition schemes are primarily used in computers and servers, and they are as follows:

- The **Master Boot Record** (**MBR**) is a traditional partition scheme known as a legacy boot option. It operates on a disk sector of 512 bytes and allows for a maximum of four primary partitions, three primary and one extended partition. The extended partition can have up to 26 logical partitions. MBR uses **Logical Block Addressing** (**LBA**) to support disks up to 2 TB and has been a helpful partition scheme for multiboot platforms.

- On the other hand, the **GUID Partition Table** (**GPT**) is a new partition scheme that overcomes the limitations of MBR. In GPT, the **Global Unique Identifier** (**GUID***) is a 128-bit number used by Microsoft to identify resources. GPT supports block sizes starting from 512 bytes and up, with the most common default being 4,000 or 4,096 bytes,

and the size of each partition entry is 128 bytes. The GPT is part of the **Unified Extensible Firmware Interface** (**UEFI**) standard, which replaces the older **Basic Input/Output System** (**BIOS**) and supports modern hardware. The GPT is fault-tolerant and can handle up to 18 EB of disk storage and 128 partitions per disk.

The boot option

The boot option represents a configuration setting that determines the method or source used to initiate the operating system on a computer. It specifies the device from which the computer should begin the boot process, including options such as the hard drive, DVD, USB, or network connection. Modifying the boot option allows you to start the computer from a different source, install a new operating system, or troubleshoot issues with the current operating system. Typically, these options are managed through the computer's BIOS (Basic Input/Output System). The specific key(s) required to access the BIOS may vary depending on the manufacturer, but commonly used keys include Delete, F1, F2, F10, and F12. Once you have entered the BIOS, you will find various available boot options. Presently, some of the commonly utilized boot options include:

- **Installation media:** Using a bootable DVD in many scenarios is common for the installation media. First, insert the DVD into the DVD drive before entering the BIOS. Once inside the BIOS, set the DVD as the primary boot option, save the modifications, and exit the BIOS.

- **USB flash drive:** When utilizing a USB flash drive, ensure it has a minimum capacity of 8 GB. Before accessing the BIOS, connect the bootable USB drive to the computer. Within the BIOS settings, designate the USB drive as the first boot option, save the changes, and exit the BIOS.

- **Network boot:** In the case of network booting, this method is employed when installing Windows Server 2022 via a network connection. First, enable network booting within the BIOS settings. Then, specify network booting as the

primary boot option. Lastly, save the adjustments and exit the BIOS.

Note: The Windows USB/DVD download tool and Rufus can create a bootable USB flash drive. You can obtain the Windows USB/DVD download tool from **https://www.microsoft.com/en-GB/download/details.aspx?id=56485**, and Rufus can be obtained from **https://rufus.ie/en/**.

Advanced Startup Options

In Windows Server 2022, the traditional F8 option to access advanced startup options is no longer available. Instead, you can utilize the Advanced startup options to recover the server operating system. To access these options, follow the steps outlined below:

1. Click on the Start button at the screen's bottom left corner.
2. From the Start menu, select Settings.
3. In the Windows Settings as shown in *Figure 3.1* window, choose Update & Security.
4. On the left side of the screen, navigate to the Recovery section.
5. Click on the Restart Now button (refer to *Figure 3.1*) **and then click on Continue.**
6. By following these steps, you can access the Advanced startup options in Windows Server 2022, allowing you to perform recovery or troubleshooting tasks as needed.
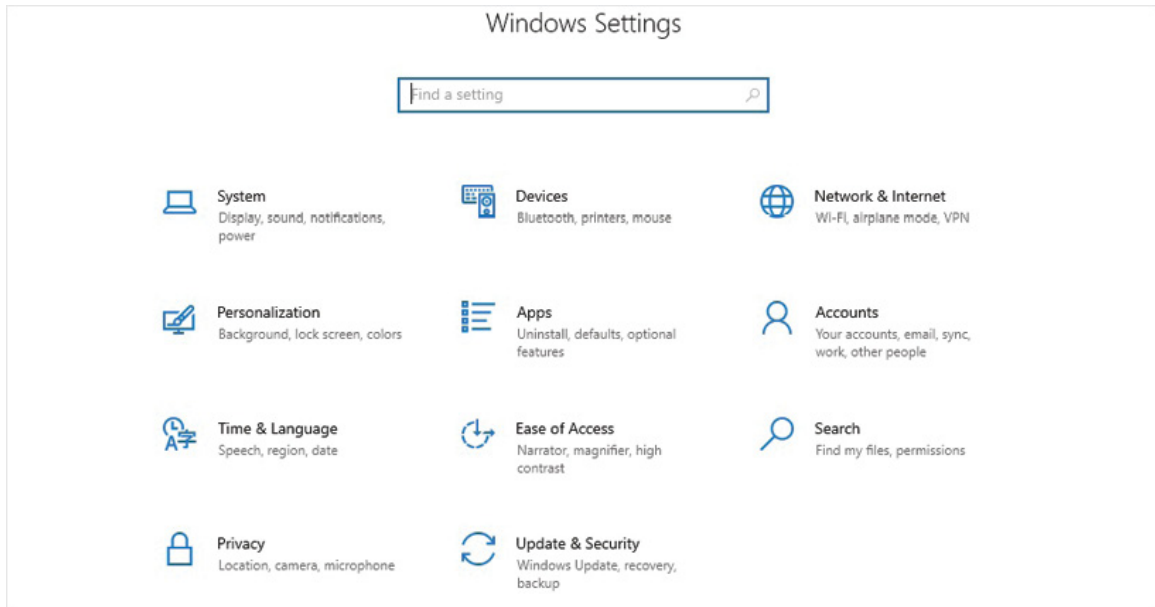
Figure 3.1: *Accessing the Update and Security within Windows Settings*

7. After a brief moment, you will see various options, including Continue, Troubleshoot, and Turn off your PC.

8. To access the advanced options, click on Troubleshoot. That will take you to the Advanced options screen, where you can choose from various available options, as depicted in *Figure 3.2*. You can select the advanced option from this screen that aligns with your requirements or troubleshooting needs.
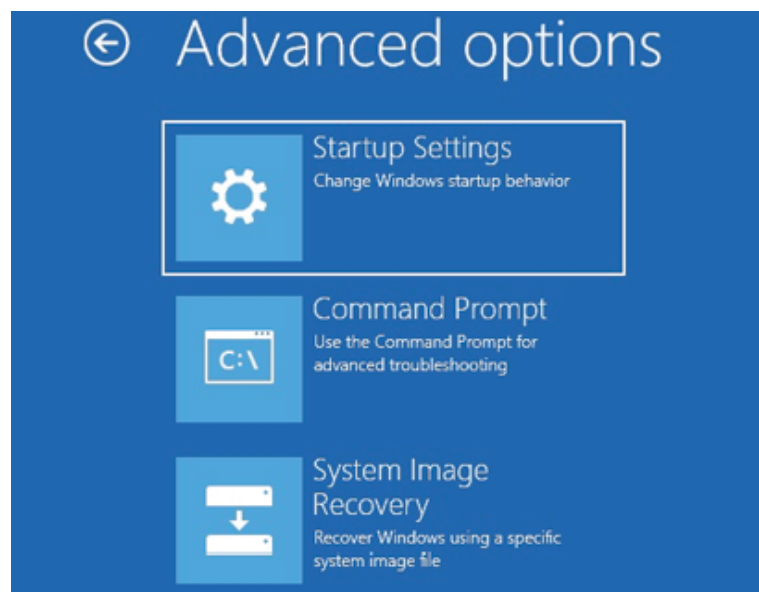
Getting to know installation methods

There are various methods for installing Windows Server 2022. Your chosen method depends on the environment in which you will deploy Windows Server 2022. The available methods include the following:

- **Clean installation:** Involves overwriting the existing operating system on a hard disk with the new one. That requires user interaction, although it may be less than the upgrade option.

- **Upgrade:** Replace the current operating system with a new one while retaining your files and settings. This type of installation is often called an *in-place upgrade*, as it takes place on the same machine. Before proceeding with the upgrade, it is recommended to back up your files and settings. An in-place upgrade can be performed if the server runs Windows Server 2019, 2016, or 2012 R2. However, Microsoft does not recommend upgrading directly from Windows Server 2012 R2. In this case, upgrading to Windows Server 2016 and then to Windows Server 2022 is necessary. Windows Server 2016 and 2019 can be upgraded to Windows Server 2022 in a single step.

- **Migration:** This is the process of moving roles, features, applications, settings, and network services from an old server to a new one. To do this, first, the operating system must be installed on the new server. Then, before migrating, ensure that Windows Server 2022 supports the existing apps. The **Windows Server Migration Tool** (**WSMT**) can assist in the migration process, or the appropriate cmdlets can be run to migrate the necessary services.

- **Network installation (using WDS or MDT)**: Organizations deploying multiple servers can benefit from using **Windows Deployment Services** (**WDS**) or **Microsoft Deployment Toolkit** (**MDT**). Setting up WDS

involves installing the WDS role on the server and adding the install and boot images. On the other hand, MDT requires downloading and installing the tool on a server to automate desktop and server deployments. An unattended network installation is an automated installation that involves minimal user interaction and can be performed using WDS or MDT. This type of installation is facilitated by an answer file and an XML file containing installation prompts. You can create an answer file using Notepad or download sample answer files from the Internet.

These various installation methods provide flexibility and cater to different deployment scenarios when installing Windows Server 2022.

Getting to know installation options

In the previous section, you learned about different installation methods for Windows Server 2022. This section will focus on the various installation options available. Understanding the difference between the installation methods and installation options is essential for successfully installing Windows Server 2022 or any operating system. Windows Server 2022 offers three installation options, and the chosen option will impact the availability of roles and features. So, it is essential to consider the following options before deciding:

- **Desktop experience:** The first installation option is Desktop Experience, which includes all the features of Windows Server 2022. However, your hardware must fully meet the minimum system requirements to utilize the **Graphical User Interface** (**GUI**) fully.

- **Server core:** The second option is Server Core, which Microsoft recommends. It utilizes fewer hardware resources and enhances security. Roles and features can be installed on the local server using Windows PowerShell or remotely through Server Manager.

- **Nano server:** The third option is Nano Server, an alternative to Server Core. It offers greater efficiency in

terms of updates and reboots, and it has a smaller server image size, allowing more disk space for other purposes. Nano Server prioritizes enhanced security and improved performance. However, it has limitations: it only supports 64-bit applications and cannot function as a standalone server. Instead, it must operate within another host as a container. Nano Server lacks local login access and can only be managed remotely. It is often regarded as a "set and forget" installation option.

Conclusion

In this chapter, you have been introduced to installing Windows Server 2022. Before installing, you are provided information about partition schemes, boot options, and installation methods. The different installation methods discussed include a clean install, an in-place upgrade, migration, and installation via WDS or MDT. These methods will help you install Windows Server 2022 on new or old servers, upgrade from previous versions of Windows Server, migrate services to Windows Server 2022, and deploy it in an enterprise network in an automated manner. In addition, you learned about the installation options of Desktop Experience, Server Core, and Nano Server. This chapter also included hands-on exercises, such as setting up virtual switches and VMs in Hyper-V Client and performing a Windows Server 2022 installation. All that is presented in this chapter is helping you prepare for the upcoming chapter of learning about and carrying out post-installation tasks in Windows Server 2022.

Exercise 3.1—Setting up virtual switches in Hyper-V client

A switch is an essential component in computer networking at the layer 2 level. It connects computers and other devices within a **Local Area Network** (**LAN**), whether in a home or workplace environment. Additionally, switches can be employed to expand networks and accommodate more devices. These switches possess multiple physical ports, known as switch ports, where network cables are inserted to establish connections and

construct the network infrastructure. Switches utilize a star physical topology and a logical bus topology to facilitate forwarding frames between computers.

There are two main categories of switch types: unmanaged and managed. Unmanaged switches function independently without configuration options, while managed switches offer more control and administration capabilities.

Furthermore, in virtual networks, similar to how physical networks require switches to connect computers, virtual networks necessitate virtual switches to link **virtual machines** (**VMs**). Hyper-V, a virtualization platform, provides three types of virtual switches:

- The first type is the *external switch*, which connects to a physical network adapter. That enables VMs to access and communicate with the external physical network, allowing them to connect to other devices and resources within the network.

- The second type is the *internal switch*, which operates exclusively within the confines of the physical server. It facilitates communication between the VMs and the physical server itself. However, it does not provide direct access to the external physical network or other devices outside the server.

- The third type is the *private switch,* which is isolated and accessible only to the VMs residing within the physical server. It creates a private network environment exclusively for communication between the VMs within the server without external network connectivity.

By utilizing these different types of virtual switches, administrators can establish the desired level of connectivity and isolation for their virtualized environments, enabling effective communication and network management for the VMs.

To create a virtual switch on the Hyper-V client, you can follow the provided steps below:

1. The **external switch** links the physical network adapter, enabling the VMs to access the physical network.
2. The **internal switch** can only be used within the physical server and between the VMs and the physical server.
3. The **private switch** is only accessible to the VMs within the physical server.

To establish a virtual switch on the Hyper-V client, follow the following steps:

1. Click the **Start** button in Windows 11 to open the **Start** menu.
2. Search for the **Hyper-V Manager** in the **Start** menu and launch it.
3. Once the **Hyper-V Manager** is open, click on **Virtual Switch Manager...** in the **Actions** pane on the right side of the **Hyper-V Manager,** as in *Figure 3.3:*
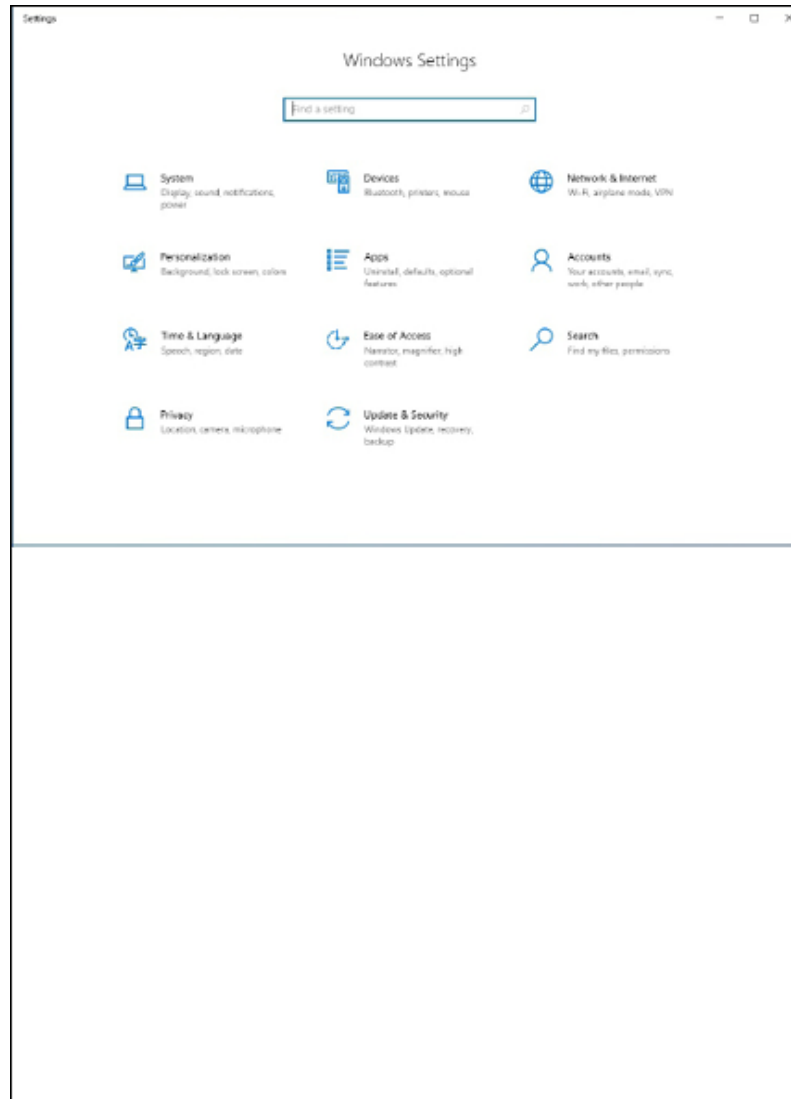
Figure 3.3: *Selecting Virtual Switch Manager… in the Actions pane of Hyper-V Manager*

4. In the **Virtual Switch Manager** window, select **External** Virtual Switch and click **Create Virtual Switch**.

5. Give the virtual switch the name "**Internet**," as in *Figure 3.4*, select the network adapter you want to use, and then choose **Apply**:
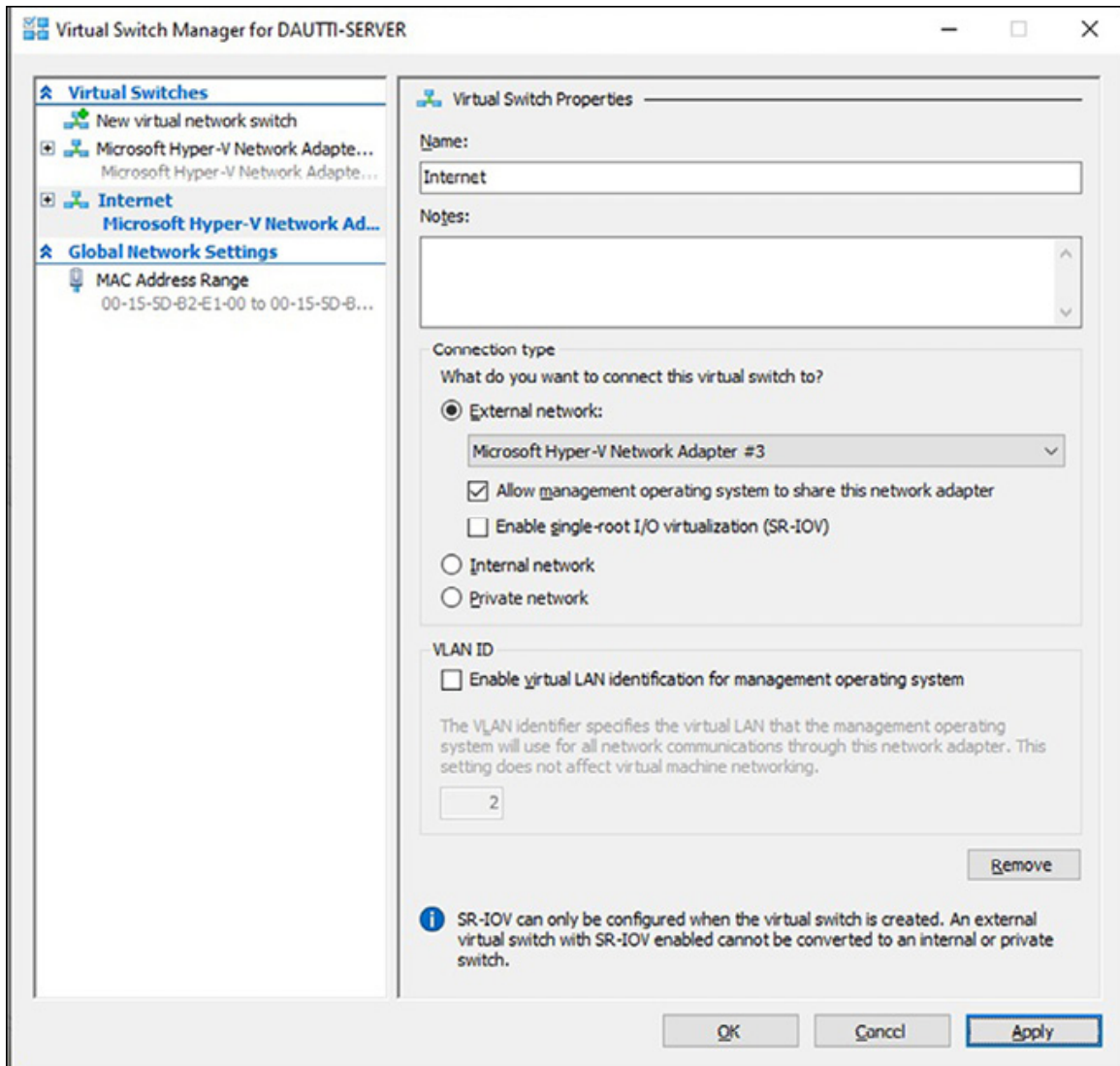
Figure 3.4: *Setting up the external virtual switch in Virtual Switch Manager*

6. Wait for the changes to be implemented, then select the **New virtual network switch** in the **Virtual Switches** pane.

7. Choose **Internal** Virtual Switch and click on **Create Virtual Switch**.

8. Name the virtual switch "**Intranet**," select "**Internal network**" as the connection type, then choose **OK**.

After completing the steps mentioned, you will observe two virtual switches configured in the Hyper-V Manager: "Internet" and "Intranet." The "Internet" virtual switch will facilitate communication between the physical server and the VMs. On the

other hand, the "Intranet" virtual switch will be exclusively utilized for communication among the VMs themselves.

With these virtual switches, you establish distinct communication pathways within the Hyper-V environment. The "Internet" switch enables connectivity between the VMs and the external network, while the "Intranet" switch fosters seamless communication and interaction solely among the virtual machines within the server. By segregating their roles, you can efficiently manage the networking aspects of your virtualized environment and ensure secure and effective data exchange.

Exercise 3.2—Setting up a virtual machine in Hyper-V client

With the essential virtual switches in place, you can now create the VM for installing Windows Server 2022 using the clean installation method. Follow the steps below to configure the VM promptly and efficiently:

1. To launch the **New Virtual Machine Wizard** with **Hyper-V Manager**, click on **New | Virtual Machine** from the **Actions** pane.

2. Take a moment to review the **Before You Begin** page, and then click on **Next**.

3. On the **Specify Name and Location** page, give the VM the name **WinSrv2k22_DC1** and choose a location to store the VM, either the default location or a location of your choice, as shown in *Figure 3.5*. Click on **Next**:
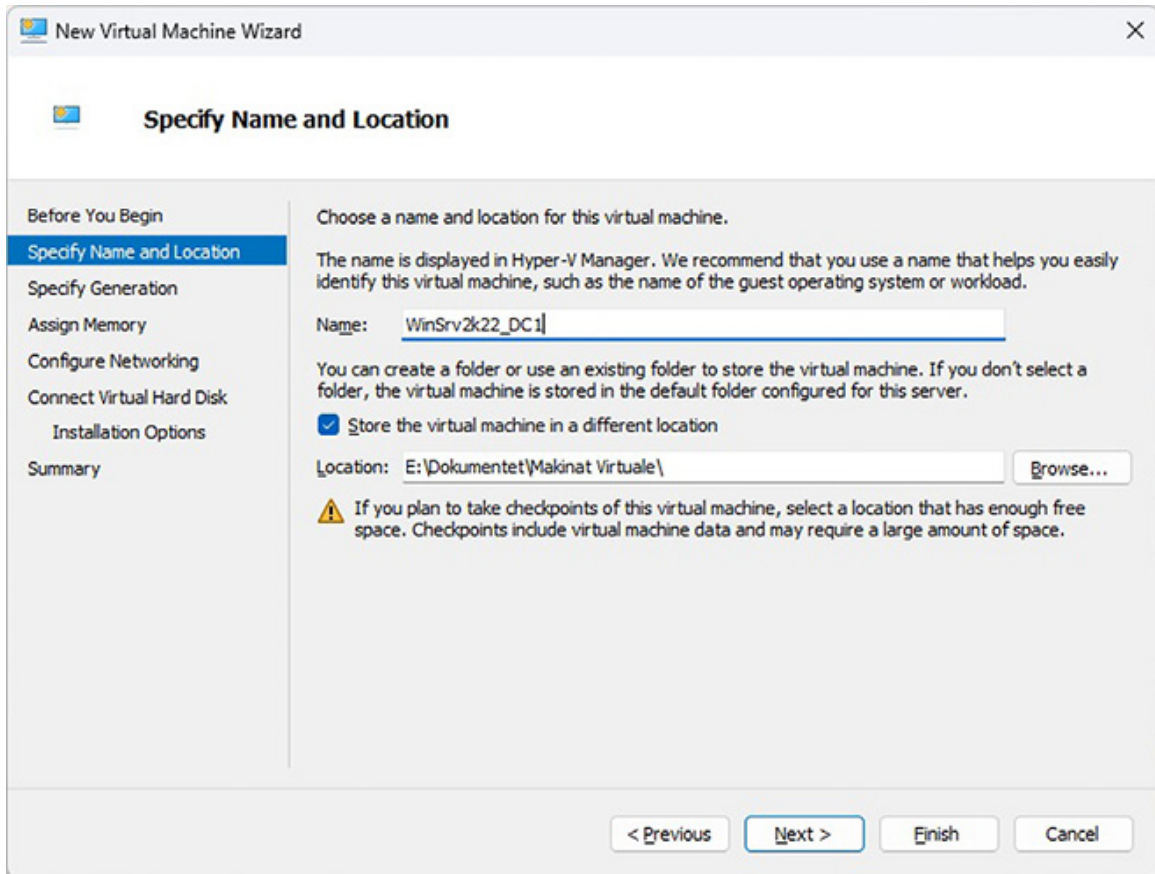
Figure 3.5: Specifying the name and location of the virtual machine

4. On the **Specify Generation** page, ensure the **Generation 1** option is selected (as this is a test environment), then click on **Next**.

5. On the **Assign Memory** page, enter **2048** for the **Startup Memory** value and keep **Use Dynamic Memory** selected. Click on the **Next** button.

6. Choose the **Internet** virtual switch on the **Configure Networking** page and click **Next**.

7. On the **Connect Virtual Hard Disk** page, keep the default name for the virtual hard disk (**.vhdx**) and set the disk size to **35**. Keep the default location and click on **Next** when finished.

8. On the **Installation Options** page, choose to **Install an operating system from a bootable CD/DVD-Rom**, then select the **Image file (.iso)** option. Next, click **Browse** to locate the Windows Server 2022 evaluation .iso file you downloaded in *Chapter 2, Introduction to Windows Server 2022*. Click on **Next** when done.

9. On the **Completing the New Virtual Machine Wizard** page, review the information in the **Description** section, as shown in *Figure 3.6*, to ensure everything is correct, then click on **Finish**:
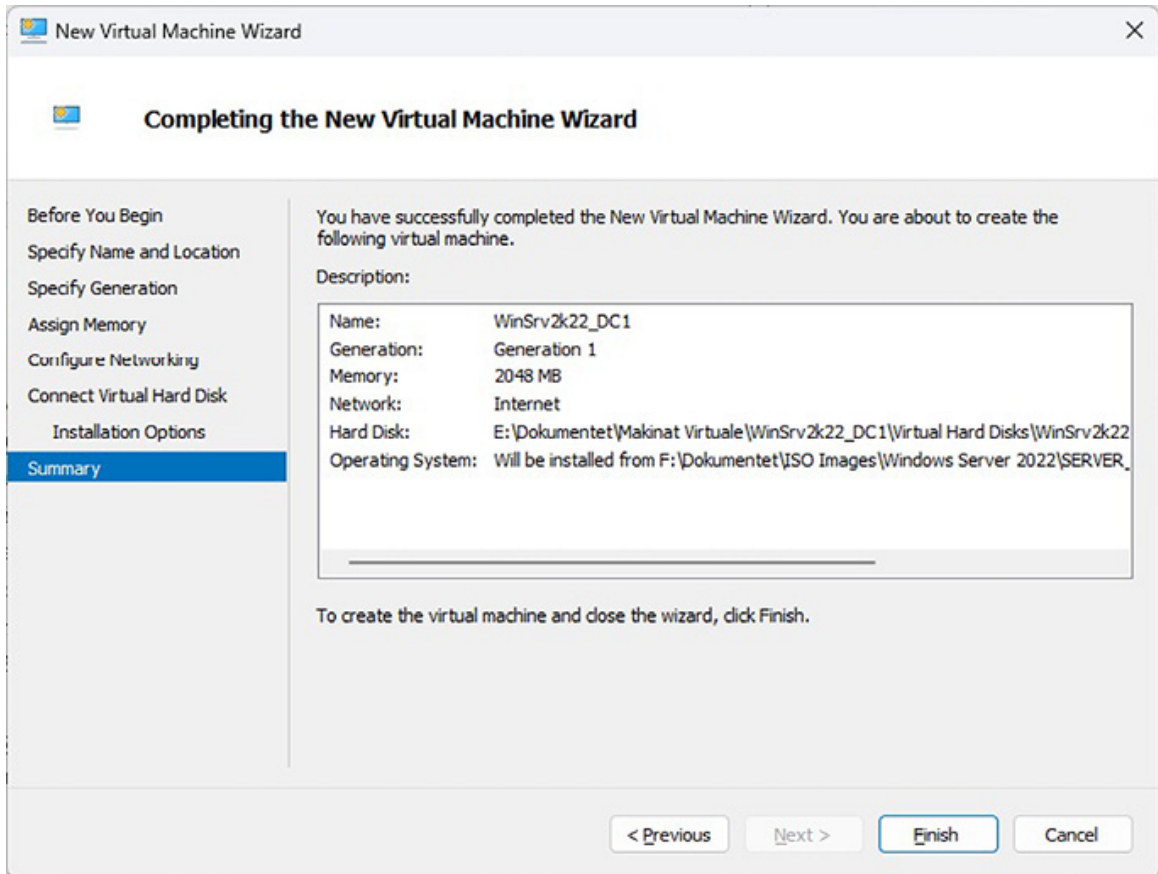
Figure 3.6: Reviewing the entries in completing the New Virtual Machine Wizard page

Before installing Windows Server 2022, a couple of essential tasks must be completed. Firstly, it is necessary to disable the Checkpoint feature, a functionality provided by Hyper-V to create restore points or snapshots of virtual machines. Disabling Checkpoint ensures that any previous snapshots or restore points do not affect the installation process.

A new network adapter must be added to the virtual machine where Windows Server 2022 will be installed. This network adapter will be connected to the Internet virtual switch, which facilitates communication between VMs and is similar to an organization's LAN. By connecting the VM to the Internet virtual

switch it enables the VM to establish network connectivity and communicate with other VMs within the virtual environment.

These steps ensure that the installation of Windows Server 2022 proceeds smoothly, without any interference from previous checkpoints, and allow the VM to connect to the Internet virtual switch for efficient communication with other VMs.

To disable Checkpoints and add a new network adapter to the VM, you can follow the steps provided below:

1. In the **Virtual Machines** pane of the Hyper-V Manager, right-click on **WinSrv2k22_DC1** and select **Settings**.
2. In the **Settings** window for the VM, go to the **Management** section and select **Checkpoints**, as shown in *Figure 3.7:*
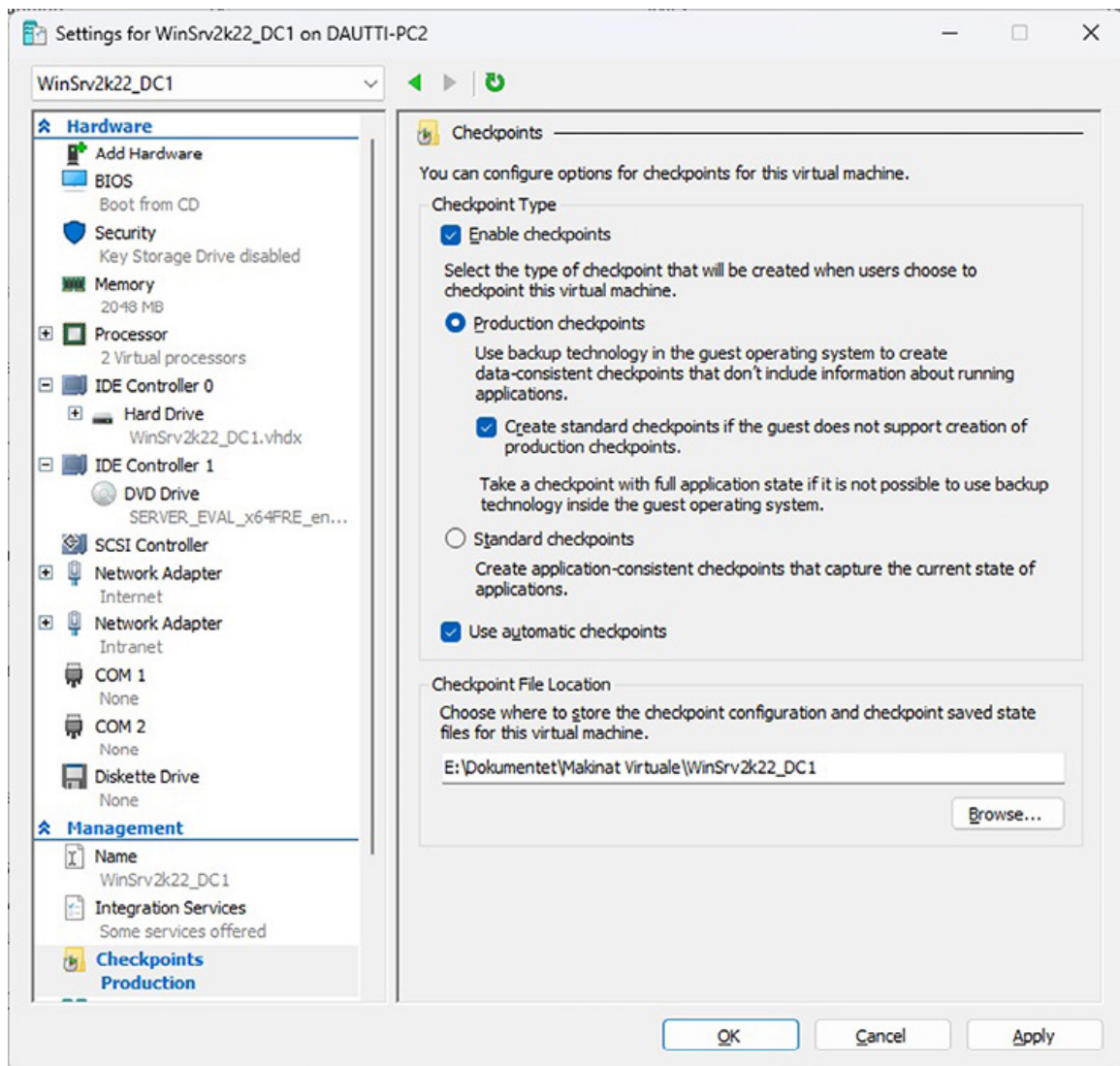
Figure 3.7: *Disabling checkpoints and adding a new network adapter*

3. Within the same **Management** section, uncheck the **Enable checkpoints** box. Then click on the **Apply** button.

4. At the top of the **Settings** window, go to the **Hardware** section and select **Add Hardware**. From the list, choose **Network Adapter**, and then click on the **Add** button.

5. Select **Intranet** as this network adapter's virtual switch and click **OK**.

Exercise 3.3—Performing Windows Server 2022 installation

Once all the necessary steps have been completed, it is time to install Windows Server 2022. To perform a clean installation, please follow the provided steps below:

1. In the **Virtual Machines** pane of the Hyper-V Manager, right-click on `WinSrv2k22_DC1` and select **Start**.

2. Again, right-click on `WinSrv2k22_DC1` and select **Connect**. As depicted in *Figure 3.8*, the setup files are stored in the **Random Access Memory** (**RAM**):

Figure 3.8: Setup files are stored in the RAM

3. Configure your language and other settings and press the **Next** button.

4. Press the **Install Now** button to begin installing Windows Server 2022, as illustrated in *Figure 3.9*:
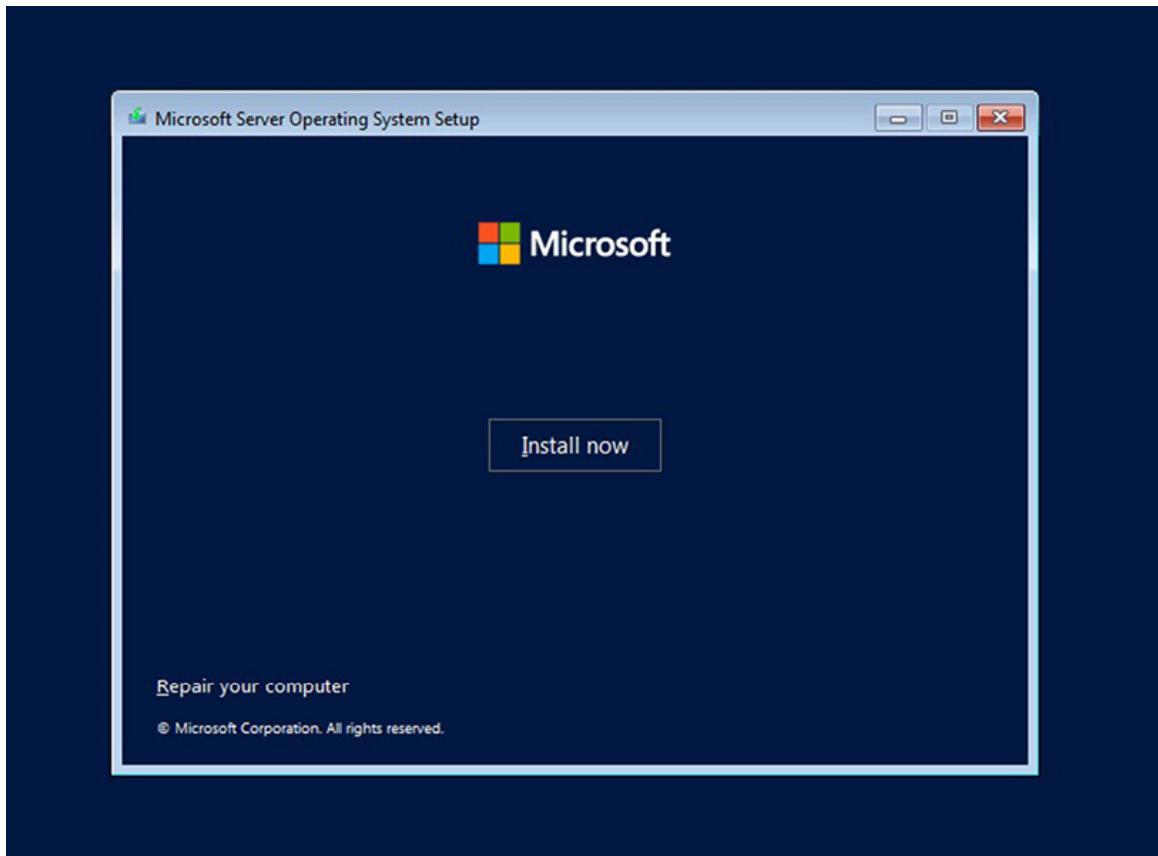
Figure 3.9: *Setting up Windows Server 2022*

5. Choose **Windows Server 2022 Standard Evaluation (Desktop Experience)** as your desired edition of Windows Server 2022 and press the **Next** button.

6. Thoroughly review the license terms. Once you have read them, check the **I accept the license terms** check box and click **Next**.

7. Choose **Custom: Install Windows only (advanced)** to perform a clean installation.

8. On the page labeled **Where do you want to install the operating system?** Click on **Next** to install Windows Server 2022 on a default disk.

9. **Windows Setup** will now install Windows Server 2022, so sit back and wait to complete it.

10. After getting the devices ready and undergoing a few reboots, enter your administrator password and click on **Finish**, as shown in *Figure 3.10*:
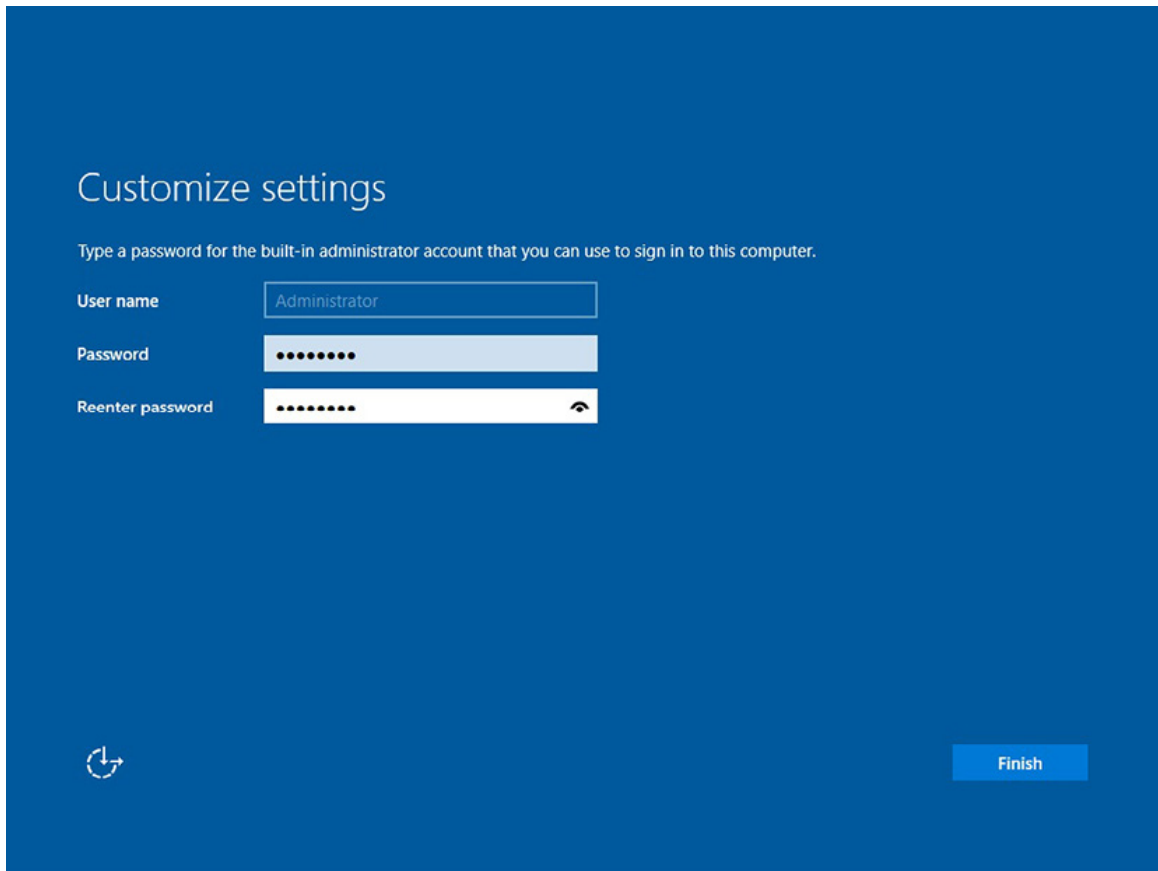
Figure 3.10: Setting up the password in Windows Server 2022

11. Well done! You have successfully installed Windows Server 2022. Enter the **administrator password** to log in to Windows Server 2022 for the first time.

Questions

1. What are the two primary partition schemes typically used in computers and servers?

2. What is the boot option?

3. Can you provide the names of installation methods?

4. What installation options should be considered before installing Windows Server 2022?

5. What is the purpose of a virtual switch in Hyper-V?

CHAPTER 4
Initial Configuration of Windows Server 2022

Introduction

A gentle reminder that this book is structured around the *Installing and Configuring Windows Server 2022* project. So far, this book has introduced you to network components, explained what Windows Server is, and guided you through the installation of Windows Server 2022. After installing the server, the next step is to configure its services. However, before diving into this task, you will need to learn about the initial configuration tasks of Windows Server 2022, such as managing devices and drivers, checking the registry and service status, and configuring the server. Just like the previous chapters, this chapter will provide detailed instructions and practical exercises to help you understand and perform various aspects of the initial configuration of Windows Server 2022. That includes configuring the server name, remote access settings, IP address, time zone, server updates, and more. The goal is to guide you through the process and demonstrate how to do it step-by-step.

Structure

In this chapter, we will cover the following topics:
- Overview of devices and device drivers

- Discussing plug and play, IRQ, DMA, interrupts, and driver signing
- Understanding the registry and services
- Describing registry entries, service accounts, and dependencies
- Initial configuration of Windows Server 2022

Objectives

This chapter aims to provide clear explanations and instructions for post-installation tasks and the initial configuration of Windows Server 2022. The post-installation tasks section will cover devices and drivers, plug and play, IRQ, DMA, interrupts, driver signing, registry and services, registry entries, service accounts, and dependencies. In contrast, the initial configuration will provide step-by-step instructions for hands-on exercises such as setting up the IP address, changing the time zone, activating Windows Server 2022, and many more in an understandable and more apparent format.

Overview of devices and device drivers

Learning about the interaction between computer hardware and software is exciting because computer hardware is more than just physical components, and the operating system is merely a collection of programmed instructions. For the operating system to communicate with the physical components, it needs a "translator" like a device driver. The *device driver* manages and operates the hardware, which can be obtained through installation media or downloaded from the manufacturer's website. However, let us assume that you recently purchased a computer that did not include installation media with a device driver. It is acceptable because modern operating systems such as Windows 10 and 11 support **Plug and Play** (**PnP**). However, when working with a Windows Server 2022, you will likely have to download the device driver from the manufacturer's website.

Because this book is centered on Windows Server 2022, Windows settings is the new administrative console used to manage devices. The legacy applet used to work with device drivers in Device Manager. It is essential to remember, however, that in Device Manager, depending on the status of the device driver, there are additional representations aside from the standard presentation of device drivers. Let us take a look and examine the various statuses of the device driver in Device Manager, as illustrated in *Figure 4.1*:
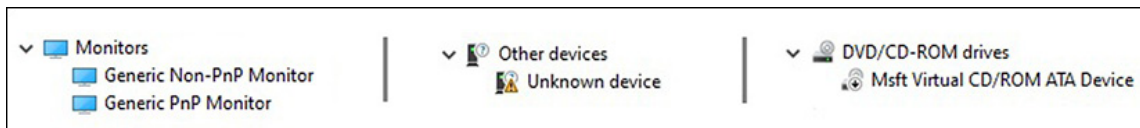
Figure 4.1: *Various statuses of device drivers in Device Manager*

If we refer to the exact figure and analyze the statuses of the device drivers from the left-hand side to the right-hand side, we encounter the following situations:

- If the status of a device driver is **Generic**, it means that an alternative device driver has been installed rather than the appropriate one.

- If there is a **black exclamation mark on a yellow triangle**, it means that either the device driver is missing, or the installed device driver is not suitable.

- If there is a **black downward arrow**, it means that the device is disabled.

Discussing plug and play, IRQ, DMA, interrupts, and driver signing

The computer system comprises hardware and software, with the operating system requiring system resources to manage the hardware, such as the CPU, memory, disk, input/output devices, and network connections. Hence, *system resources* refer to the various hardware and software components used to perform tasks and provide services for a computer system. These resources can be broadly classified into two categories: hardware resources and

software resources. For example, **Interrupt Request** (**IRQ**) and **Direct Memory Access** (**DMA**) are well-known system resources that the operating system must manage to use computer hardware alongside I/O ports and memory addresses. Refer to the following:

- The origins of **Plug and Play** (**PnP**) can be traced back to a collaboration between Intel and Microsoft. This technology has significantly reduced the complexity of working with devices and drivers. With PnP, connecting a device to a computer is a straightforward process; the Windows operating system detects the device as soon as it is plugged in. The device driver is then installed from the Driver Store, which in Windows Server 2022 is located at `C:\Windows\System32\DriverStore`.

- An **Interrupt Request** (**IRQ**), as in *Figure 4.2*, is a signal a device sends via communication channels to the computer's processor, indicating that it needs attention to perform a task. In modern computers, an IRQ is denoted by a numerical value between 0 and 31.

Refer to *Figure 4.2:*
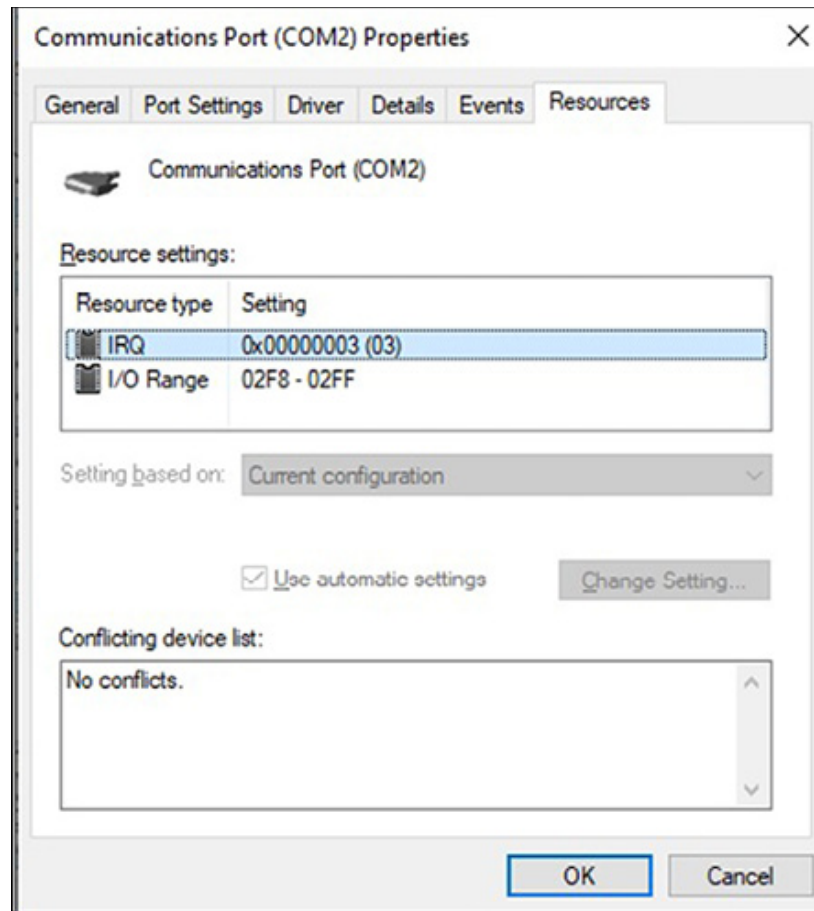
Figure 4.2: *A Communications Port (COM2) IRQ settings*

- **Direct Memory Access** (**DMA**) is a method for transferring data between devices and the computer's memory without the direct involvement of the CPU. DMA is commonly used in devices that quickly transmit large amounts of data, such as disk drives, network adapters, and video cards. DMA is assigned a value between 0 and 8.

- **Driver signing** adds a digital signature to device drivers, as shown in Figure 4.3, to ensure their authenticity and integrity. The digital signature acts as a unique identifier attached to the driver package, verifying that it has stayed the same since it was signed. In addition, the signature is used to confirm that Microsoft has tested and approved the driver package, which reduces the risk of reliability and security issues that may arise during installation.

Refer to *Figure 4.3:*
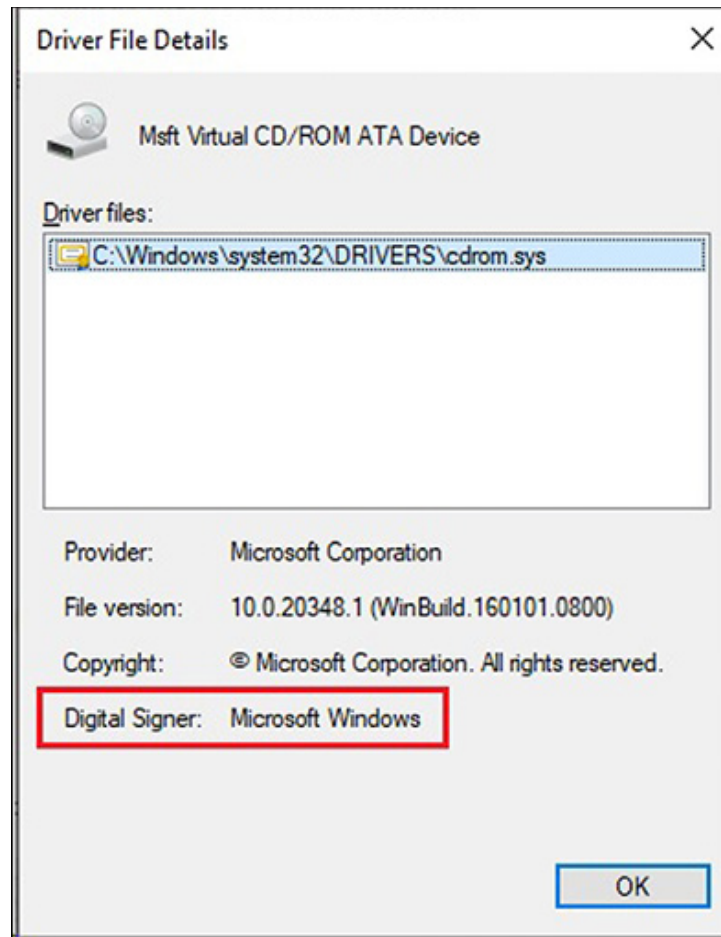
Figure 4.3: *Digitally signed driver*

Understanding the registry and services

The Windows Registry and Windows services are essential components of the Windows operating system. The *Windows Registry* is a hierarchical database that stores the Windows operating system's configuration settings and system information. It is considered an essential component of the Windows OS and contains information about installed hardware, software, and user preferences. The registry is organized into five primary hives or HKEYs, as shown in *Figure 4.4*. These hives are divided into subkeys and values that can be accessed and modified using the Registry Editor tool. The registry plays a crucial role in the operation of Windows, and any changes can affect the operating system's behavior and installed applications. These hives follow the standard Windows file path syntax,

separated by a backslash, and Windows Server 2022 has five of such hives, which are given as follows:

- **HKEY_CLASSES_ROOT**: Stores details about installed applications and their file extensions.

- **HKEY_CURRENT_USER**: Stores information related to the currently logged-in user.

- **HKEY_LOCAL_MACHINE**: Stores information specific to the local computer, including hardware and software configuration settings.

- **HKEY_USERS**: Contains information about the profiles of all currently logged-in users.

- **HKEY_CURRENT_CONFIG**: Stores information collected during the boot process, such as the current hardware profile.

Refer to *Figure 4.4*:
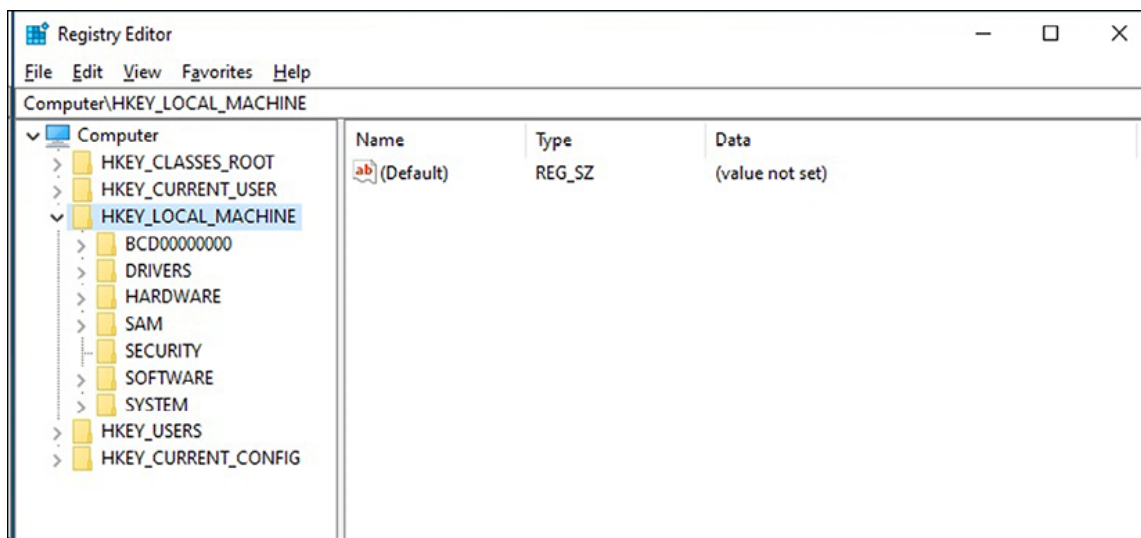
Figure 4.4: Windows Registry in Windows Server 2022

In any computer system, background programs or *services* run in the background to support applications and network services. These services can be controlled using the **Services Control Manager**, allowing you to start, stop, restart, or pause them. If you access services through the Services Control Manager, you will observe that each service has a startup type, which can be

one of several options. For example, there are four different startup types for services, as follows:

- **Automatic:** The service will automatically start when the operating system starts.

- **Automatic (Delayed Start):** The service will begin around two minutes after all other services are marked as automatic.

- **Manual:** The service must be started by a user or other dependent services.

- **Disabled:** The service cannot be started by the operating system, a user, or dependent services.

Refer to *Figure 4.5:*
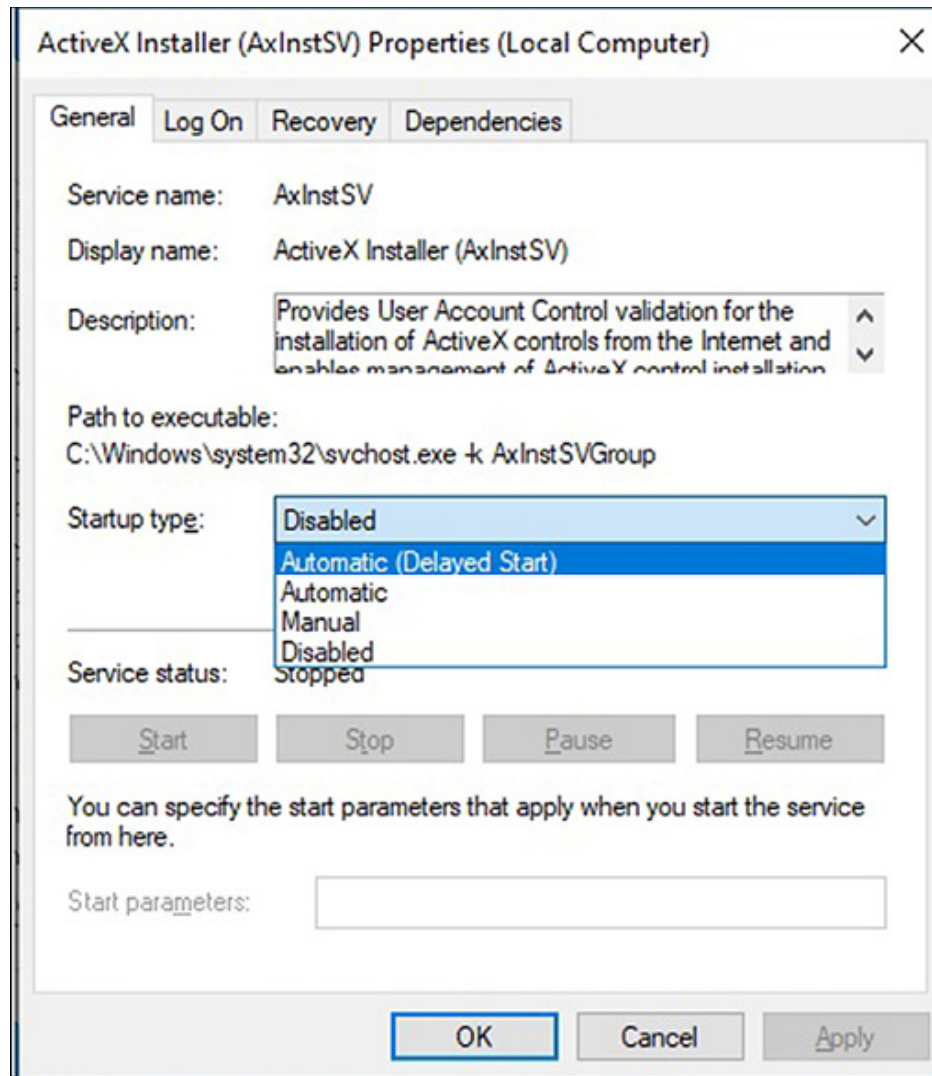
Figure 4.5: *Windows Service startup types*

Describing registry entries, service accounts, and dependencies

You may need to create a new registry key or value when making changes or adding new features to a Windows Server. A registry entry can represent a particular setting or configuration value for a component or application installed on the system. For example, the information stored in a registry entry can include file paths, program settings, user preferences, and system configurations. Registry entries are organized into a hierarchical structure, with each entry organized into a key containing one or more subkeys and values. As shown in Figure 4.6, Windows Registry entries can

be added, modified, or deleted using the Registry Editor tool or through programmatic interfaces provided by the Windows API. However, it is essential to be cautious when working with the Windows Registry entries, regardless of your operation.

Refer to *Figure 4.6:*
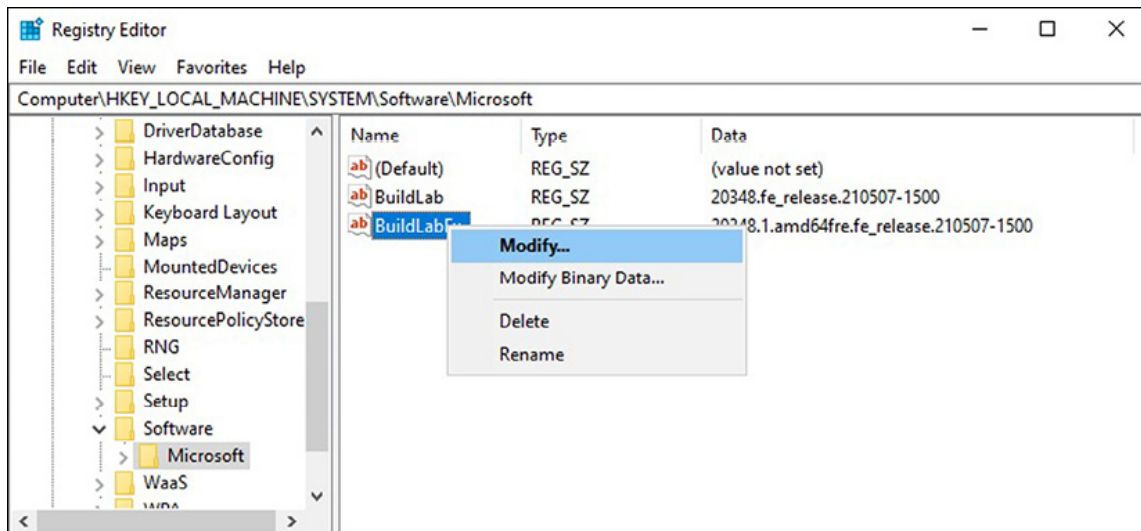
Figure 4.6: *Various actions can be performed on entries within the Windows Registry*

In addition, Windows services use a service account, either a native Windows Server account or an account created by the user to manage running services. The *service account* enables the service to access resources on the local and network level, providing security and authentication for the service. Each service can use a different service account, and you can choose from various types of service accounts, such as built-in system accounts or user-created accounts with specific permissions. In Windows Server 2022, there are several native accounts available for services to run, as follows:

- The **local system** is a built-in account in a Windows operating system with the highest privileges and access to system resources. This account is sometimes called a **superuser** account and has more power than any user account, including administrative accounts.

- **NT Authority\LocalService** is another built-in account in a Windows operating system that runs system services and

some applications with limited privileges, the same as those of a regular user account in the "Users" group.

- **NT Authority\NetworkService** is also a built-in account in a Windows operating system that runs system services and some applications with more privileges than the LocalService account but fewer privileges than the Local System account.

Refer to *Figure 4.7:*
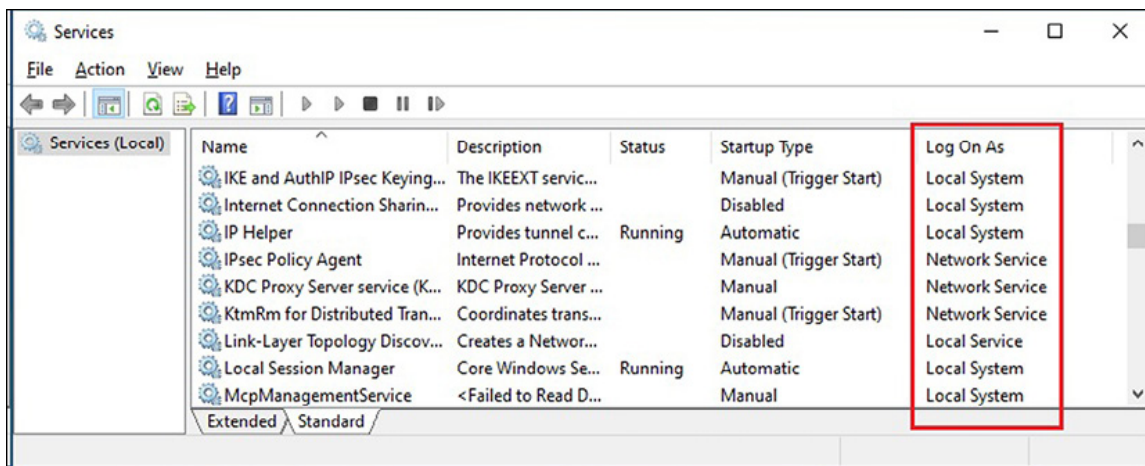
Figure 4.7: *Several built-in systems accounts in Windows Server 2022*

Initial configuration of Windows Server 2022

Performing the server's initial configuration is a crucial task affecting its functional state before it takes on any roles. Therefore, based on my experience, the initial configuration should start with setting up the IP address, changing the time zone, and activating Windows Server 2022. Then, it is necessary to check for updates, change the default server name, join the domain, and enable Remote Desktop. The following steps ensure the server is correctly configured and ready to perform its intended role in the IT infrastructure. In Windows Server 2022, two tools can be used to perform the initial configuration.

- **Server Manager** is a Windows Server tool that provides a centralized interface for managing servers and their roles and features. It allows administrators to perform various

management tasks, such as adding or removing server roles and features, configuring settings, and monitoring server performance. Server Manager is included in Windows Server versions starting from Windows Server 2008 and is designed to simplify server management for administrators. For example, when logging into Windows Server 2022, Server Manager, as in *Figure 4.8*, will automatically start and will continue to do so unless the configuration is changed:

Refer to *Figure 4.8:*
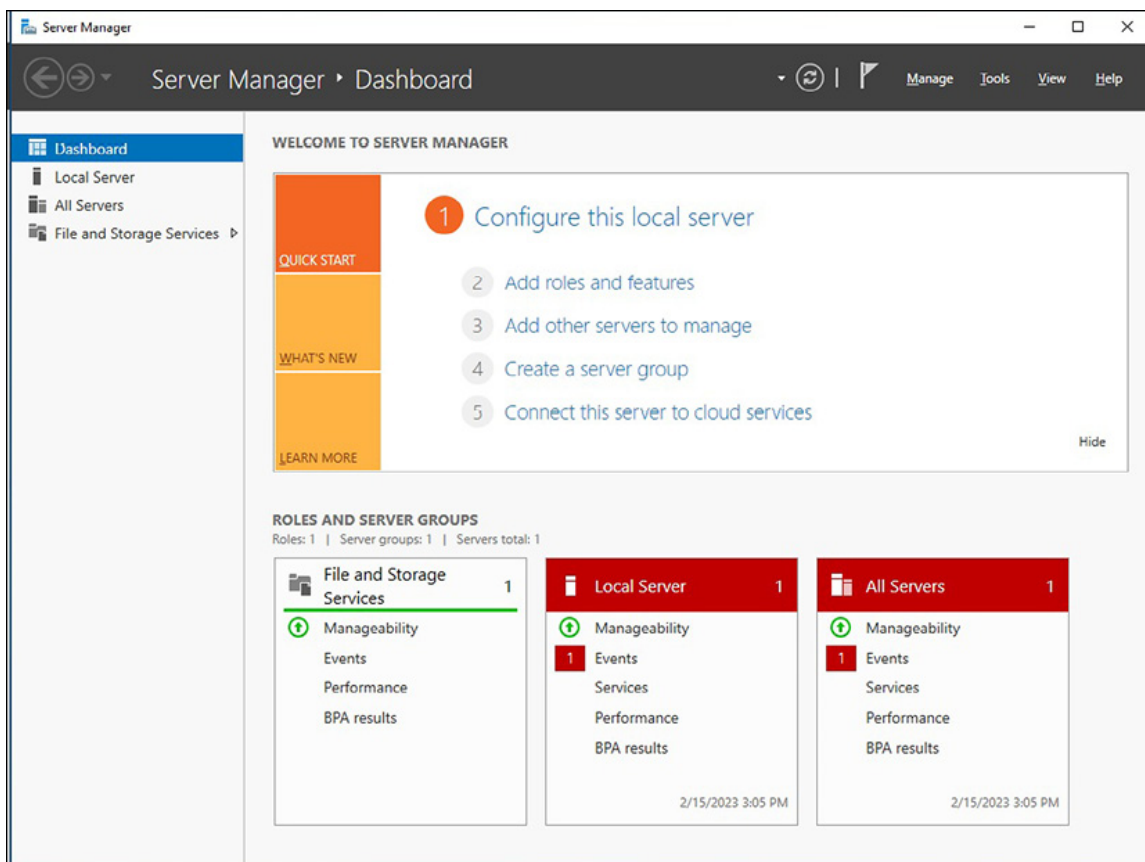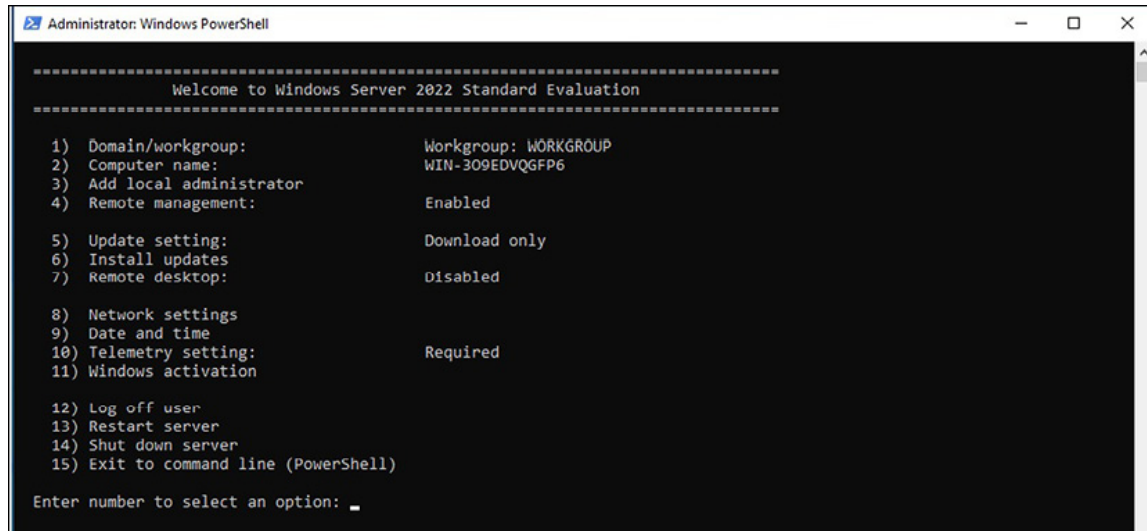
Figure 4.8: Server Manager in Windows Server 2022

- **Server configuration** is a Windows Server **command-line** (**cmd**) tool that can perform basic server configuration tasks on a Server Core installation option. Server configuration provides a simple menu-driven interface that allows administrators to configure various settings, such as

network settings, domain membership, and Windows Update settings. The tool is designed to simplify server configuration on Server Core installations, which do not include a **Graphical User Interface** (**GUI**). As shown in *Figure 4.9*, server configuration is available on all Windows server editions and can be accessed from the Command Prompt by running the `SConfig.cmd` command:

Figure 4.9: *Server configuration in Windows Server 2022*

Exercise 4.1—Device Manager access

To open Device Manager from the administrator's menu, follow the following steps:

1. Right-click on the `Start` button to open the `administrator's menu.`

2. From the `administrator's menu`, choose `Device Manager`.

3. The `Device Manager` window will open soon, as shown in *Figure 4.10*:
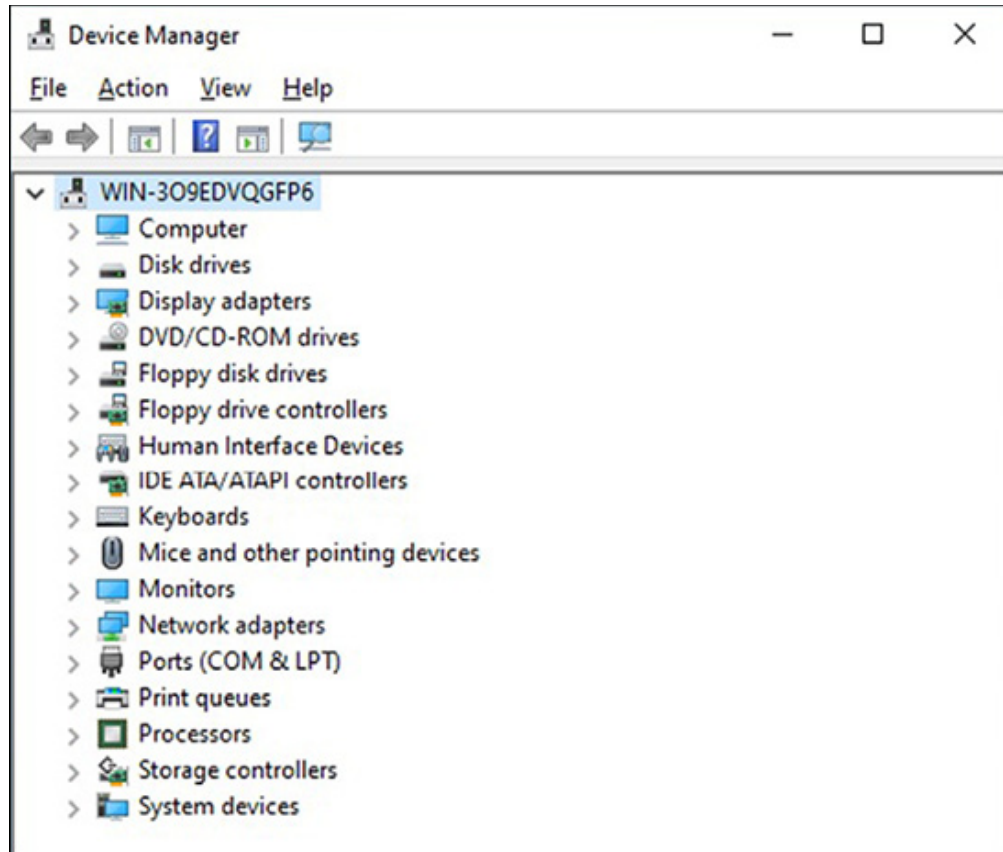
Figure 4.10: *Device Manager in Windows Server 2022*

Note: In addition to right-clicking on the Start button to access the administrator's menu, you can also use the Windows key + X combination. Similarly, you can use the Windows key + I combination to open Windows Settings. For example, open Device Manager or enter devmgmt.msc in the Run dialog box.

If you experience technical difficulties with a device driver, there are several options available to troubleshoot the issue, including the following:

- **Updating the driver:** You can update the driver automatically or browse the server for driver software.

- **Rolling back the driver:** You can roll back the driver to a previous version if the current driver is causing problems.

- **Disabling the driver:** You can disable the driver if it is causing significant issues, such as server instability.

- **Uninstalling the driver:** You can uninstall the current driver if you have found the appropriate driver from the device manufacturer.

Refer to *Figure 4.11*:
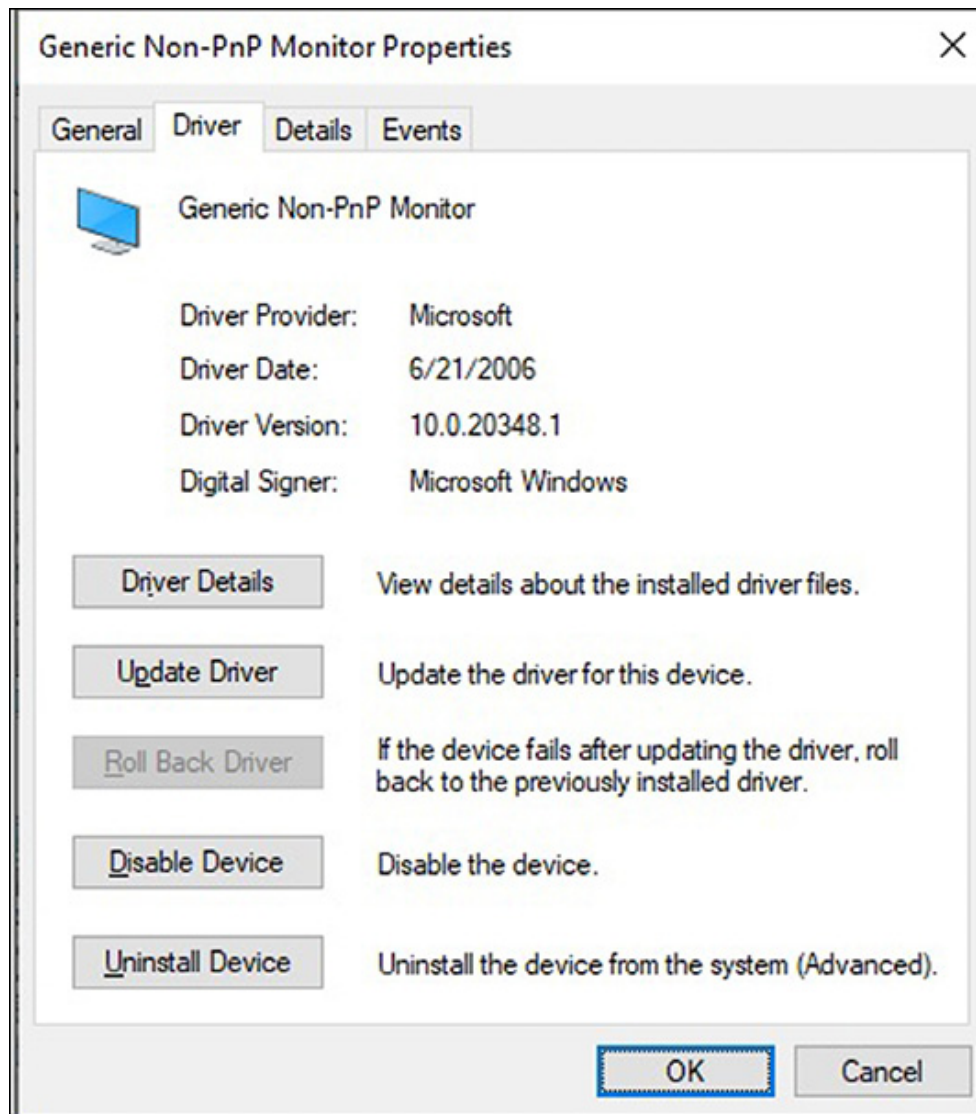
Figure 4.11: *Troubleshooting device drivers using Device Manager*

Exercise 4.2—Performing initial configuration with Server Manager and sconfig.cmd

This activity is designed to teach you how to finish the initial setup of Windows Server 2022 using two approaches: one via Server Manager and the other via Server Configuration. It is important to note that, depending on which tool is being used, you must have accessed it and executed the procedure outlined

in the following instructions. For example, using Server Manager, you need to choose **Local Server** from the panel on the left-hand side.

Changing the server name using the Server Manager

To change the server name, as shown in *Figure 4.12*, follow the following instructions:

1. After opening **Server Manager** and selecting **Local Server**, click the link for the **Computer name** in the **server's properties**.
2. Select the **Change** button in the **System Properties** window.
3. Click on the **Computer name** text box highlighted in the **Computer Name/Domain Change** window.
4. In the **Computer Name/Domain Changes** window, erase the current computer name, type in the *server's new name, and click* **OK**.

   Refer to *Figure 4.12:*

5. Confirm that you want to **restart the server** to activate the changes by clicking **OK**.

6. Choose the **Close** button in the **System Properties** window.

7. Finally, click **Restart Now** in the **Microsoft Windows** dialog box.

Changing the server name using the Server Configuration

To change the server name, as shown in *Figure 4.13*, follow the following instructions:

1. Type "**2**" in the **Server Configuration** menu prompt and hit *Enter*.

2. Input the *new server name* and press *Enter*.

3. Click **Yes** in the **Restart** dialog box to restart the server.

   Refer to *Figure 4.13:*

Figure 4.13: Changing the name of the server using Server Configuration

4. The server will *restart* to implement the changes made to the *server name*.

Joining server to an existing domain using Server Manager

Before adding the server to a domain, it is essential to determine its role. Suppose the server will be a Domain Controller (DC). In that case, there is no need to join a domain, as adding the **Active**

Directory Domain Service (**AD DS**) role will automatically make the server a domain controller. However, if the server has a role other than AD DS, it must join the domain as a domain member, as shown in *Figure 4.14*. To do so, follow the following steps:

1. Click on the link for the **Workgroup** in the server's properties.
2. Click on the **Change** button in the **System Properties** window.
3. Select the "**domain:**" option in the **Computer Name/Domain Changes** window, enter your organization's domain in the textbox, and click **OK**.

    Refer to *Figure 4.14*:
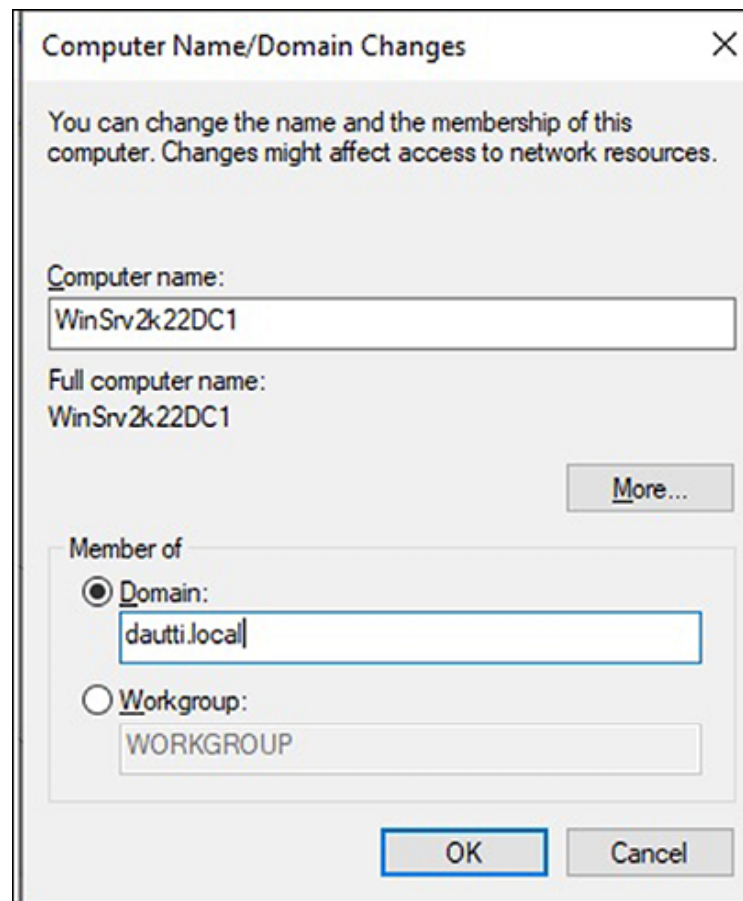
Figure 4.14: *Joining a domain using Server Manager*

4. In the **Windows Security** window, provide the name and password of an account with permission to join the domain, then click **OK**.
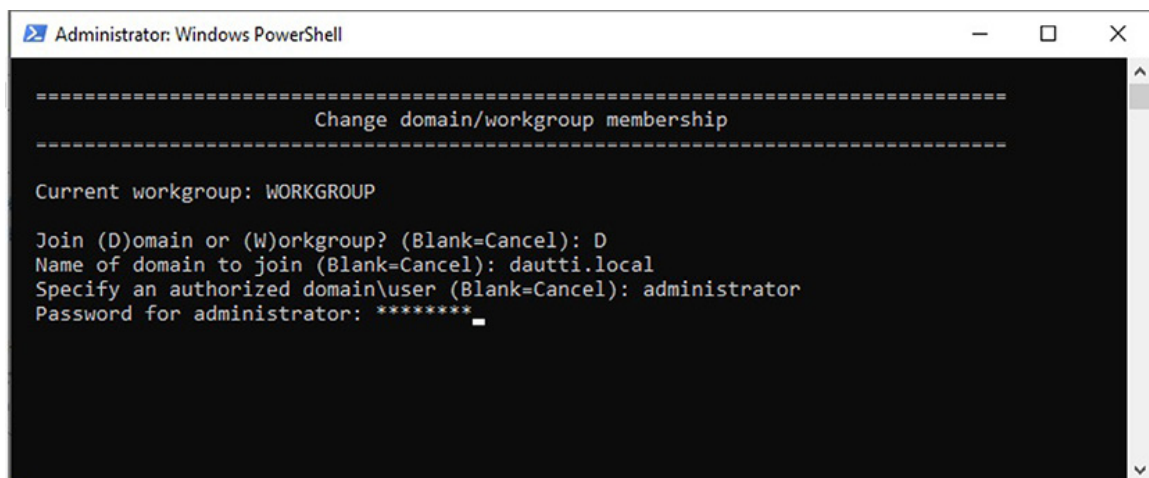
5. The **Computer Name/Domain Changes** dialog box will welcome the server to the organization's domain. Click on **OK** to close it.

6. Click **OK** to confirm that the server must be *restarted* to apply these changes.

7. Click on the **Close** button in the **System Properties** window.

8. Click on **Restart Now** in the **Microsoft Windows** dialog box.

Joining server to an existing domain using Server configuration

To join a server to a domain, follow the following steps as shown in *Figure 4.15*:

1. On the **Server Configuration** menu, select option "**1**" and press *Enter*.

2. Enter "**D**" to join the organization's domain and press *Enter*.

3. Type the *organization's domain* and press *Enter*.

4. Enter the *username* authorized to join the domain and press *Enter*.

5. Type the *password* for the authorized user and press *Enter*.

   Refer to *Figure 4.15:*

Figure 4.15: Joining a domain using server configuration

6. When asked to change the server's name in the **Change Computer Name** dialog box, select "**No**."

Enabling remote desktop using Server Manager

To enable a remote desktop, as shown in *Figure 4.16*, follow the following steps:

1. Click on the link for the **Remote Desktop** in the *server's properties*.

2. Click on the **Remote** tab in the **System Properties** dialog box.

3. Choose the "**Allow remote connections to this computer**" option in the **System Properties** window.

4. The **Remote Desktop Connection** dialog box will notify you that the **Remote Desktop firewall exception** will be activated. Press **OK** to close it.

   Refer to *Figure 4.16:*
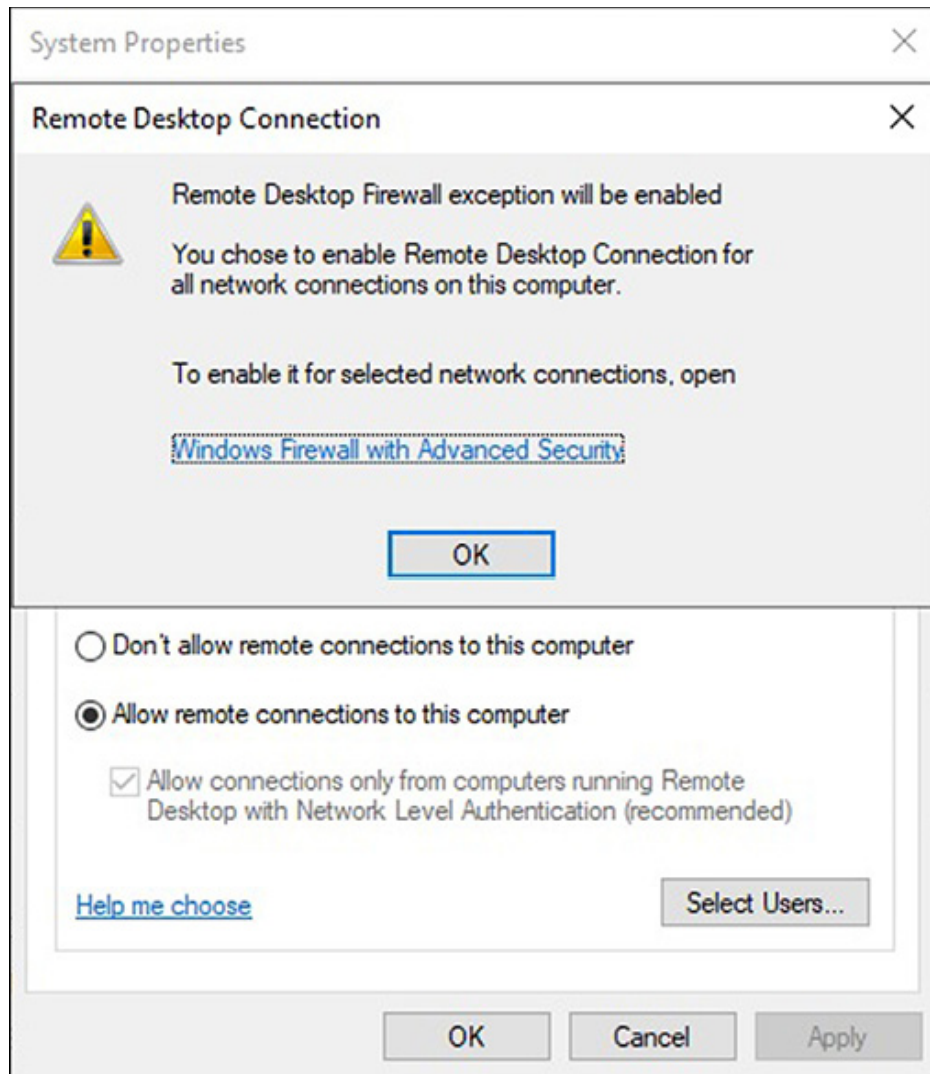
Figure 4.16: Enabling Remote Desktop using Server Manager
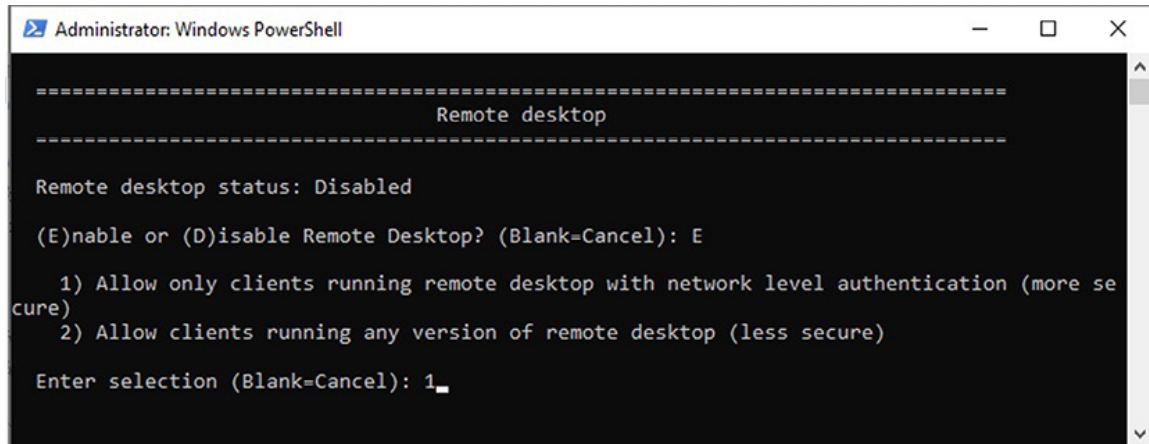
5. Click the "**Select Users...**" button to add **Remote Desktop** users.

6. In the **Remote Desktop Users** window, select **users or groups** from your *AD DS* and click on the **Add button** to add them. Once you have finished adding **Remote Desktop users**, press **OK** to close the **Remote Desktop Users** window.

7. Finally, click on **OK** to close the **System Properties** window.

Enabling remote desktop using Server configuration

To enable a remote desktop, follow the following steps as shown in *Figure 4.17*:

1. Access the **Server Configuration** menu prompt and choose option 7 by typing "**7**" and pressing *Enter*.
2. Activate Remote Desktop by typing "**E**" and pressing *Enter*.
3. Choose a more secure access option by typing "**1**" and pressing *Enter*.

   Refer to *Figure 4.17:*

Figure 4.17: Enabling remote desktop using server configuration

4. Click OK to verify that the remote desktop is enabled on the **Remote Desktop** dialog box.

Setting up the IP address using Server Manager

To configure the IP address as shown in *Figure 4.18*, follow the following steps:

1. Click on the link for the **Ethernet** in the **server's properties**.
2. Right-click on the **Ethernet** setting of the server in the **Network Connections** window, then choose **Properties**.
3. Select "**Internet Protocol Version 4 (TCP/IPv4)**" in the **Ethernet Properties** window and click the **Properties** button.
4. In the "**Internet Protocol Version 4 (TCP/IPv4) Properties**" window, choose the "**Use the following IP address**" option and fill in the IP address, Subnet Mask, and Default Gateway fields. Also, select the "**Use the following DNS server addresses**" choice and supply the **Preferred and Alternate DNS** server fields. Finally, click on **OK** to save the changes.

Refer to *Figure 4.18:*
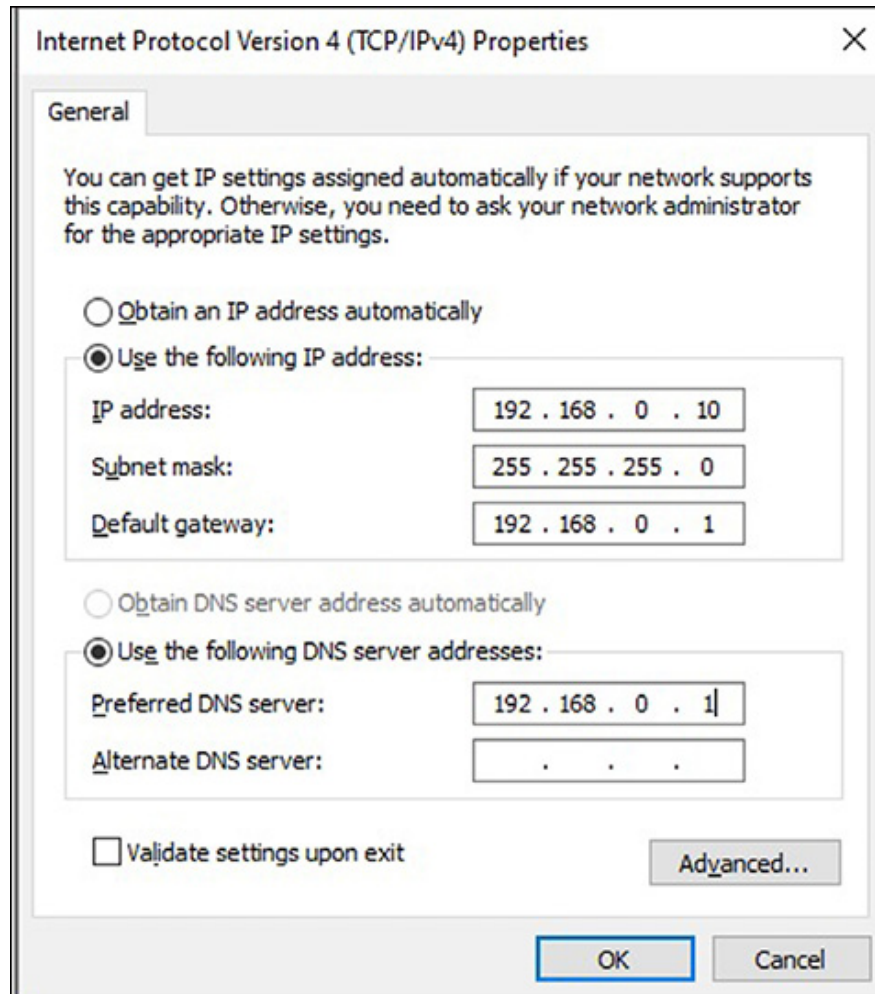
Figure 4.18: *Setting up the IP address using Server Manager*

5. Click on the **Close** button to exit the **Ethernet Properties** window.

6. Finally, click the **Close** button (the red X) in the upper-right corner to close the **Network Connections** window.

Setting up the IP address using Server configuration

To configure the IP address for a network adapter, as shown in *Figure 4.19*, perform the following steps:

1. Access the **Server Configuration** menu and select option "**8**".

2. Specify the **network adapter number** you want to configure the IP address and hit *Enter*.

3. Enter **1** in the submenu to set the *network adapter address*, then press *Enter*.

4. Type **s** to select a *static IP address*, then press *Enter*.

5. Enter the *static IP address* and press *Enter*.

6. Enter the *subnet mask* and press *Enter*.

7. Enter the *default gateway* and press *Enter*.

    Refer to *Figure 4.19*:

Figure 4.19: *Setting up the IP address using server configuration*

8. Enter "**2**" in the submenu to set the *DNS servers*, and press *Enter*.

9. Enter the *new preferred DNS server* and press *Enter*.

10. Click **OK** in the **Network Settings** dialog box to close it.

11. Enter the *alternate DNS server* and press *Enter*.

12. Enter "**4**" in the *submenu* to exit and return to the *main menu*.

Checking for updates using Server Manager

To check for updates, follow the following steps as shown in *Figure 4.20*:

1. Click on the link for the **Last checked for updates** in the **server's properties**.

2. The available updates (if any) are listed in the **Settings** window on the right-hand side of the **Windows Update** section. If updates are ready for installation, click the **Install Now** button.

    Refer to *Figure 4.20:*
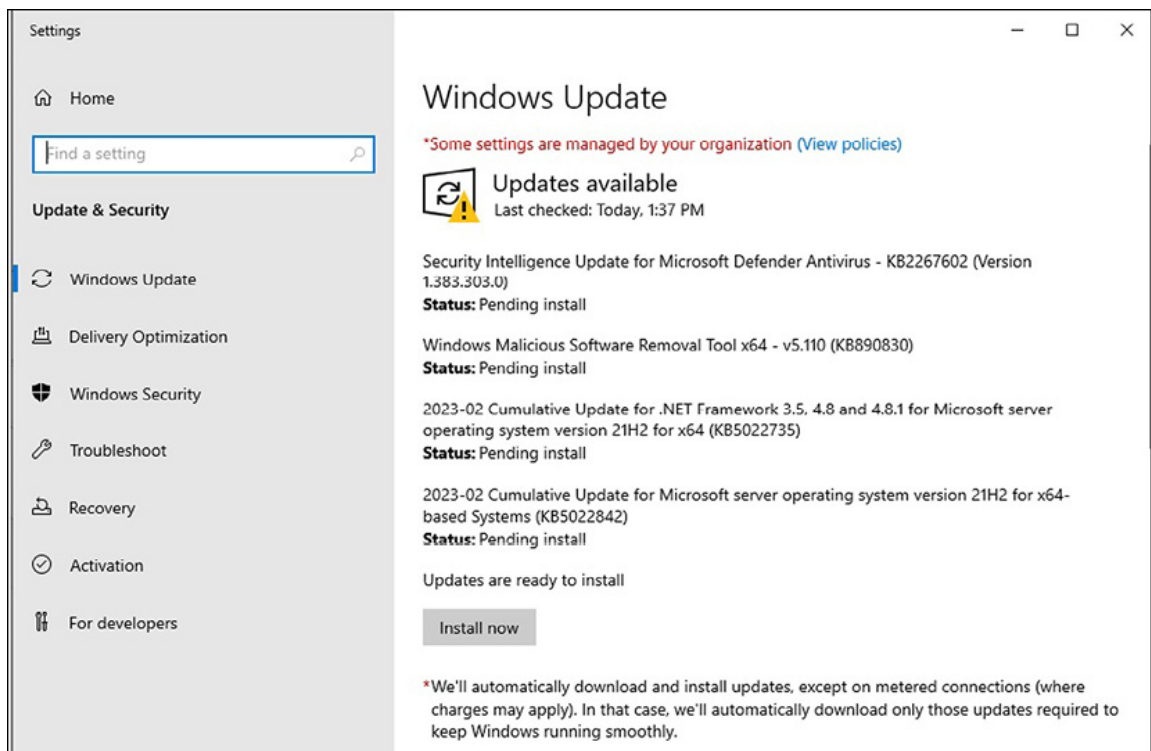
Figure 4.20: *Checking for updates using Server Manager*
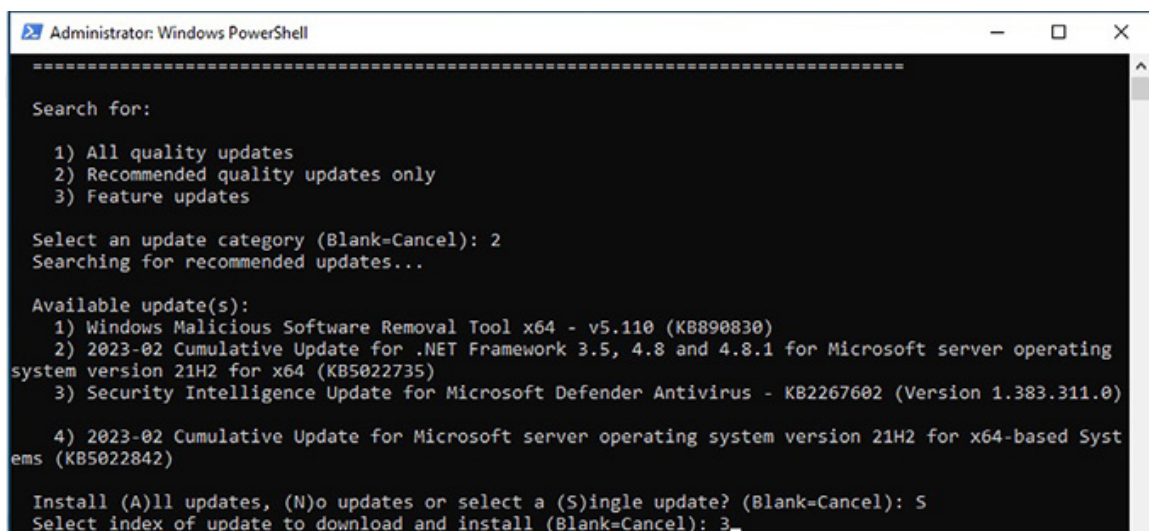
3. Note that installing updates may take some time. In addition, once the installation is **complete**, you may need to *restart the server* for the updates to take effect.

Checking for updates using Server configuration

To check for updates, follow the following steps shown in *Figure 4.21*:

1. Select option "**6**" in the **Server Configuration** menu prompt and press *Enter*.
2. Choose whether to search for *all updates (1)*, only *recommended ones (2)*, or *feature updates (3),* then press *Enter*.
3. Wait while **Windows Update** searches for updates.
4. If updates are found, choose whether to install *all of them (A)*, *none of them (N)*, or a *single one (S)*, then press *Enter*.

   Refer to *Figure 4.21:*

Figure 4.21: Checking for updates using server configuration

5. After the updates are *downloaded*, they will be **installed automatically**. Click on **Yes** to restart the server if prompted.

Changing the time zone using Server Manager

To adjust the time zone, follow the following steps as shown in *Figure 4.22*:

1. Click on the link for the **Time zone** in the *server's properties*.

2. Click the "**Change time zone…**" button in the **Date and Time** window.

3. Select your **Time zone** from the drop-down list in the **Time Zone Settings** window.

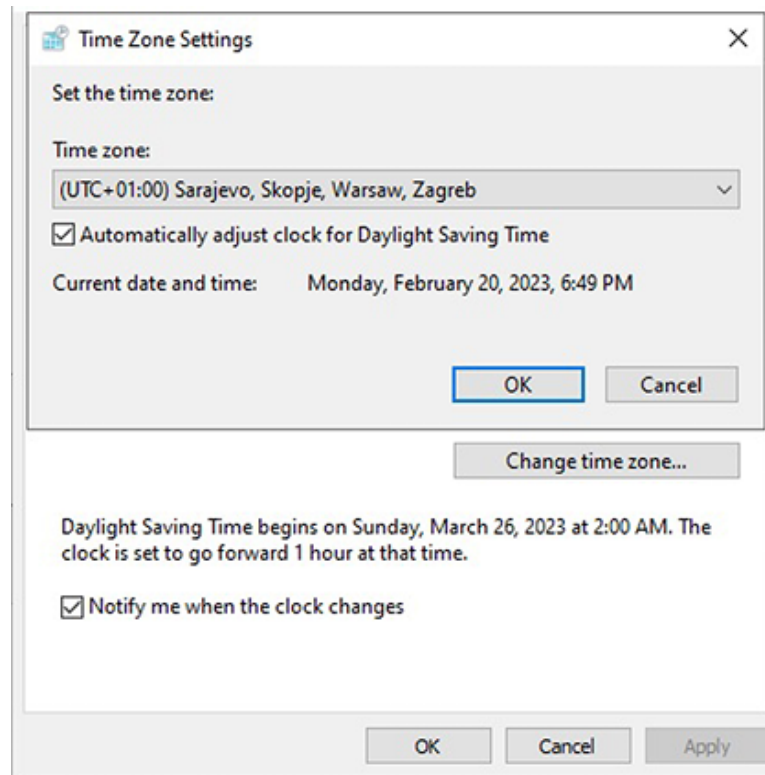   Refer to *Figure 4.22:*

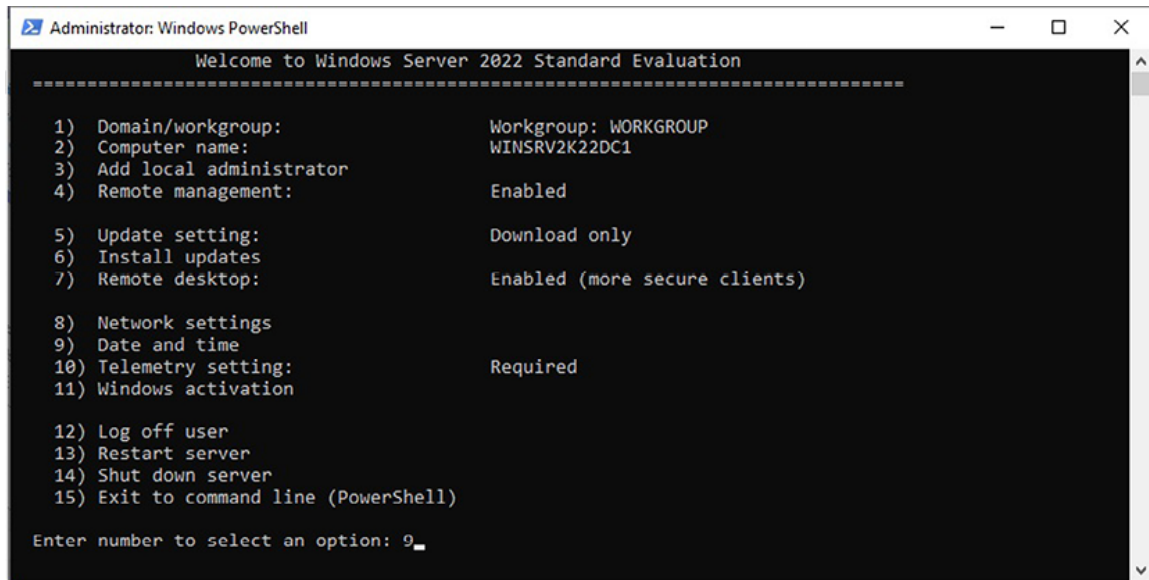*Figure 4.22: Changing Time Zone using server manager*

4. Close the **Time Zone Settings** window by clicking the **OK** button.

5. To complete the process, click **OK** again to close the **Date and Time** window.

Changing the time zone using the Server Configuration

To change the time zone, do the following steps as illustrated in *Figure 4.23*:

1. Input "**9**" as the selected option in the **Server Configuration** menu prompt and then press *Enter*.

   Refer to *Figure 4.23:*

Figure 4.23: *Changing time zone using server configuration*

2. Click the "**Change date and time…**" button in the **Date and Time** window.

3. Choose the **Date or Time** section to adjust the time and date as needed.

4. Click the **OK** button to exit the **Date and Time** window.

5. Click the **OK** button again to confirm and close the **Date and Time** window.

Activating Windows Server using Server Manager

To activate your Windows Server 2022 (Desktop Experience) like the example shown in *Figure 4.24*, try with the following instructions:

1. Click the link for the **Product ID** in the **server's properties**.

2. Enter your *Windows Server 2022* **product key** into the "**Product key**" text box and click on **Next**.
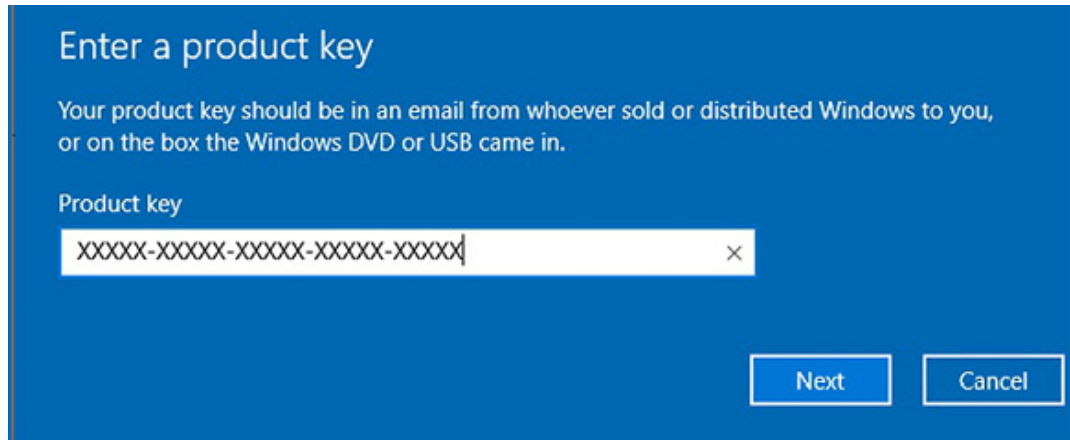
   Refer to *Figure 4.24:*

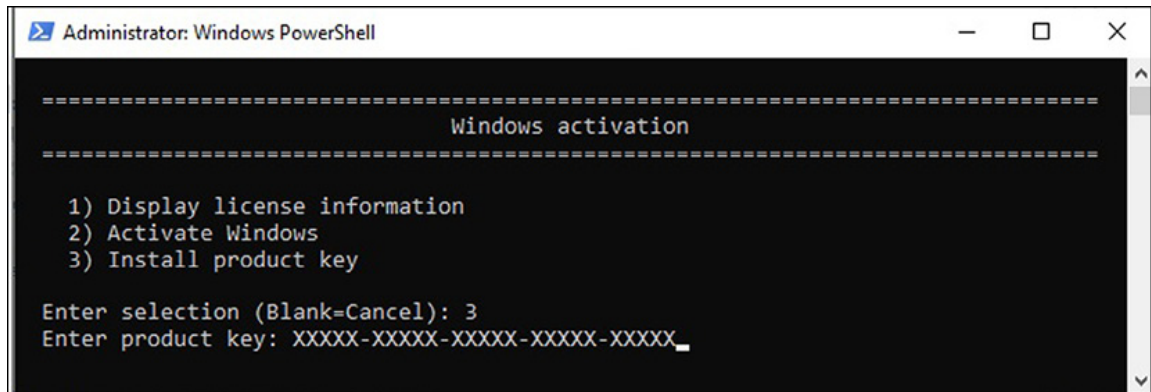**Figure 4.24:** *Activating Windows Server 2022 using Server Manager*

3. *Microsoft's Activation Server* will **verify** the product key you entered. If *confirmed*, click **Next** in the "**Activate Windows**" window.

4. Once activation is complete, click on **Close** to close the "**Thank you for activating**" window.

Activating Windows Server using Server Manager

To activate Windows Server 2022 (Server Core), as in *Figure 4.25*, follow the following steps:

1. Select "**11**" in the **Server Configuration** menu prompt and press *Enter*.

2. Select option "**3**" in the sub-menu to install the product key and press *Enter*.

3. Enter the product key for *Windows Server 2022 (Server Core)* and press *Enter*.

   Refer to *Figure 4.25:*

Figure 4.25: *Activating Windows Server 2022 using Server configuration*

4. Choose an option "**2**" in the sub-menu to activate Windows and press *Enter*.

5. Wait briefly until *Windows Server 2022 (Server Core)* is started, and then close the activation window by entering **Exit**.

Conclusion

In this chapter, you are introduced to different tasks that need to be done after installing Windows Server 2022, which includes managing device drivers, registries, and services. You were also taught about the organization of hardware components in a computer system and the purpose of device drivers. In addition, you learned about system resources, the Windows Server registry, and services. You also became familiar with regedit and performing basic activities on the Windows Registry, such as adding, changing, and deleting keys. Finally, you were introduced to the Windows Server's initial configuration concept and performed post-installation tasks as an exercise. The upcoming chapter will focus on teaching you about Active Directory Domain Services in Windows Server 2022.

Questions

1. What are device drivers?

2. What is Windows Registry?

3. What is Windows service?

4. Why is initial configuration essential for Windows Server?

5. Which tools can you use to run the initial configuration in Windows Server 2022?

Join our book's Discord space

Join the book's Discord Workspace for Latest updates, Offers, Tech happenings around the world, New Release and Sessions with the Authors:

https://discord.bpbonline.com

Installing Roles Using Server Manager and PowerShell

Introduction

Welcome to this chapter on installing roles in Windows Server 2022. This chapter provides step-by-step instructions on installing roles using the Add Roles and Features Wizard available in the Server Manager of Windows Server 2022 and PowerShell. Roles are a set of features that enable the server to perform specific tasks, and by installing these roles, you can tailor your server to meet your organization's requirements. The explanation in this chapter covers what roles are available in Windows Server 2022, how to use the Add Roles and Features Wizard, and what additional features you may need to select for the role to function correctly. In addition, the guidance in this chapter helps you configure the role to meet your organization's specific needs. The exercises given in this chapter include instructions on installing AD DS, DNS, DHCP, Hyper-V, IIS, PDS, Remote Access, RDS, and WSUS, using both Server Manager and PowerShell. You can choose the method that best suits your preferences and expertise by including PowerShell, making the installation process even more accessible and flexible. This chapter aims to provide an easy and efficient way to install roles in Windows Server 2022. Whether you prefer using Server Manager or PowerShell, you can customize your server to meet your organizational needs.

Structure

In this chapter, we will cover the following topics:

- Understanding Role, Role Service, and Feature
- Understanding the active directory domain service role
- Understanding the domain name system role
- Getting to know the dynamic host configuration protocol role
- What is Hyper-V's role?
- What is the use of a Web server role?
- Getting to know the print and document services role
- What is unique about the remote access role?
- The need for a Remote Desktop Services role
- Understanding Windows Server update services role

Objectives

The primary objective of this chapter is to offer comprehensive guidance on installing roles in Windows Server 2022. That can be achieved through step-by-step instructions and clear explanations on using the add Roles and Features Wizard in Server Manager and PowerShell to install various roles such as **Active Directory Domain Service** (**AD DS**), **Domain Name System** (**DNS**), **Dynamic Host Configuration Protocol** (**DHCP**), Hyper-V, **Internet Information Services** (**IIS**), **Print and Document Services** (**PDS**), Remote Access, **Remote Desktop Services** (**RDS**), and **Windows Server Update Services** (**WSUS**). In addition, this chapter aims to help readers understand the purpose of each role and configure them to meet their organization's specific needs. By the end of this chapter, readers will have gained the necessary skills and knowledge to install roles effectively and customize their Windows Server 2022 efficiently, allowing them to tailor it to their organizational requirements.

Understanding Role, Role Service, and Feature

To correctly add a role to a server in an organization's IT infrastructure, it is essential to understand the function of the server. In Windows Server 2022, a server role is the server's primary function, and it should ideally have only one role, although it can perform multiple roles. Therefore, when adding a role to the server, choosing the required hardware is essential based on the function the server needs to perform.

In addition to adding roles, there are times when role services need to be added to augment the functionality of the role. Role services are the components that are added to a role to provide additional functionality. For example, suppose an organization needs an internet print server. In that case, it will add the **Print and Document Services** (**PDS**) role to the server and then add internet printing as a role service to augment the functionality of the role.

Finally, server features are added to support a given function. For instance, the .NET Framework 3.5 feature may need to be installed to help the added role, or the **IP Address Management** (**IPAM**) feature may be required to support the DHCP or DNS roles in the organization's network infrastructure. Adding a WINS server alongside DNS may also be necessary to resolve problems arising from NetBIOS name resolution in routed environments. These are just a few examples of situations where server features may need to be added.

Understanding the Active Directory Domain Services role

Active Directory Domain Services (**AD DS**) is a vital component of the Windows Server operating system introduced by Microsoft back in 2000. Before the release of Windows 2000 Server, the primary mechanism for managing Windows-based networks was the **Primary Domain Controller** (**PDC**) and **Backup Domain Controller** (**BDC**) architecture of Windows NT. However, AD DS was designed to replace this outdated

architecture and provide a more efficient, scalable, and secure way of managing networks.

AD DS is a distributed database that stores objects such as users, computers, peripheral devices, and network services in a hierarchical, structured, and secure format. These objects are uniquely identified by their name and attributes, making them easily searchable and manageable. The network topology of AD DS is divided into domains, forests, and trees, each representing a logical network division.

One of the most significant benefits of AD DS is its ability to provide **Organizational Units** (**OU**) that allow administrators to manage objects more efficiently. **Group policies** (**GP**) can be applied to these OUs, which makes it easier to manage and configure settings across multiple objects. In addition, AD DS supports the delegation of administrative control, which allows administrators to delegate specific administrative tasks to non-administrative users, making it easier to manage the network securely.

AD DS uses several protocols to perform its functions, including the following:

- The **Lightweight Directory Access Protocol** (**LDAP**) is used to access directory services data.
- Kerberos provides a mechanism for authenticating users and servers on the network.
- The **Domain Name System** (**DNS**) translates domain names into IP addresses.

Active Directory consoles

As explained earlier, **Active Directory** (**AD**) is a system that provides centralized management for various services. It simplifies administration tasks by offering a centralized platform for managing different aspects of its services. In **Microsoft Management Console** (**MMC**), several administrative consoles, also known as snap-ins, can manage AD services.

- The Active Directory Administrative Center (dsac.exe), as shown in *Figure 5.1*, is the first administrative console, a graphical user interface for managing Windows Server's directory services. It provides a convenient way to perform administrative tasks related to user management, computer management, **Organizational Units** (**OUs**), and other relevant information:
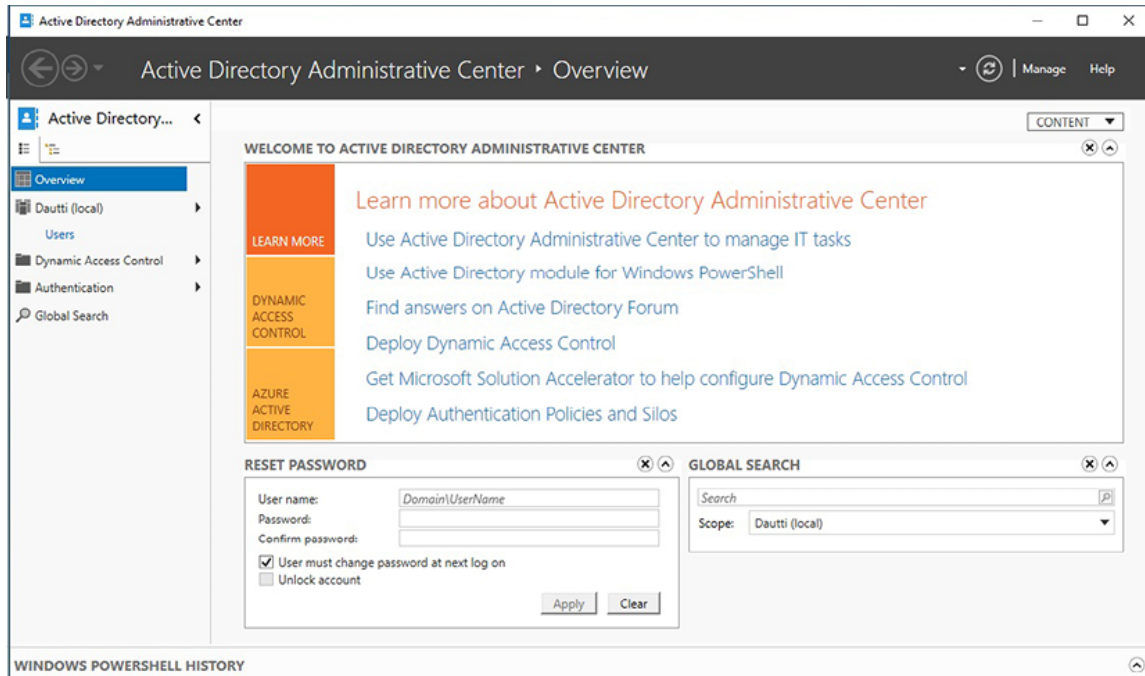

Figure 5.1: *The Active Directory Administrative Center in Windows Server 2022*

- Another administrative console is the Active Directory Users and Computers (dsa.msc), specifically designed to manage users, computers, OUs, and related information. It offers comprehensive tools and options to efficiently handle user accounts, group memberships, computer objects, and other AD-associated operations.

- The Active Directory Domains and Trusts (domain.msc) administrative console manages domains, trusts, and associated information. It allows administrators to configure trust relationships between domains, manage domain properties, and perform tasks related to domain management.

- The Active Directory Sites and Services (dssite.msc) administrative console manages replication and services between different sites in an AD environment. It enables administrators to control the replication of directory data between domain controllers located on various sites, ensuring efficient data synchronization and availability.

- In addition to the graphical consoles, there is the Active Directory Module for Windows PowerShell, which provides a command-line interface for managing Windows Server's directory services. Usually, the Active Directory Module for Windows PowerShell is installed using Add Roles and Feature Wizard, as shown in *Figure 5.2*. It offers a set of cmdlets (commands) that allow administrators to perform various administrative tasks efficiently through scripting or direct command execution:
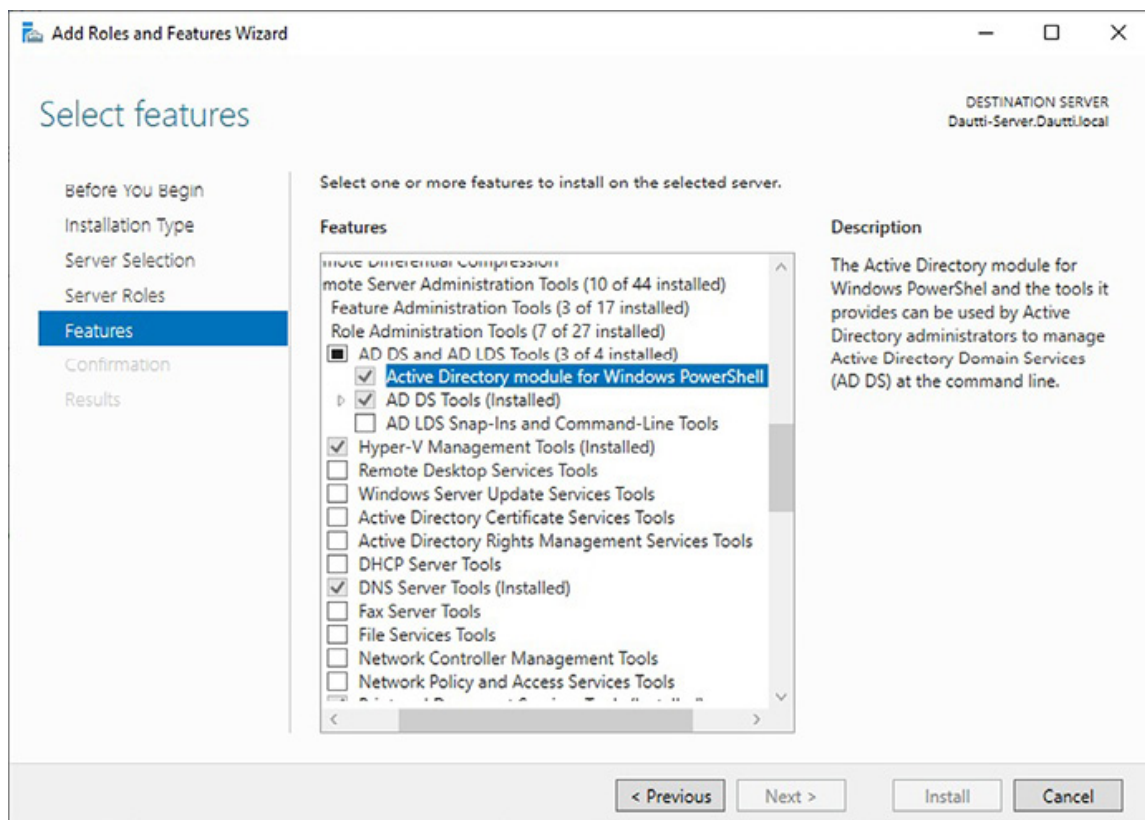

Figure 5.2: Adding Active Directory Module for Windows Powershell in Windows Server 2022

These administrative consoles in the MMC provide administrators with diverse options for managing different aspects of AD services, including user and computer management, domain and trust administration, site and service management, and PowerShell-based administration.

Active Directory structure

Active Directory is a powerful and flexible service that Microsoft provides as the backbone of many enterprise networks. It provides a centralized and secure way to manage and organize resources such as users, computers, and network services. AD uses a hierarchical structure consisting of forests, trees, and domains to efficiently manage and control access to network resources. Understanding this structure is crucial for effectively configuring, securing, and maintaining an AD environment. Within this structure, various components such as Domain Controllers, trust relationships, replication, and schema play essential roles in ensuring seamless authentication, data synchronization, and efficient management of network resources. Let us delve deeper into these components to understand how AD functions and empowers organizations to streamline network operations.

- A **Domain Controller** (**DC**) server securely authenticates users to access an organization's network resources. In the past, there was a primary domain controller and backup domain controllers in Windows NT, where each domain had one PDC and other DCs acted as backups. However, in Windows Server 2022, the concept of primary and backup is no longer used. Instead, DCs are identified by numbers, such as DC1 and DC2, to indicate their order.

- A domain is a logical grouping of users, computers, peripheral devices, and network services. Regarding network architecture, domains are centralized network environments where a DC handles authentication. The AD DS role powers the domain controller and authentication functions in Windows Server-based networks.

- In an AD structure, multiple domains can be organized into a tree domain. Domains in a tree are interconnected

through transitive trust. That means that if Domain A trusts Domain B and Domain B trusts Domain C, then Domain A also trusts Domain C. When a new domain joins an existing tree, it automatically trusts all the existing domains. Configuring a new domain within a tree is done by promoting a server to a domain controller.

- A forest in AD consists of one or more tree domains or a collection of tree domains. The tree domains within a forest share a standard schema and configuration, forming a contiguous namespace. That means the tree domain is considered a domain within the forest, creating a circular relationship.

- To illustrate the concept of a child domain, consider the example where "`bpb.local`" and "`books.local`" are tree domains. However, "`bpb.local`" is the root domain and represents the forest. The domain "`marketing.bpb.local`" is a child domain of the "`bpb.local`" tree domain. Like a tree data structure, the tree and child domain concept establishes the parent-child relationship.

- When the AD DS role is installed, and a server is promoted to a DC, AD DS automatically assigns **Flexible Single Master Operation** (**FSMO**) roles. The first two roles, the master schema and domain naming master, are forest-wide operations. The remaining three roles, **Relative Identifier** (**RID**), PDC emulator, and infrastructure master, are specific to the tree domain. The master schema and domain naming master manage AD's schema, ensuring only one unique domain exists within the forest. The RID assigns **Security Identifiers** (**SIDs**) to DCs, the PDC emulator handles password updates, and the infrastructure master tracks changes to other domain objects.

- Trust relationships exist between computers, DCs, and domains in AD. When a computer joins a domain, its local **Security Account Manager** (**SAM**) trusts the AD's authentication mechanism, Kerberos, on a DC. That means that user authentication occurs through a DC on the network, not locally on the computer's SAM. Similarly, the

authentication mechanism of each tree domain trusts the authentication mechanisms of other trusted tree domains within the forest. For example, the "`bpb.local`" domain authenticates users from the "`user.local`" domain, and this authentication is accepted by the "`books.local`" domain because they are part of the same forest, with "`bpb.local`" as the root domain.

- The **Forest Functional Level** (**FFL**) and **Domain Functional Level** (**DFL**) are critical functional levels in AD. The FFL determines which versions of Windows Server can be used in the **entire forest's Domain Controllers (DCs)**, and it also enables specific capabilities across all domains within the forest. On the other hand, the DFL controls the versions of Windows Server that can be run on the DCs of a specific domain and enables capabilities within that domain only. In the context of Windows Server 2022, it is recommended to lower the DFL and FFL to at least Windows Server 2008 because Windows Server 2003 is no longer supported. That ensures compatibility and takes advantage of the features and improvements offered by newer versions of Windows Server. It is worth noting that the DFL and FFL can be raised to Windows Server 2016 at maximum.

Note: Please note that Windows Server 2022 does not have its functional level. Instead, the highest available functional level is Windows Server 2016.

- Referring to the previous example, the domain "`bpb.local`" represents both a forest and a root domain simultaneously. The "`bpb.local`" and "`books.local`" are tree domains within the forest. Furthermore, the "`bpb.local`" tree domain contains a child domain named "`programming.bpb.local`." The child and tree domains share a common namespace, "`administration.bpb.local`," within the "`bpb.local`" domain. This arrangement is known as a contiguous namespace. To understand namespaces better, one can draw a parallel with **Uniform Resource Locators** (**URLs**), unique Web addresses used to locate websites on a Web server.

- As in computer networks, AD has physical and logical topologies. A domain represents the logical topology, defining the organization and structure of objects within the domain. On the other hand, a site is a computer network's physical location within a specific domain. Sites in AD infrastructure reflect the actual physical topology.

- Replication is a crucial process in an AD infrastructure. It involves synchronizing the standard directory partition across all DCs in a forest. Replication ensures that changes made to the directory data in one DC are propagated to other DCs, maintaining consistency and data availability. Replication topology refers to communication paths where the replication data travels between DCs.

- In AD, objects, classes, and attributes are essential components that define the schema. The class represents the object type, while the attribute represents the characteristics or properties of the object—AD stores objects identified by their classes and attributes. The schema acts as a blueprint or model that establishes rules and structures for the types of objects stored in AD. Replication also ensures that the schema remains synchronized among all DCs in the forest, allowing consistent object definitions and operations throughout the AD environment.

Note: A server that has become part of a domain within an organization's network is called a member server.

Exercise 5.1—Adding AD DS role

This exercise outlines the procedure for adding an AD DS role using Server Manager and PowerShell.

Adding AD DS role using Server Manager

To begin the process of adding an AD DS role in Windows Server 2022 using Server Manager, follow the following steps:

1. Open **Server Manager** from the Start menu and click the **Add Roles and Features** link.

2. Click on the **Next** button on the **Before you begin** page of the Add Roles and Features Wizard.

3. Accept the default settings on the Select *Installation Type* page and click **Next**.

4. Accept the default settings on the Select destination server page and click **Next**.

5. Choose the **Active Directory Domain Services** role from the Select *Server Roles* page list. When the Add Features required for AD DS window appears, click the **Add Features** button. Then, click the **Next** button to continue adding the AD DS role.

6. Accept the default settings on the **Select Features** page and click the **Next** button to proceed.

7. Click the **Next** button on the Active Directory Domain Services page.

8. Review the options on the page and click on the **Install** button.

9. The installation process for confirming installation selections for the AD DS role will begin, as indicated by the progress bar shown in *Figure 5.3*. Once the installation is complete, click on the **Close** button to exit the Add Roles and Features Wizard, which is shown in the following figure:
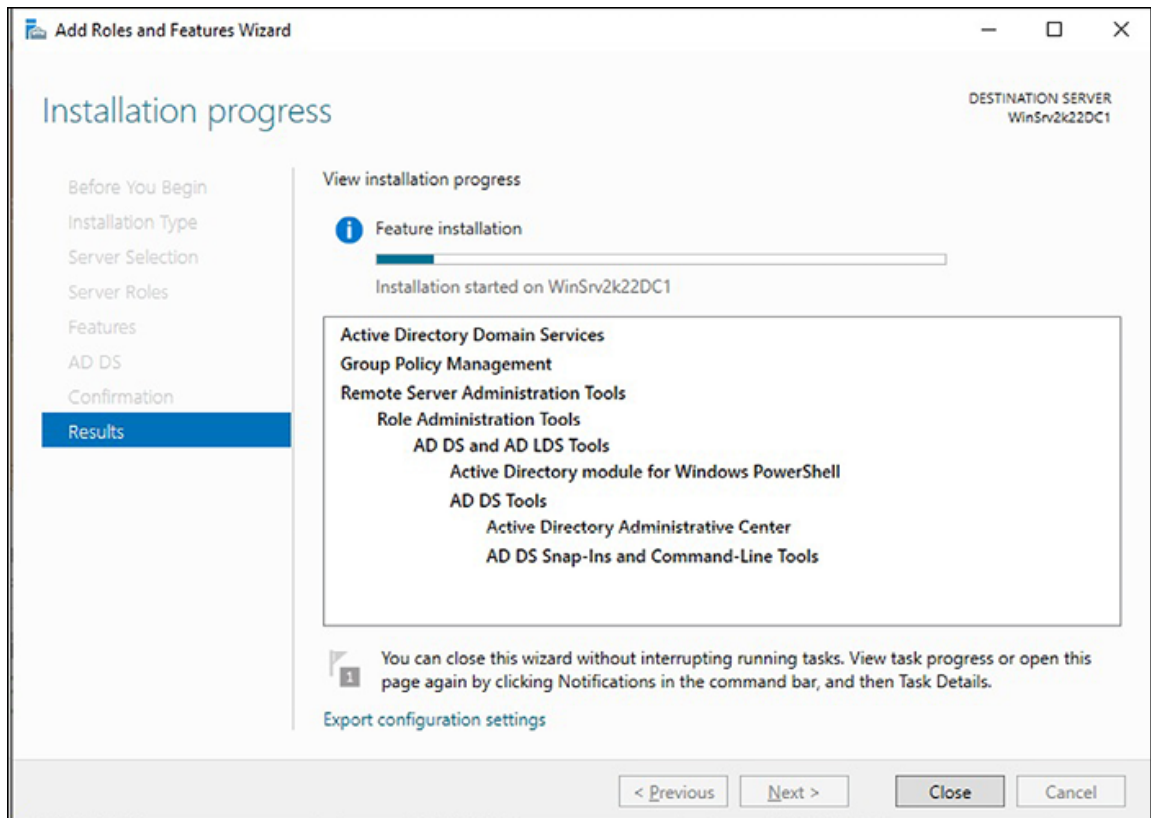
Figure 5.3: *Installing AD DS role in Windows Server 2022 using Server Manager*
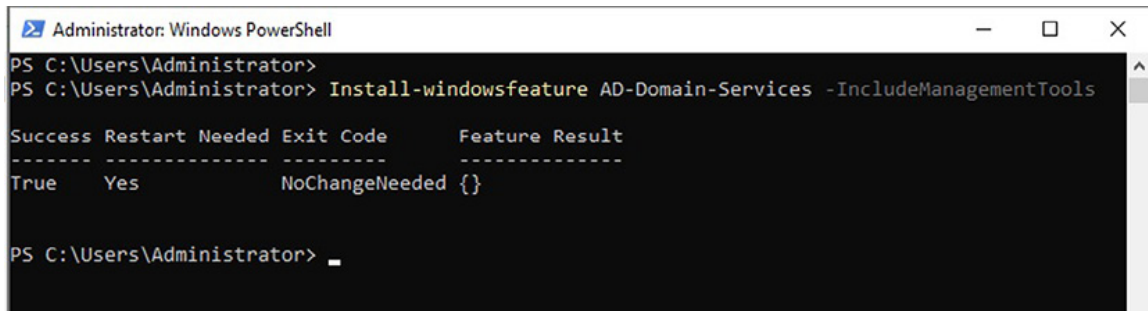
Adding AD DS role using Windows PowerShell

To begin the process of adding an AD DS role in Windows Server 2022 using Windows PowerShell, follow the following steps:

1. Launch **Windows PowerShell** by right-clicking on the Start button.

2. Within the Windows PowerShell interface, input the provided cmdlet and then press *Enter*:

   ```
   Install-WindowsFeature AD-Domain-Services -
   IncludeManagementTools
   ```

3. The installation of the AD DS role will commence shortly, as depicted in *Figure 5.4:*

Figure 5.4: *Installing AD DS role in Windows Server 2022 using Windows PowerShell*

Understanding the Domain Name System role

The **Domain Name System** (**DNS**), a protocol to convert domain names into IP addresses, controls the name resolution process. DNS has been around since ARPANET, but it became a standard with the publication of the first DNS specifications in the early 1980s as **Requests for Comments** (**RFC**) documents.

The DNS architecture is hierarchical and comprises three main components: the domain name, domain namespace, and name server. These three components are explained as follows:

- The domain name represents the specific website and includes multiple parts known as labels, separated by periods (for example, Dautti.com).

- The domain namespace is a hierarchical naming system that organizes the DNS database into zones. Each zone represents a different level of the domain hierarchy, such as the root domain, **Top-Level Domains** (**TLDs**), **Second-Level Domains** (**SLDs**), subdomains, and hostnames.

- The name server plays a crucial role in the DNS system. It is a network server that handles queries sent to a directory service. For example, when a query is made with a domain name, the name server responds by mapping the domain name to the correct IP address, allowing the client to connect with the desired website.

Understanding the DNS architecture helps comprehend how the internet's addressing system functions and enables seamless communication between websites and devices.

DNS zones

To understand the DNS architecture comprehensively, it is essential to examine its zones. DNS zones are fundamental components that contribute to the overall structure and functionality of the system. A DNS zone is a hierarchical structure within the DNS namespace that facilitates the organization and management of DNS information. It allows for dividing the DNS namespace into separate zones, each responsible for storing information about specific domains or subdomains.

Within the DNS architecture, three primary types of zones exist, each serving the specific purpose given as follows:

- The primary zone is the authoritative source for a particular DNS domain. It stores a complete and direct copy of the DNS database, including all the zone records. Changes made to the primary zone are propagated to other DNS servers, ensuring consistent and up-to-date information for the domain.

- The secondary zone acts as a backup to the primary zone. It contains a replicated copy of the primary zone's DNS database. The secondary zone is not editable; it aims to provide redundancy and fault tolerance. When the primary zone becomes unavailable, the secondary zone can step in and handle DNS queries, ensuring continuity of service.

- A stub zone is conceptually similar to a secondary zone but with one notable difference. It does not store a complete copy of the DNS database like a secondary zone. Instead, it contains essential information to identify and locate the authoritative DNS servers for a specific domain. The stub zone acts as a reference point for DNS resolution, directing queries to the authoritative DNS servers for further processing.

By offering these different zone types, DNS allows for efficient management, replication, and fault tolerance within the domain name system. Primary zones ensure authoritative control, while secondary and stub zones provide redundancy and distributed resolution capabilities.

How does DNS work?

DNS is upheld by a database that employs a distributed client/server architecture, where network hosts represent the servers' names. Consequently, DNS uses a distributed structure in which the recursive resolver acts as an intermediary between your browser and the DNS infrastructure. The resolver undertakes actions involving root servers, **Top-Level Domains** (**TLDs**), and domain name servers to translate the domain name into its associated IP address. This systematic process enables your browser to communicate with the intended Web server and retrieve the requested content. In this regard, the subsequent steps describe the process of how DNS works:

1. Enter `www.dautti.com` in your browser's address bar and hit *Enter*. Your computer's browser initiates a request to access the website **www.dautti.com**.

2. The first server your browser encounters is the **recursive resolver**. This resolver is usually provided by your **Internet Service Provider (ISP)** and handles the request on your behalf.

3. The recursive resolver then contacts the **root servers** spread across different locations worldwide. In our example, these root servers contain crucial information about **Top-Level Domains (TLDs)**, such as **.com**.

4. The root servers provide the necessary DNS information to the recursive resolver, enabling it to proceed with the **resolution process**.

5. Once the recursive resolver receives the information from the root servers, it contacts the **domain name server** responsible for dautti.com. Next, the recursive resolver seeks to determine the **IP address** associated with the domain name by leveraging the DNS's local DNS database.

6. After obtaining the Web server's IP address, the recursive resolver communicates it back to your computer's browser. Now equipped with the correct IP address, your browser can connect with the Web server and access its content.

Components of name resolution

Several components and configurations are vital in ensuring efficient name resolution and smooth communication within networks. These elements work together to provide a seamless experience for users:

- The hosts and lmhosts files are essential for local device name resolution. These files, stored in the `C:\Windows\system32\drivers\etc` directory, contain mappings of IP addresses to hostnames (in the host's file) and IP addresses to computer names (in the `lmhosts` file). They are manually edited and used for DNS and NetBIOS name resolution, respectively.

- A hostname is a unique logical identifier assigned to a device in a network. It represents the device's name and is used for internal communication within a **Local Area Network** (**LAN**). The hostname is crucial for locating and addressing machines accurately.

- Authoritative DNS servers are responsible for holding the DNS records of a specific domain. System administrators can configure these servers manually or rely on dynamic updates from other DNS servers. Authoritative DNS ensures the accuracy and reliability of domain-related information.

- Non-authoritative DNS servers store cached information obtained from previous DNS lookups. This cache holds frequently accessed domain records, allowing for faster name resolution by eliminating the need to query authoritative servers repeatedly.

- **Windows Internet Naming Service** (**WINS**) servers are used in Windows networks to map IP addresses to NetBIOS names. They play a critical role when devices connect to shared folders or printers, facilitating seamless communication by resolving NetBIOS names to corresponding IP addresses.

- **Universal Naming Convention** (**UNC**) is a standard method for identifying network shares in Unix systems. It uses a syntax with double backslashes (\) preceding the

server's name, followed by the specific folder or resource, for example, `\\hostname\folder`. UNC simplifies the process of accessing and sharing files across Unix-based networks.

By leveraging these components and configurations, networks can achieve efficient name resolution, enabling devices to locate and communicate with each other effectively.

Note: There is a significant distinction between a domain and a domain name. The former refers to the logical arrangement of users, servers, devices, and resources within a specific group of such elements. On the other hand, the latter denotes the logical naming system that governs the internet, encompassing Web servers and websites.

Exercise 5.2—Adding DNS server role

This exercise outlines the procedure for adding a DNS server role using the Server Manager and PowerShell.

Adding DNS server role using Server Manager

To begin the process of adding a DNS Server role in Windows Server 2022 using Server Manager, follow the following steps:

1. Open **Server Manager** from the Start menu and click the **Add Roles and Features** link.

2. Click on the **Next** button on the **Before you begin** page of the Add Roles and Features Wizard.

3. Accept the default settings on the Select *Installation Type* page and click **Next**.

4. Accept the default settings on the Select destination server page and click **Next**.

5. Choose the **DNS Server** role from the select server roles page list. When the **Add Features required for the DNS** window appears, click the **Add Features** button. Then, click the **Next** button to continue adding the DNS Server role.

6. Accept the default settings on the *Select Features* page and click the **Next** button to proceed.

7. On the DNS Server page, click on the **Next** button.

8. Review the options on the Confirm installation selections page and click the **Install** button.

9. The installation process for the DNS Server role will begin, as indicated by the progress bar shown in *Figure 5.5*. Once the installation is complete, click the **Close** button to exit the Add Roles and Features Wizard. Please refer to the following figure:
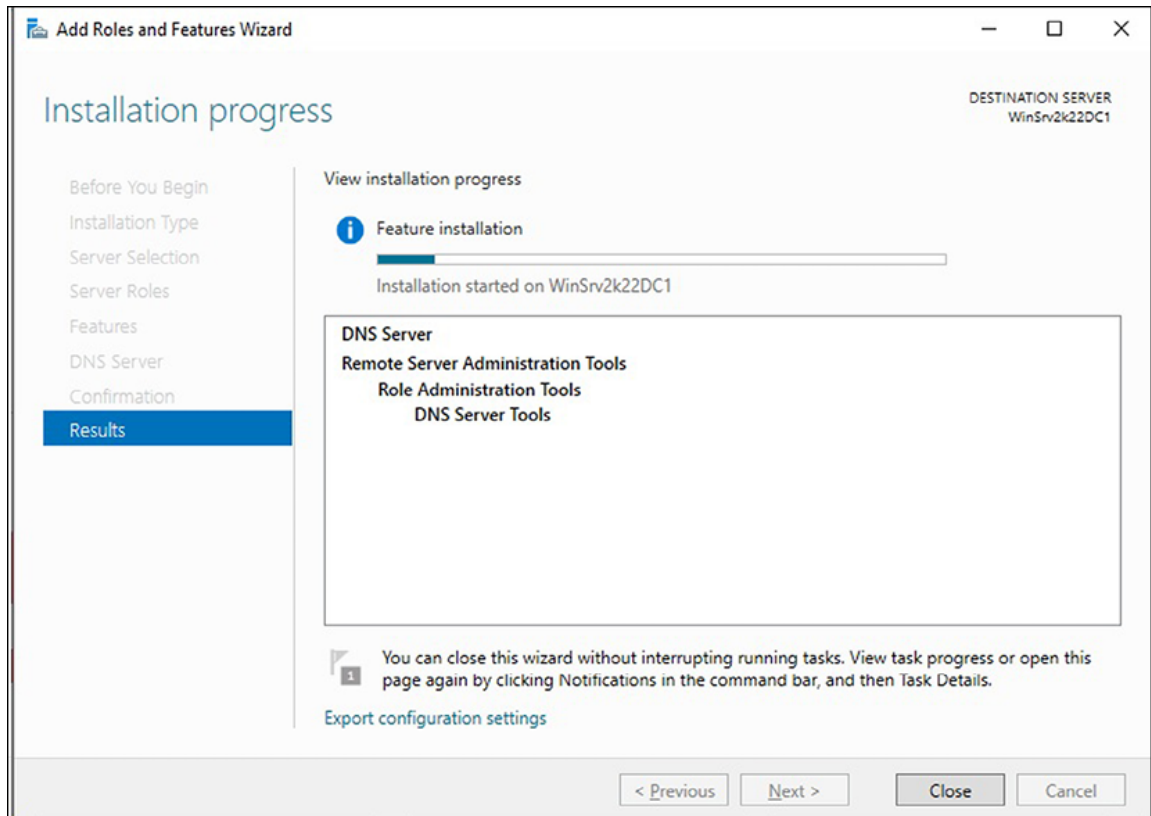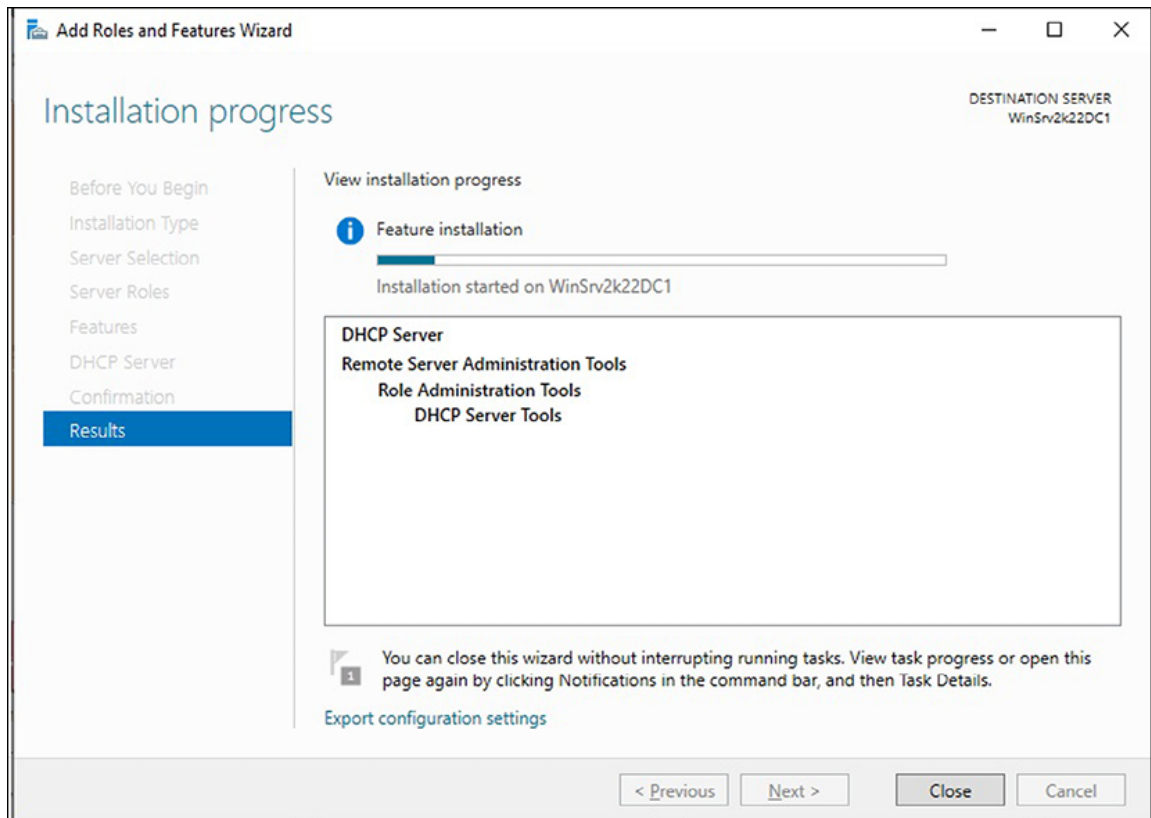

Figure 5.5: *Installing DNS server role in Windows Server 2022 using Server Manager*

Adding DNS server role using Windows PowerShell
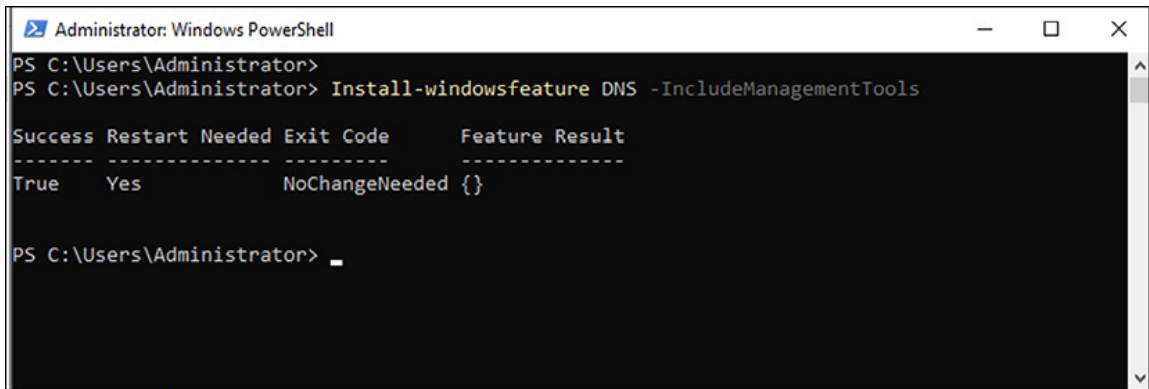
To begin the process of adding a DNS Server role in Windows Server 2022 using Windows PowerShell, follow the following steps:

1. Launch **Windows PowerShell** by right-clicking on the **Start** button.

2. Within the Windows PowerShell interface, input the provided cmdlet and then press *Enter*:

```
Install-WindowsFeature DNS -IncludeManagementTools
```

3. The installation of the DNS Server role will commence shortly, as depicted in *Figure 5.6*:

Figure 5.6: *Installing DNS server role in Windows Server 2022 using Windows PowerShell*

Getting to know the Dynamic Host Configuration Protocol role

The **Dynamic Host Configuration Protocol** (**DHCP**) is a network service that automatically assigns IP addresses to devices within a network. In a client/server architecture, DHCP operates by clients requesting IP addresses and servers responding with the requested services. In this context, a DHCP service is called a DHCP server.

This section focuses on DHCP servers, which dynamically assign IPv4 addresses to devices. Typically, these IP addresses are allocated from a designated pool within the DHCP server. The assigned IP addresses have a predetermined lease period and are referred to as leased IP addresses. Once the lease expires, the DHCP client must request another IPv4 address, which may sometimes result in reassigning the same IP address. This process is known as IP address renewal.

The presence of a DHCP server significantly simplifies and expedites the IP address assignment process for network

administrators.

How does DHCP work?

The **Discovery, Offer, Request, and Acknowledgment** (**DORA**) process outlines the functioning of DHCP. It unfolds as follows:

- When a computer is powered on and its operating system boots up, the DHCP client service broadcasts a **DHCPDISCOVER** message, which requests an IP address. This broadcast aims to locate a DHCP server within the LAN. If a DHCP server is available, it accepts the DHCPDISCOVER message from the client and reserves an **IP address**.

- In response to the client's request, the DHCP server sends a **DHCPOFFER** message. This message contains the allocated IP address and additional information like the subnet mask, default gateway, lease time, and the DHCP server's IP address.

- Upon receiving the DHCPOFFER message, the client sends a **DHCPREQUEST** message to the DHCP server, confirming its interest in the offered IP address. This step ensures the client formally requests the IP address it intends to use.

- On the server side, once the DHCPREQUEST message reaches the DHCP server, it initiates an **acknowledgment** process. The server responds to the client with a **DHCPPACK** message, which includes the requested elements mentioned earlier. This DHCPPACK message marks the completion of the IP address assigned to the DHCP client by the DHCP server.

The DORA process provides a systematic and standardized approach for DHCP to allocate IP addresses efficiently within a computer network.

Exercise 5.3—Adding DHCP server role

This exercise outlines the procedure for adding a DHCP server role using the Server Manager and PowerShell.

Adding DHCP server role using Server Manager

To begin the process of adding a DHCP Server role in Windows Server 2022 using Server Manager, follow the following steps:

1. Open **Server Manager** from the Start menu and click the **Add Roles and Features** link.

2. Click on the **Next** button on the **Before you begin** page of the Add Roles and Features Wizard.

3. Accept the default settings on the Select *Installation Type* page and click **Next**.

4. Accept the default settings on the Select destination server page and click **Next**.

5. Choose the **DHCP Server** role from the **Select Server Roles** page list. When the **Add Features required** for the DHCP window appears, click the **Add Features** button. Then, click the **Next** button to continue adding the DHCP Server role.

6. Accept the default settings on the **Select Features page** and click the **Next** button to proceed.

7. On the DHCP Server page, click on the **Next** button.

8. Review the options on the **Confirm installation selections** page and click the **Install** button.

9. The installation process for the DHCP Server role will begin, as indicated by the progress bar shown in *Figure 5.7*. Once the installation is complete, click on the **Close** button to exit the Add Roles and Features Wizard, as shown in the following figure:

Figure 5.7: *Installing DHCP server role in Windows Server 2022 using Server Manager*
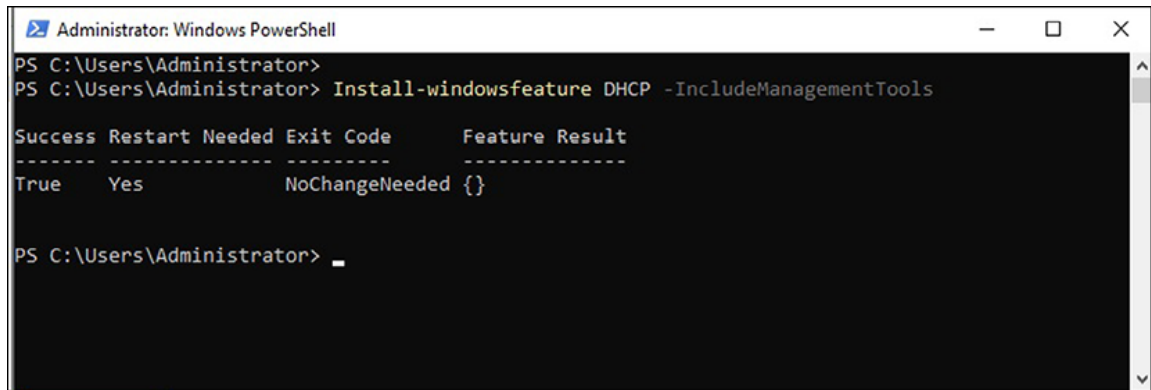
Adding DHCP server role using Windows PowerShell

To begin the process of adding a DHCP Server role in Windows Server 2022 using Windows PowerShell, follow the following steps:

1. Launch **Windows PowerShell** by right-clicking on the `Start` button.

2. Within the Windows PowerShell interface, input the provided cmdlet and then press *Enter*:

   ```
   Install-WindowsFeature DHCP -
   IncludeManagementTools
   ```

3. The installation of the DHCP Server role will commence shortly, as depicted in *Figure 5.8*:

Figure 5.8: *Installing DHCP server role in Windows Server 2022 using Windows PowerShell*

What is Hyper-V's role?

To gain a technical understanding of virtualization and the technology involved in setting up a **Virtual Machine** (**VM**), we can explore how it allows us to run operating systems, applications, and other tools within the VM. Moreover, virtualization extends to configuring storage devices and network resources. Instead of operating multiple physical servers, virtualization consolidates them into a single physical server, enabling efficient utilization of resources.

Windows Server 2022 includes the Hyper-V feature, which facilitates virtualization. Hyper-V originated from Windows Virtual PC and was first introduced in Windows Server 2008. Since then, it has garnered attention from system administrators, establishing itself as a prominent contender in the virtualization platform market, competing with VMware. From a technical standpoint, Hyper-V provides services that enable the provisioning and managing VMs and their associated resources.

Modes of virtualization

In today's virtualized environments, there are three commonly used modes of virtualization, which are explained as follows:

- *A fully virtualized mode* enables the secure execution of one or more **Operating Systems** (**OSs**) in isolation on a single physical server. In this mode, the guest OSs cannot be recompiled but instead use the resources of the host OS. It

provides a complete virtual environment for each OS instance.

- In *para-virtualized mode*, a computer within a computer is created, where an OS is installed without simulating the hardware. Instead, it offers an **Application Programming Interface** (**API**) that allows the guest OS to be recompiled. This mode requires modifications to the guest OS and the virtualization software to achieve efficient communication.

- *Containerization mode* involves containers, which are self-contained packages comprising the runtime environment, system tools, and necessary settings to run the application code. Containers provide an isolated environment for applications, allowing them to run consistently across different systems without needing full OS virtualization. This mode offers lightweight and efficient deployment of applications.

These three virtualized modes cater to different needs and use cases in virtualized environments, providing flexibility and optimization based on the applications and systems' specific requirements.

The architecture of Hyper-V

The architecture of Hyper-V follows a hierarchical structure, with the hypervisor serving as the central element that forms the foundation of the Hyper-V virtual platform. The hypervisor resides at the root level and directly interacts with the underlying hardware. It is responsible for managing and controlling the virtualization environment.

The root component creates branch OSs within this architecture as isolated execution environments. These branch OSs operate within a logical isolation unit without direct access to the underlying hardware. They are designed to host guest OSs and provide a secure and isolated environment for their execution.

Specific components known as the **Virtualization Service Provider** (**VSP**) and **Virtualization Service Consumer** (**VSC**) facilitate communication between the root portion and the branch

OSs. These components use logical channels called the **Virtual Machine Bus** (**VMBus**) to establish communication pathways. The VMBus enables efficient and secure communication between the root portion (hypervisor) and the branch OSs, allowing coordinated operations and resource sharing.

The Hyper-V architecture employs a hierarchical structure with the hypervisor at the root, branch OSs for isolated execution, and communication facilitated by VSP, VSC, and the virtual machine bus. This architecture enables the efficient management and operation of virtualized environments within the Hyper-V virtual platform.

Nesting the virtualization

Nested virtualization refers to the capability of running a virtual machine within another VM. That means that the host machine's hardware allows the execution of Hyper-V from within a VM, enabling the creation and management of additional VMs within this nested setup.

Although nested virtualization may seem unusual, it has gained support and recognition since Windows Server 2016. Microsoft has introduced features and enhancements to facilitate nested virtualization, making it a viable option for specific use cases. To better grasp and manage this concept, you can think of running Hyper-V from the guest **Operating System** (**OS**) in the same manner as it runs from the host OS. This approach allows for effectively nesting one instance of Hyper-V within another, enabling multiple virtualization layers.

Using nested virtualization, you can explore scenarios where running VMs within VMs becomes essential. This approach enables testing, development, and experimentation within a controlled virtual environment. While not commonly used in everyday scenarios, nested virtualization provides flexibility and versatility for specific use cases, expanding the possibilities of virtualized environments.

Prerequisite for virtualization

To utilize Hyper-V, the server's processors must have virtualization support. That means the physical server's processor must be equipped with virtualization technology. Hence, it is imperative that the hosting machine is equipped with an Intel or AMD processor that has Intel **Virtualization Technology** (**VT**) or AMD Virtualization enabled.

Enabling virtualization technology on the processor allows for efficient and secure execution of virtual machines. It provides the necessary hardware-level support for virtualization, enabling the virtualization software, such as Hyper-V, to effectively create and manage virtual machines.

Having processors with VT or AMD Virtualization support is a fundamental requirement for deploying and utilizing Hyper-V and other virtualization platforms. It ensures the smooth operation and optimal performance of virtualized environments.

Exercise 5.4—Adding Hyper-V role

This exercise outlines the procedure for adding a Hyper-V role using Server Manager and PowerShell.

Adding Hyper-V role using Server Manager

To begin the process of adding a Hyper-V role in Windows Server 2022 using Server Manager, follow the following steps:

1. Open **Server Manager** from the Start menu and click the **Add Roles and Features** link.
2. Click on the **Next** button on the Before you begin page of the **Add Roles and Features** Wizard.
3. Accept the default settings on the Select *Installation Type* page and click **Next**.
4. Accept the default settings on the Select destination server page and click **Next**.
5. Choose the **Hyper-V** role from the Select *Server Roles* page list. When the Add Features required for the Hyper-V window appears, click the **Add Features** button. Then, click on the **Next** button to continue adding the Hyper-V role.

6. Accept the default settings on the **Select Features** page and click the **Next** button to proceed.

7. On the Hyper-V page, click the **Next** button.

8. On the **Create virtual switches** page, reserve a network adapter that the virtual switch will use, and then click on the **Next** button.

9. Accept the defaults on the **Virtual machine migration** page and click the **Next** button to move forward.

10. Accept the defaults on the **Default stores** page and click the **Next** button.

11. Review the options on the Confirm installation selections page and click the **Install** button.

12. The installation process for the Hyper-V role will begin, as indicated by the progress bar shown in *Figure 5.9.* Once the installation is complete, click the **Close** button to exit the Add Roles and Features Wizard. Afterward, **restart** the server to complete the installation of the Hyper-V role:

Adding Hyper-V role using Windows PowerShell

To begin the process of adding a Hyper-V role in Windows Server 2022 using Windows PowerShell, follow the following steps:

1. Launch **Windows PowerShell** by right-clicking on the `Start` button.

2. Within the Windows PowerShell interface, input the provided cmdlet and then press *Enter*:

   ```
   Install-WindowsFeature Hyper-V -IncludeManagementTools
   ```

3. The installation of the *Hyper-V* role will commence shortly, as depicted in *Figure 5.10*. Afterward, **restart** the server to complete the installation of the *Hyper-V* role. Please refer to the following figure:

Figure 5.10: Installing Hyper-V role in Windows Server 2022 using Windows PowerShell

What is the use of a Web server role?

A Web service is a network service that operates within Web technology. It facilitates communication between a Web browser and a web server, following the request/response paradigm. Typically, Web services function over the internet, using the **Hypertext Transfer Protocol** (**HTTP**) as the communication protocol. To gain a comprehensive understanding of web services,

it is essential to familiarize oneself with IIS **Internet Information Services** (**IIS**), the **World Wide Web** (**WWW**), and **File Transfer Protocol** (**FTP**).

IIS, developed by Microsoft, is a robust and scalable Web server for hosting Web applications. It supports various communication protocols, including HTTP, HTTPS, FTP, FTPS, SMTP, and NNTP, enabling seamless interaction between Web browsers and the Web server. Microsoft introduced a scripting technology known as **Active Server Pages** (**ASP**) to allow dynamic content on the server side.

With the release of IIS version 10, Microsoft has significantly emphasized enhancing security. That includes support for scripts with longer execution times and adopting the HTTP/2 protocol. In addition, Microsoft introduced the Microsoft Edge browser based on the Chromium engine, which offers improved compatibility and performance. Noteworthy features introduced in IIS 10 for Windows Server 2022 include upgraded server-side cipher suite negotiation for HTTP/3, PowerShell cmdlets for IIS administration, wildcard host headers, and other enhancements. These improvements have contributed to enhanced performance and strengthened security within IIS.

Understanding the concepts of IIS, WWW, and FTP, along with the advancements in IIS 10, provides valuable insights into Web services' operation, capabilities, and security measures within the Web technology landscape.

Web elements and technologies

Understanding the intricacies of Web technology and its various Internet services is essential in today's digital landscape. One common source of confusion is the distinction between the Internet and the World Wide Web. While the internet is a vast network connecting computers globally, the WWW represents just one of the many services operating within this network. In this context, it becomes crucial to grasp concepts such as Web services, **Internet Information Services** (**IIS**), **File Transfer Protocol** (**FTP**), Web directories, sites, hardware and software ports, and security measures like **Secure Sockets Layer** (**SSL**)

and certificates. This comprehensive understanding will enable us to navigate the Web effectively, develop robust Web applications, and ensure secure communication between browsers and Web servers. Now, let us delve deeper into the intricacies of these concepts to gain a holistic view of Web technology and its underlying mechanisms.

- The confusion between the internet and the World Wide Web is common. Many people mistakenly perceive the WWW as synonymous with the internet itself, but in reality, the WWW is just one of the numerous Internet services accessible through the HTTP protocol. It comprises electronic documents created with **Hypertext Markup Language** (**HTML**) and is a platform for accessing and navigating Web pages.

- On the other hand, File Transfer Protocol is a specific internet service primarily used for transferring files between computers over the internet. It finds extensive applications in corporate networks for sending and receiving corporate data. FTP is commonly employed on websites and Web servers for uploading and downloading files. It operates on a client/server network architecture, establishing sessions through port 21 and transferring data through port 20.

- In the IIS context, a Web directory represents a website associated with an application pool. A Web directory encompasses multiple applications, each supported by a dedicated worker process within the application pool. This separation ensures that if a specific Web application encounters issues, it does not impact the functionality of other applications running in different application pools.

- A website is a collection of Web pages grouped to present content on the intranet or internet through Web services. While HTML is commonly used to structure Web pages and design websites, various scripting languages introduce dynamic content to specific websites. For example, by adding the Web Server role in Windows Server 2022, the

automatic creation of a default website, representing a single Web page website, occurs.

- Hardware ports are physical interfaces in computers, peripheral devices, or network devices that facilitate communication and management. Conversely, software ports, also known as application ports, serve as logical endpoints where applications on a server communicate with other applications within a LAN, WAN, or the internet. For instance, Web servers use port 80 for the HTTP protocol and port 443 for the HTTPS protocol.

- **Secure Sockets Layer** (**SSL**) is a communication technology that encrypts the communication channel between a Web server and a browser, typically over the HTTPS protocol on port 443. SSL ensures the secure transmission of data between the server and the browser. In this secure infrastructure, certificates are crucial in encrypting all transmitted data. Certificates, often issued by a **Certificate Authority** (**CA**), are used by both the website and the browser to establish a secure session for browser-to-server or server-to-server communications.

- Digital certificates secure the communication channel between a website and a browser. They are electronic documents that enable secure data exchange over the Internet. Certificate Authorities are trusted entities that issue these certificates. The secure Web infrastructure commonly employs a **Public Key Infrastructure** (**PKI**), which utilizes certificates to validate the ownership of public keys and establish secure connections.

Exercise 5.5—Adding Web Server Role

This exercise outlines the procedure for adding a **Web Server** (**IIS**) role using Server Manager and PowerShell.

Adding Web Server role using Server Manager

To begin the process of adding a Web Server (IIS) role in Windows Server 2022 using Server Manager, follow the following steps:

1. Open **Server Manager** from the Start menu and click the **Add Roles and Features** link.

2. Click on the **Next** button on the **Before you begin** page of the Add Roles and Features Wizard.

3. Accept the default settings on the **Select Installation Type** page and click **Next**.

4. Accept the default settings on the **Select Destination Server** page and click **Next**.

5. Choose the **Web Server** role from the *Select Server Roles* page list. When the Add Features required for the Web Server window appears, click the **Add Features** button. Then, click the **Next** button to continue adding the Web Server role.

6. Accept the default settings on the **Select Features** page and click the **Next** button to proceed.

7. On the Web Server page, click on the **Next** button.

8. On the Select role services page, select the **role services** to install for the Web Server (IIS) role and click the **Next** button.

9. Review the options on the **Confirm installation selections** page and click the **Install** button.

10. The installation process for the Web Server role will begin, as indicated by the progress bar shown in *Figure 5.11*. Once the installation is complete, click on the **Close** button to exit the Add Roles and Features Wizard:
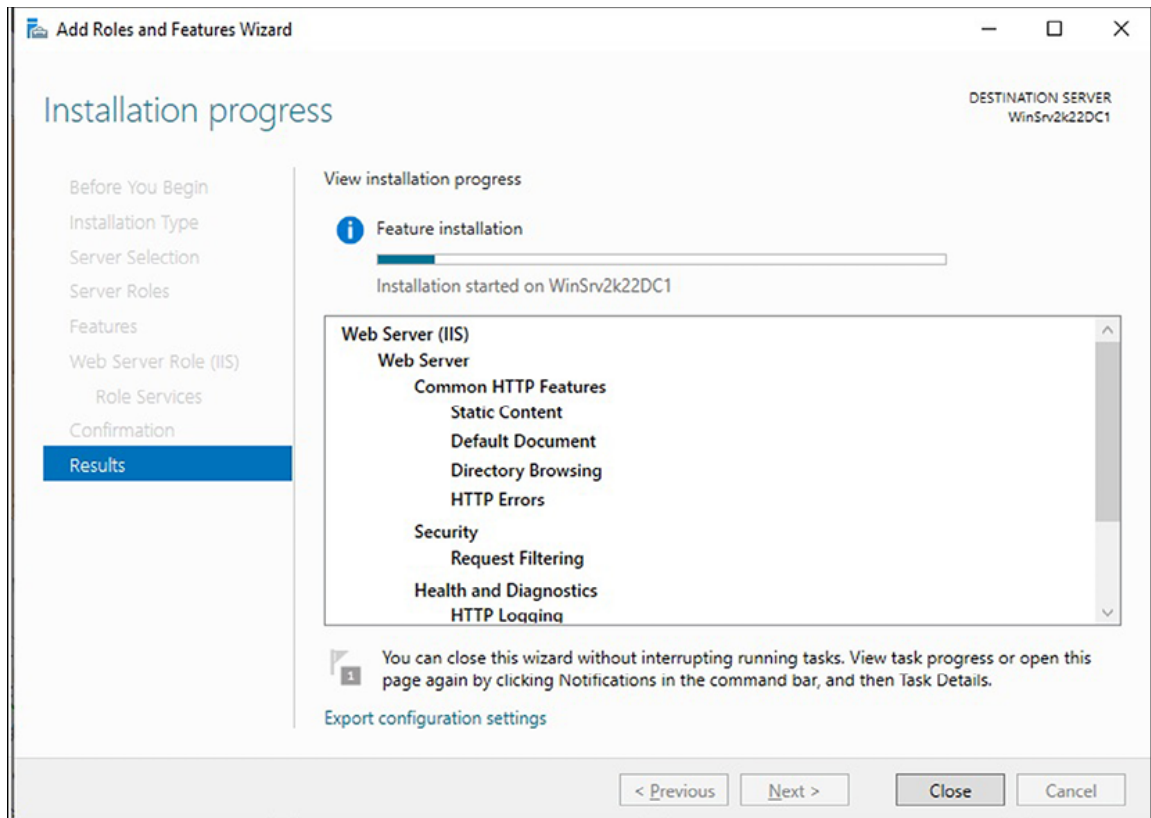
Figure 5.11: *Installing Web Server (IIS) role in Windows Server 2022 using Server Manager*
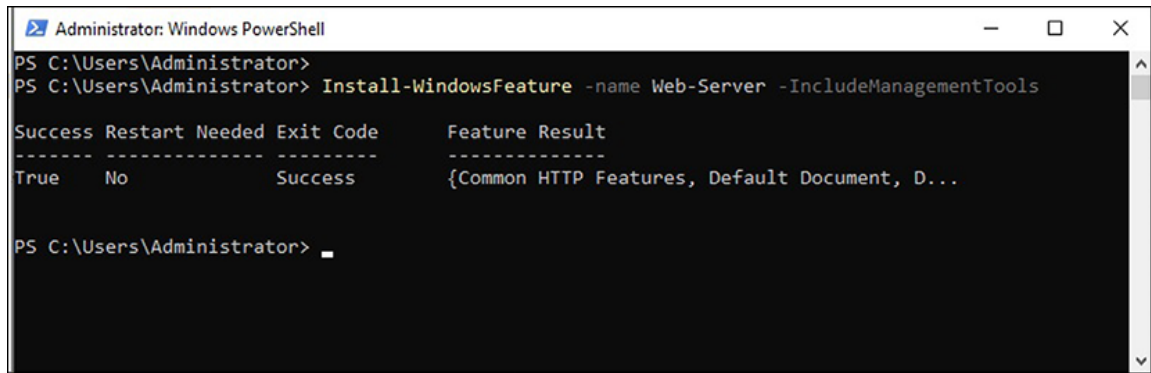
Adding Web Server role using Windows PowerShell

To begin the process of adding a Web Server (IIS) role in Windows Server 2022 using Windows PowerShell, follow the following steps:

1. Launch **Windows PowerShell** by right-clicking on the Start button.

2. Within the Windows PowerShell interface, input the provided cmdlet and then press *Enter*:

   ```
   Install-WindowsFeature -name Web-Server -
   IncludeManagementTools
   ```

3. The installation of the Web Server role will commence shortly, as depicted in *Figure 5.12*:

Figure 5.12: *Installing Web Server (IIS) role in Windows Server 2022 using Windows PowerShell*

Getting to know the Print and Document Services role

Print and Document Services (**PDS**) is a comprehensive network-based solution beyond traditional printing capabilities. In addition to facilitating centralized printing across a network, PDS offers an additional feature for document scanning. This scanning service allows users to conveniently receive scanned documents from a network scanner and efficiently send them to share network resources.

PDS is typically integrated as a role within Windows Server 2022, enhancing its functionality. Organizations can streamline their printing and document management processes by incorporating PDS into the server environment, achieving greater efficiency and productivity. Users can leverage the centralized printing capability to send print jobs from various network-connected devices, simplifying the printing workflow.

Furthermore, PDS's document scanning service enables users to digitize physical documents and seamlessly transmit them to designated network destinations. This functionality facilitates document sharing, collaboration, and archival, reducing reliance on physical paper documents.

PDS is a versatile solution that combines network printing and document scanning capabilities. By integrating PDS as a role in Windows Server 2022, organizations can optimize their printing

and document management workflows, improving efficiency and promoting a digital-centric approach to information handling.

PDS role services

PDS extends its capabilities beyond basic printing and scanning by offering these role services. It provides administrators and users with comprehensive tools to effectively manage printing queues, enable internet-based printing, facilitate client-side printing, and ensure compatibility with non-Windows operating systems. This comprehensive approach enhances the flexibility and versatility of the printing infrastructure, catering to the diverse needs of organizations and promoting efficient document management. These role services are explained as follows:

- Print Server role service empowers administrators to manage printing queues and effectively deploy and migrate print servers. Organizations can efficiently handle print jobs and ensure smooth operations across the network by using the Print Server role.

- With the Internet Printing role service, it becomes possible to establish a website that allows users to print over the Internet. This feature enables convenient remote printing capabilities, enabling users to submit print jobs from their devices and have them processed by the network printer.

- **Line Printer Daemon** (**LPD**) Service role service enables Unix-based computers and non-Windows operating systems to leverage the **Line Printer Remote** (**LPR**) protocol for printing. By incorporating LPD, organizations can ensure compatibility and allow printing functionality across diverse computing environments, promoting seamless cross-platform printing.

Printer and printing concepts

The following sections explore various concepts related to printers and printing, providing a comprehensive understanding of the topic.

- As the name implies, a local printer is physically connected to a computer through the parallel or USB port (printer port). Its primary purpose is to serve the computer to which it is connected. However, if the host computer shares the printer, it can also provide printing services to other computers on the network.

- In contrast, a network printer is a dedicated computer network printer offering printing services. It uses an Ethernet or Wi-Fi interface and can be accessed simultaneously by multiple devices connected to the same network. Network printers can even be accessed online, depending on the network setup.

- Printer pooling is a feature in Windows Server 2022 that allows configuring two or more physical printers into a single logical printer. The printers installed on the print server must be nearly identical or compatible with the same print driver. From the client's perspective (referred to as the front end), even though multiple physical network printers exist in the background, they appear as a single printer. This logical pooling of printers helps balance the workload and enhances usability, providing users with efficient printing capabilities.

- Furthermore, Web printing is a concept that integrates to integrate printing with Web browsers for easier understanding and accessibility. To set up Web printing in an organization's network, the Print and Document Services role and Internet Printing as a role service must be added. In addition, the Web Server (IIS) role is required.

- Like local and network printing, Web printing also includes methods for managing print jobs. Users can control print jobs through Web printing management tools accessible via a Web browser, just like when managing a local or network printer. For example, by entering `http://servername/printers` in the browser's address bar and selecting the printer, users can access a Web interface displaying a list of printable jobs, as the provided screenshot shows. However, it is essential to note that before utilizing Web printing, the

Internet Printing role services must be added to the server in addition to the PDS role.

By exploring these concepts, we understand printers and printing comprehensively, encompassing local and network printing, printer pooling, and Web printing. This knowledge enables organizations to effectively manage their printing infrastructure, enhance productivity, and leverage the benefits of modern printing technologies.

Exercise 5.6—Adding PDS role

This exercise outlines the procedure for adding a PDS role using Server Manager and PowerShell.

Adding PDS role using Server Manager

To begin the process of adding a PDS role in Windows Server 2022 using Server Manager, follow the following steps:

1. Open **Server Manager** from the Start menu and click the **Add Roles and Features** link.

2. Click on the **Next** button on the **Before you begin** page of the Add Roles and Features Wizard.

3. Accept the default settings on the *Select Installation Type* page and click **Next**.

4. Accept the default settings on the Select destination server page and click **Next**.

5. Choose the **PDS role** from the *Select Server Roles* page list. When the Add Features required for the PDS window appears, click the **Add Features** button. Then, click on the **Next** button to continue adding the PDS role.

6. Accept the default settings on the **Select features** page and click the **Next** button to proceed.

7. Click the **Next** button on the **Print and Document Services** page.

8. Select the **role services** to install for the PDS role on the **Select role services** page and click the **Next** button.

9. Review the options on the **Confirm installation selections** page and click the **Install** button.

10. The installation process for the PDS role will begin, as indicated by the progress bar shown in *Figure 5.13*. Once the installation is complete, click on the **Close** button to exit the Add Roles and Features Wizard:
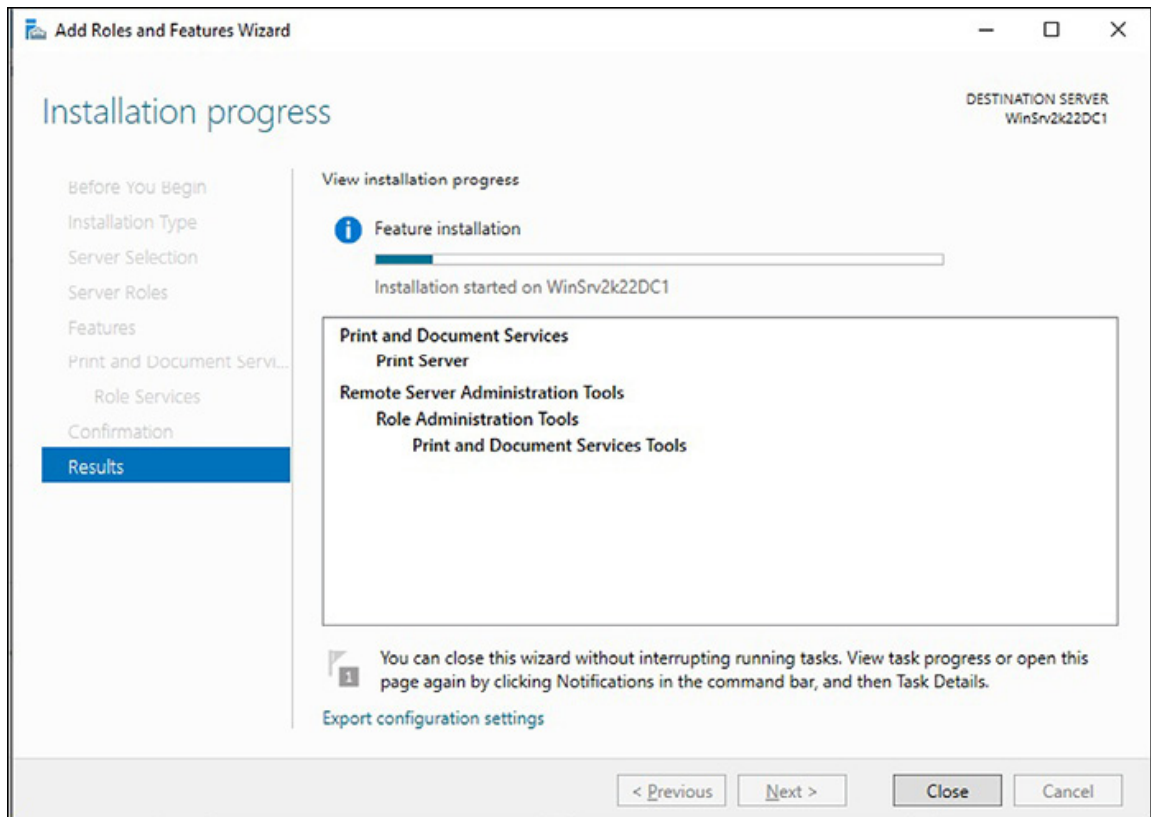
Figure 5.13: *Installing PDS role in Windows Server 2022 using Server Manager*
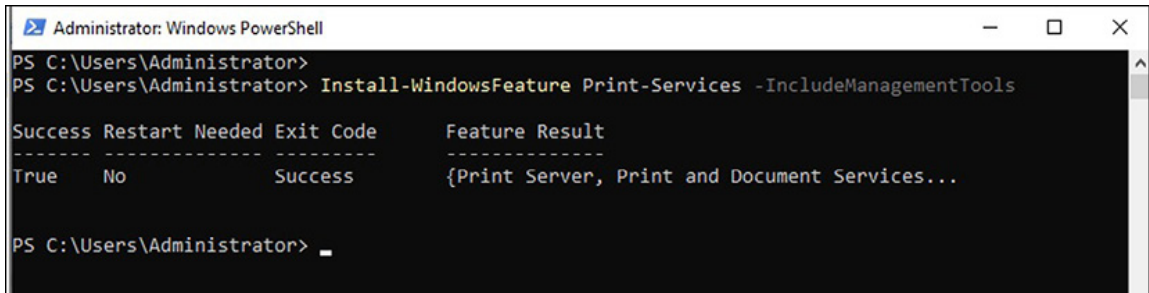
Adding PDS role using Windows PowerShell

To begin the process of adding a PDS role in Windows Server 2022 using Windows PowerShell, follow the following steps:

1. Launch **Windows PowerShell** by right-clicking on the Start button.

2. Within the Windows PowerShell interface, input the provided cmdlet and then press *Enter*:

```
Install-WindowsFeature Print-Services -
IncludeManagementTools
```

3. The installation of the PDS role will commence shortly, as depicted in *Figure 5.14*:

Figure 5.14: *Installing PDS role in Windows Server 2022 using Windows PowerShell*

What is unique about the Remote Access Role?

The **Remote Access** (**RA**) role in Windows Server 2022 facilitates remote access to corporate network resources. Remote access encompasses monitoring and controlling access to a computer or network from any location and at any time. This functionality empowers corporate users to work remotely while maintaining seamless connectivity with the corporate network.

To configure a Remote Access server in Windows Server 2022, the Remote Access role must be added to the server. This role provides the necessary infrastructure and services to enable remote access capabilities, including DirectAccess, RRAS, and Web Application Proxy. Organizations can establish a robust and secure remote connectivity solution by setting up the Remote Access role, empowering users to access network resources remotely while ensuring data confidentiality and integrity.

By deploying the Remote Access role, organizations can establish a secure and reliable infrastructure that allows authorized users to access resources within the corporate network remotely. This role enables remote workers to connect to file shares, databases, applications, and other essential resources, ensuring uninterrupted productivity and collaboration.

Moreover, remote access capabilities provided by the RA role go beyond simple connectivity. It includes features such as **Virtual Private Network** (**VPN**) services, which enable secure and encrypted connections over public networks like the Internet. VPNs establish a protected tunnel between the remote user and the corporate network, ensuring the confidentiality and integrity of the data transmitted.

By leveraging the Remote Access role, organizations can extend their network's reach beyond physical boundaries, empowering employees to work remotely while maintaining secure and efficient access to corporate resources. This flexibility promotes productivity, enables remote collaboration, and enhances business continuity by ensuring employees can perform their tasks anywhere.

Remote access' network access technologies

In Windows Server 2022, the RA feature encompasses network access technologies enabling remote connectivity. These technologies include the following:

- Initially introduced in Windows Server 2008 R2, DirectAccess uses IPsec for secure communication between the DirectAccess client and server. It also encapsulates IPv6 traffic within IPv4, allowing internet access to the corporate intranet without needing a traditional VPN. DirectAccess provides seamless and always-on connectivity for remote users.

- **Routing and Remote Access Service** (**RRAS**) is the successor to the **Remote Access Service** (**RAS**) introduced in Windows NT and is available from Windows 2000 onwards. It combines various services to establish connections between remote locations through VPNs and dial-up connections, enabling communication between sub-networks.

- As a recursive proxy in Windows Server 2022, the Web Application Proxy leverages **Active Directory Federation Services** (**AD FS**) for user authentication. It allows

corporate users to securely access Web applications hosted on the corporate intranet from an extranet environment. That enables controlled access to Web resources while maintaining security and identity management.

Understanding Virtual Private Network

As you may know, a **Virtual Private Network** (**VPN**) is a secure means of transmitting data over the Internet. True to its name, a VPN establishes a virtual connection between two computers, creating a point-to-point link between the **Wide Area Network** (**WAN**) and the Internet. Using tunneling protocols and encryption algorithms, a VPN securely connects remote users to connect to a corporate network via the Internet. Typically, VPNs are deployed in two primary ways:

- Remote Access VPN facilitates the connection of remote users, such as telecommuters, with the server residing on their organization's private network. Through a remote access VPN, authorized individuals can establish a secure and encrypted connection to access resources within the corporate network, regardless of physical location.

- A site-to-site VPN enables organizations to establish secure connections between two separate networks over the internet. This VPN allows an organization's offices, branches, or locations to connect their respective networks securely, creating a unified and secure network environment.

A specific process must be followed to set up a VPN server in Windows Server 2022. First, the Remote Access role must be added to the server. Once this role is added, the next step is to include the necessary role services, such as DirectAccess and VPN **Remote Access Service** (**RAS**). By configuring these role services, the Windows Server 2022 can function as a VPN server, enabling secure remote access and facilitating site-to-site connectivity.

Organizations can establish a VPN server using Windows Server 2022 to provide remote users with a secure and encrypted connection to access corporate resources. In addition, site-to-site

VPNs enhance connectivity and collaboration between multiple network locations, promoting seamless data transmission and communication.

Remote support and management

Remote Assistance and **Remote Server Administration Tools** (**RSAT**) are essential features in Windows Server 2022 that facilitate remote support and management capabilities.

- Remote Assistance is a notable feature in Windows Server 2022 that allows a trusted helper to remotely access and control the desktop of an invitee, providing Assistance in troubleshooting computer-related issues. This functionality is commonly used in Help Desk scenarios, where technical support is delivered remotely. To enable the Remote Assistance feature on a Windows Server 2022, the Add Roles and Features Wizard must be utilized to configure the necessary settings.

- In addition to Remote Assistance, Windows Server 2022 also offers **Remote Server Administration Tools** (**RSAT**), which empower system administrators to manage the roles and features of remote servers running Windows Server 2022. These tools can be accessed and operated in the **Graphical User Interface** (**GUI**) and **Command-Line Interface** (**CLI**) modes. It is worth noting that RSAT is not limited to Windows Server 2022 alone; it is also available for Windows 10 and 11 client computers. To enable Remote Server Administration Tools in Windows Server 2022, the Add Roles and Features Wizard can be employed to set up the required components.

By leveraging the Remote Assistance feature, organizations can streamline troubleshooting processes by allowing remote experts to address technical issues efficiently. Similarly, the Remote Server Administration Tools enable system administrators to manage and administer remote servers effectively, enhancing overall server management capabilities. These features contribute to the seamless operation and maintenance of Windows Server 2022-based environments.

Exercise 5.7—Adding remote access role

This exercise outlines the procedure for adding a Remote Access role using Server Manager and PowerShell.

Adding remote access role using Server Manager

To begin the process of adding a Remote Access role in Windows Server 2022 using Server Manager, follow the following steps:

1. Open **Server Manager** from the Start menu and click the **Add Roles and Features** link.

2. Click on the **Next** button on the Before you begin page of the Add Roles and Features Wizard.

3. Accept the default settings on the **Select installation type** page and click **Next**.

4. Accept the default settings on the **Select destination server** page and click **Next**.

5. Choose the **Remote Access** role from the *Select Server Roles* page list. Then, click the **Next** button to continue adding the Remote Access role.

6. Accept the default settings on the *Select Features* page and click the **Next** button to proceed.

7. On the Remote Access page, click on the **Next** button.

8. Select the **role services** to install on the **Select Role Services** page for the Remote Access role. When the Add Features required for the role services you are adding window appears, click the **Add Features** button. Then, click on the **Next** button.

9. Review the options on the Confirm installation selections page and click the **Install** button.

10. The installation process for the Remote Access role will begin, as indicated by the progress bar shown in *Figure 5.15*. Once the installation is complete, click on the **Close** button to exit the Add Roles and Features Wizard, as shown in the following figure:
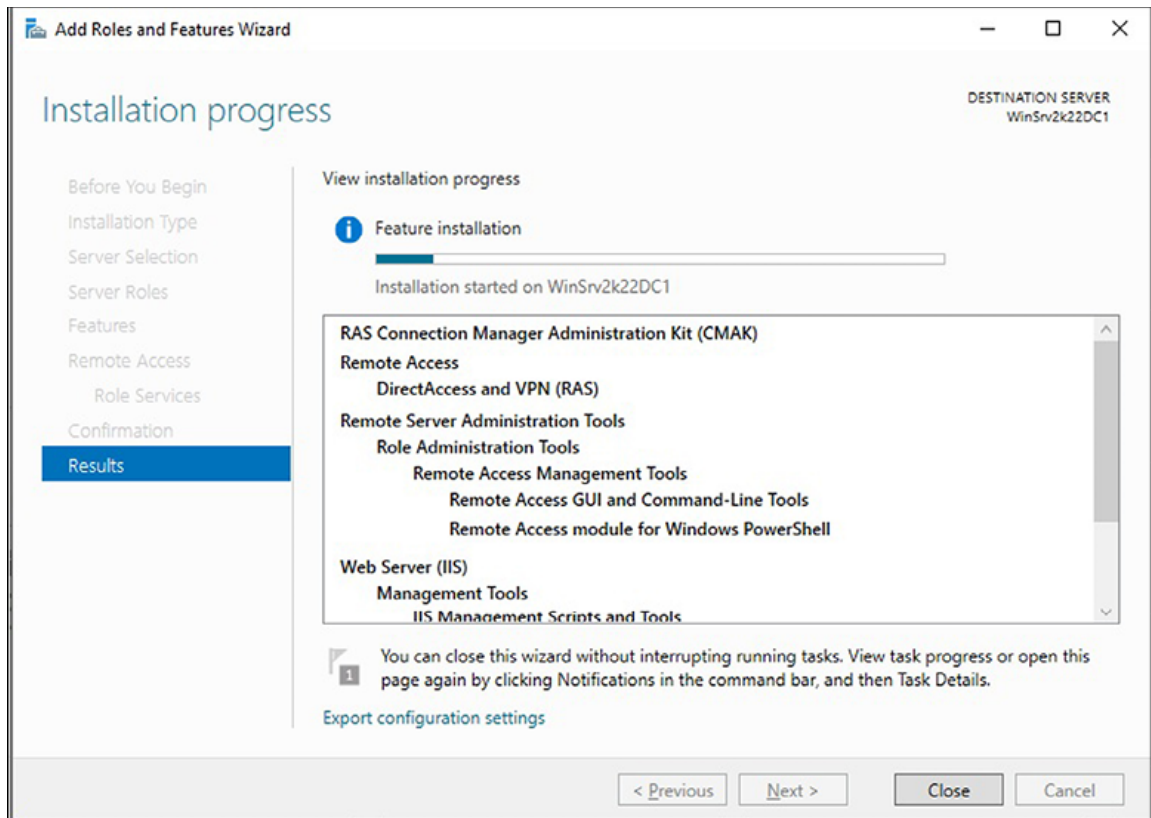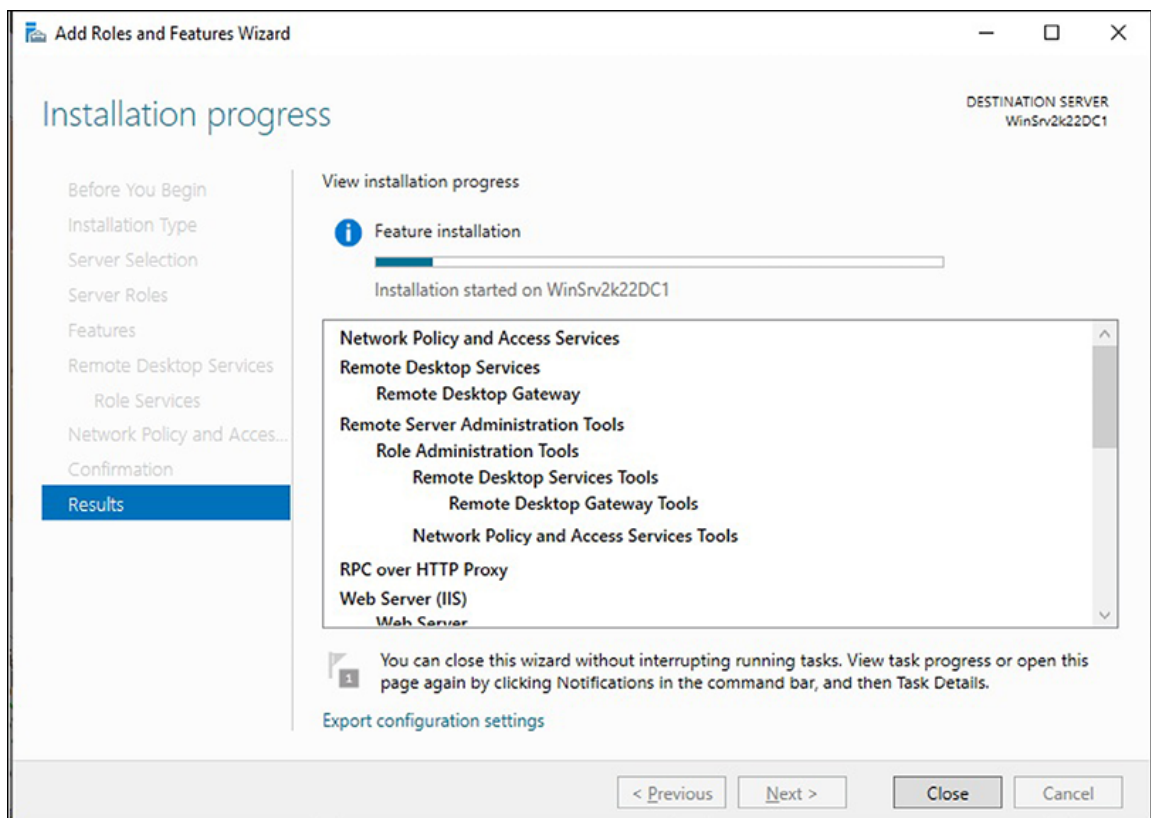
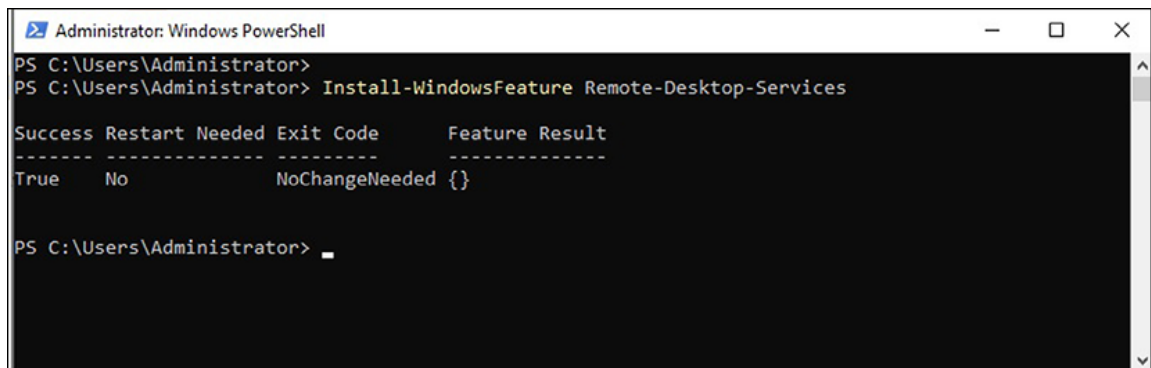***Figure 5.15:*** *Installing remote access role in Windows Server 2022 using Server Manager*
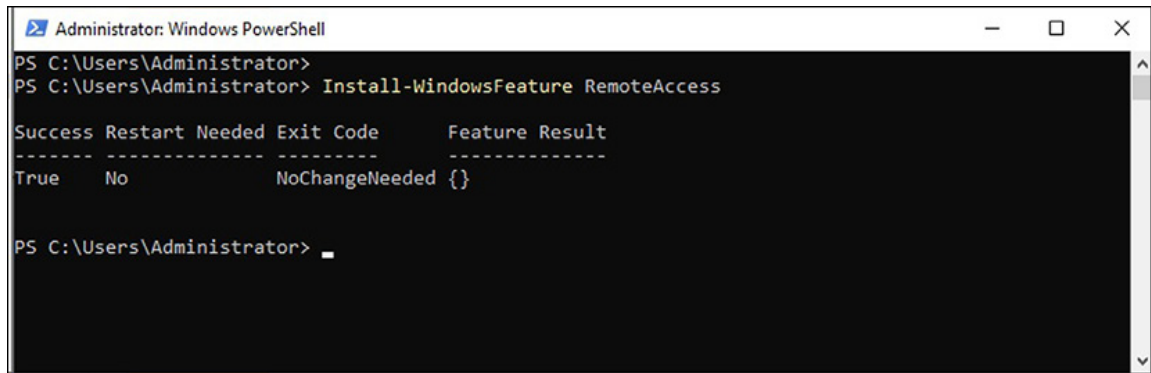
Adding remote access role using Windows PowerShell

To begin the process of adding a Remote Access role in Windows Server 2022 using Windows PowerShell, follow the following steps:

1. Launch **Windows PowerShell** by right-clicking on the Start button.

2. Within the Windows PowerShell interface, input the provided cmdlet and then press *Enter*:

   ```
   Install-WindowsFeature RemoteAccess
   ```

3. The installation of the Remote Access role will commence shortly, as depicted in *Figure 5.16*:

Figure 5.16. *Installing Remote Access role in Windows Server 2022 using Windows PowerShell*

4. To install the **Routing** role services, input the provided cmdlet and then press *Enter*:

```
Install-WindowsFeature Routing -
IncludeManagementTools
```

The need for a Remote Desktop Services role

Previously known as **Terminal Services** (**TS**) until the release of Windows Server 2008 R2, **Remote Desktop Services** (**RDS**) acquired its new name and distinct identity. This crucial role empowers organizations to establish a robust and user-friendly **Graphical User Interface** (**GUI**) that enables remote access to computers within their network, regardless of geographical location or network boundaries. Moreover, RDS goes beyond remote desktop access by offering the capability to deliver individual applications in a virtualized manner directly to users' desktops. This streamlined application delivery enhances productivity and efficiency while ensuring seamless user experiences.

By deploying an RDS server in Windows Server 2022, organizations can provide their users with a flexible and secure remote desktop infrastructure. Users gain the ability to access their workstations and applications from anywhere, enabling them to work remotely or collaborate effectively with distributed teams. The Remote Desktop Services role is a cornerstone in creating a dynamic and adaptive IT environment that caters to the evolving needs of modern organizations.

To set up an RDS server in Windows Server 2022, the first step is to add the Remote Desktop Services role to the server. This role brings a comprehensive suite of features and capabilities, including session-based virtualization, **Virtual Desktop Infrastructure** (**VDI**), and remote application delivery. Administrators can then configure and manage these services to tailor the remote desktop experience to their organization's requirements.

With Remote Desktop Services in Windows Server 2022, organizations can embrace the advantages of remote accessibility, enhanced application delivery, and improved collaboration, ultimately driving productivity and enabling efficient workflows across their network.

Various RDS role services and features

With a focus on remote support and management, Windows Server 2022 offers various role services and features. These tools enable seamless remote access, secure connections, and efficient administration, empowering organizations to enhance productivity and streamline their IT operations.

- The RDS Licensing server is crucial in managing RDS **Client Access Licenses** (**CALs**), which users and computers require to access a **Remote Desktop Session Host** (**RDSH**) server. By default, the RDS Licensing server grants two concurrent connections at no cost. If additional RDS CALs are needed, they must be purchased. To establish an RDS Licensing server in a network using Windows Server 2022, the Remote Desktop Services role must be added to the server, followed by the Remote Desktop Licensing role services.

- Another significant component of the RDS role is the **Remote Desktop Gateway** (**RDG**) server. This role service enables authorized users to connect to computers within an organization's network and over the internet using a **Remote Desktop Connection** (**RDC**) client. To set up an RDG server in an organization's network with Windows Server 2022, the Remote Desktop Services role must be

added to the server. Then, the Remote Desktop Gateway role services can be included.

- RDS uses port 3389 for data transmission. However, this port is dedicated to accessing one computer at a time. So, what happens when attempting to access multiple computers simultaneously through RDS? Sequential port numbers starting with 3390 are assigned to the additional local area network computers. Furthermore, an IP socket is used when accessing multiple computers from a remote location. An IP socket comprises an IP address and a port number, which guide the application on where to deliver the data. The syntax for an IP socket is as follows: Public_IP_address:Port_number. For example, 192.168.2.10:8080 denotes accessing a computer with the IP address 192.168.2.10 through port number 8080.

Exercise 5.8—Adding Remote Desktop Services role

This exercise outlines the procedure for adding a Remote Desktop Services role using Server Manager and PowerShell.

Adding Remote Desktop Services role using Server Manager

To begin the process of adding a Remote Desktop Services role in Windows Server 2022 using Server Manager, follow the following steps:

1. Open **Server Manager** from the Start menu and click the **Add Roles and Features** link.
2. Click on the **Next** button on the Before you begin page of the Add Roles and Features Wizard.
3. Accept the default settings on the **Select Installation Type** page and click **Next**.
4. Accept the default settings on the **Select Destination Server** page and click **Next**.
5. Choose the **Remote Desktop Services** role from the *Select Server Roles* page list. Then, click the **Next** button to continue

adding the Remote Desktop Services role.

6. Accept the default settings on the *Select Features* page and click the **Next** button to proceed.

7. On the Remote Desktop Services page, click the **Next** button.

8. Select the **role services** to install on the Select role services page for the Remote Desktop Services role. When the Add Features required for the role services you are adding window appears, click the **Add Features** button. Then click on the **Next** button.

9. Click the **Next** button on the Network Policy and Access Services page.

10. Review the options on the **Confirm installation selections** page and click the **Install** button.

11. The Remote Desktop Services role installation process will begin, as indicated by the progress bar shown in *Figure 5.17*. Once the installation is complete, click on the **Close** button to exit the Add Roles and Features Wizard:

Adding Remote Desktop Services role using Windows PowerShell

To begin the process of adding a Remote Desktop Services role in Windows Server 2022 using Windows PowerShell, follow the following steps:

1. Launch **Windows PowerShell** by right-clicking on the Start button.

2. Within the Windows PowerShell interface, input the provided cmdlet and then press *Enter*:

   `Install-WindowsFeature Remote-Desktop-Services`

3. The installation of the Remote Desktop Services role will commence shortly, as depicted in *Figure 5.18*:

Figure 5.18: Installing Remote Desktop Services role in Windows Server 2022 using Windows PowerShell

4. To install the **RDS Connection Broker** role services, input the provided cmdlet and then press *Enter*:

   `Install-WindowsFeature RDS-Connection-Broker -IncludeManagementTools`

5. To install the **RDS Gateway** role services, input the provided cmdlet and then press *Enter*:

   `Install-WindowsFeature RDS-Gateway -IncludeManagementTools`

6. To install the **RDS Licensing** role services, input the provided cmdlet and then press *Enter*:

```
Install-WindowsFeature RDS-Licensing -
IncludeManagementTools
```

Understanding Windows Server Update Services role

As the successor to **Software Update Services** (**SUS**), **Windows Server Update Services** (**WSUS**) empowers system administrators to efficiently manage the distribution of Microsoft's product updates across their organization's computer network. By leveraging WSUS, administrators can establish an infrastructure where updates, patches, and fixes are downloaded to a central server within the organization. This server then handles the approval and distribution of updates to the computers in the network.

WSUS provides administrators with comprehensive control over the update process. They can selectively approve or decline updates, schedule the installation of updates at specific times, and generate detailed reports to assess the update status of each computer. With WSUS in place, there is no longer a need for organizational computers to access Microsoft Updates directly, as WSUS is responsible for delivering the necessary updates.

In Windows Server 2022, WSUS is offered as a role that can be easily added to the server using the Server Manager tool. That allows organizations to seamlessly integrate WSUS into their server infrastructure, facilitating efficient and centralized management of Microsoft product updates.

WSUS deployment methods

WSUS is vital for updating Windows 10/11 computers within a corporate network. Organizations often employ WSUS to reserve external traffic for business-critical services. By deploying WSUS, end-user devices in the network receive updates directly from the WSUS server, which downloads the updates from the Microsoft Windows Update server.

To initiate the deployment of WSUS, crucial decisions need to be made. These include selecting the WSUS deployment scenario, determining the network topology, and understanding the system requirements. Hardware and database software requirements are driven by the number of client computers requiring updates. Before adding the WSUS server role, verifying that the server meets the specified system requirements is essential.

- A fundamental WSUS deployment involves a server within the corporate firewall, serving client computers on a private intranet. The WSUS server connects to Microsoft Updates for downloading updates, a process known as synchronization. During synchronization, WSUS identifies any newly available updates since the last synchronization. For the initial synchronization, all updates are made accessible for download. The WSUS server typically uses port 80 for HTTP protocol and port 443 for HTTPS protocol to communicate with Microsoft Updates. If a corporate firewall exists between the network and the internet, these ports must be opened to enable direct communication with Microsoft updates.

- Alternatively, WSUS can be deployed with multiple servers synchronized within the organization's intranet. One server, the upstream server, is exposed to the internet and downloads updates from Microsoft Update. The remaining servers called downstream servers, synchronize with the upstream server. Sometimes, servers may be distributed across geographically dispersed networks to ensure optimal connectivity to all client computers.

WSUS connection modes

WSUS servers offer two connection modes: autonomous mode and replica mode. It is advisable to deploy a WSUS solution that leverages both connection modes. Let us explore the following modes further:

- Autonomous mode, also known as distributed administration, is the default installation option for WSUS. In this mode, an upstream WSUS server shares updates

with downstream servers during synchronization. Downstream WSUS servers are managed independently and do not receive updated approval status or computer group information from the upstream server. With the distributed management model, each WSUS server administrator has control over selecting update languages, creating computer groups, assigning computers to groups, testing and approving updates, and ensuring the installation of the appropriate updates in the designated computer groups.

- On the other hand, replica mode, also called centralized administration, involves an upstream WSUS server that shares updates, approval status, and computer groups with downstream servers. Replica servers inherit update approvals and are not administered separately from the upstream WSUS server. This mode provides a centralized administration approach and allows consistent update management across all replica servers.

By combining autonomous mode and replica mode in your WSUS deployment, you can benefit from the flexibility and distributed management capabilities of autonomous mode while maintaining centralized control and synchronization with replica mode.

Exercise 5.9—Adding Windows Server Update Services role
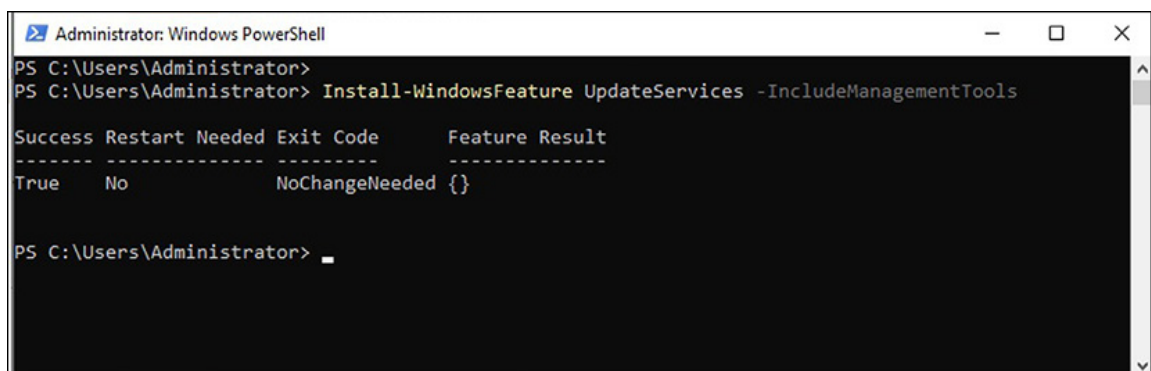
This exercise outlines the procedure for adding a Windows Server Update Services role using Server Manager and PowerShell.

Adding Windows Server update services role using Server Manager

To begin the process of adding a Remote Desktop Services role in Windows Server 2022, using Server Manager, follow these steps:

1. Open **Server Manager** from the Start menu and click the Add Roles and Features link.

2. Click on the **Next** button on the **Before you begin** page of the Add Roles and Features Wizard.

3. Accept the default settings on the **Select Installation Type** page and click **Next**.

4. Accept the default settings on the **Select Destination Server** page and click **Next**.

5. Choose the **Windows Server Update Services** role from the Select Server Roles page list. When the Add Features required for the Windows Server Update Services window appears, click the **Add Features** button. Then, click the **Next** button to continue adding the Windows Server Update Services role.

6. Accept the default settings on the **Select Features** page and click the **Next** button to proceed.

7. Click the **Next** button on the **Windows Server Update Services** page.

8. Select the **role services** to install on the Select role services page for the Windows Server Update Services role. Then click on the **Next** button.

9. Enter the **local or remote path** on the page and click the **Next** button.

10. Review the options on the Confirm installation selections page and click the **Install** button.

11. The installation of the Windows Server Update Services role will begin, as indicated by the progress bar shown in *Figure 5.19*. Once the installation is complete, click on the **Close** button to exit the Add Roles and Features Wizard, as shown in the following figure:

Figure 5.19: *Installing Windows Server Update Services role in Windows Server 2022 using Server Manager*
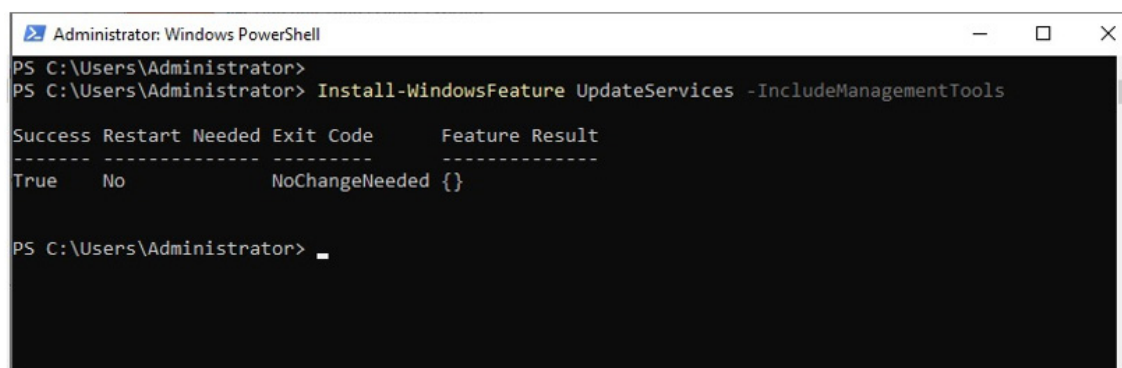
Adding Windows Server Update Services role using Windows PowerShell

To begin the process of adding a Windows Server Update Services role in Windows Server 2022 using Windows PowerShell, follow the following steps:

1. Launch **Windows PowerShell** by performing a right-click on the Start button.

2. Within the Windows PowerShell interface, input the provided cmdlet and then press *Enter*:

   ```
   Install-WindowsFeature UpdateServices -
   IncludeManagementTools
   ```

3. The Windows Server Update Services role installation will commence shortly, as depicted in *Figure 5.20*:

Figure 5.20: *Installing Windows Server Update Services role in Windows Server 2022 using Windows PowerShell*
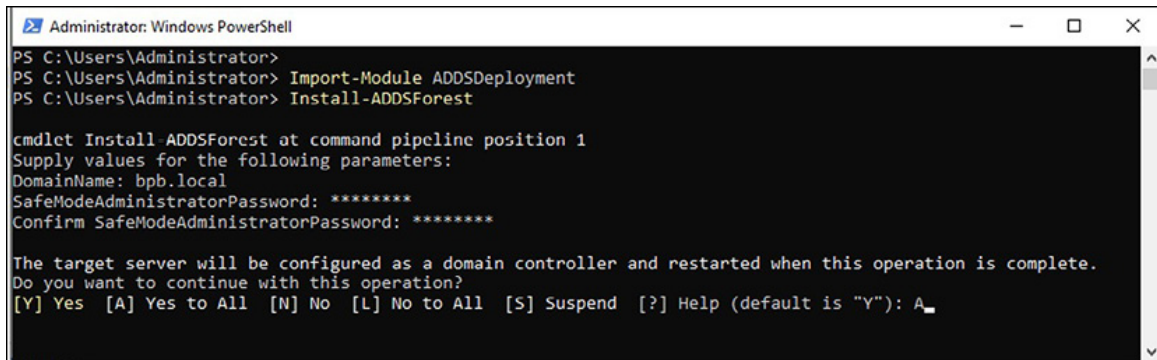
Until now, we have successfully included most of the roles offered by Windows Server 2022. The approach involved using PowerShell to add each role. At this stage, there is a need to examine all the roles that have been added. It is worth noting that the `Get-WindowsFeature` cmdlet lists all the installed roles on the server. Furthermore, suppose there are new roles the system administrator wishes to add to the server. In that case, the `Get-WindowsFeature` cmdlet will provide the installation name (found in the Name column), which you should use when executing the `Install-WindowsFeature <name of the service>` cmdlet.

Conclusion

In this chapter, you have learned about installing roles in Windows Server 2022 using the Add Roles and Features Wizard available in the Server Manager and PowerShell. You have gained comprehensive guidance on the steps to follow and the additional features required for each role to function correctly. The chapter covered roles such as AD DS, DHCP, Hyper-V, IIS, PDS, Remote Access, RDS, and WSUS and provided hands-on exercises for readers to follow. In addition, you have learned about each role's purpose and how to configure them to meet your organization's needs. With this knowledge, you can efficiently install roles and customize your Windows Server 2022 to meet your organization's requirements.

In the upcoming chapter, you will learn about configuring roles and setting up services in Windows Server 2022 using both GUI and Windows PowerShell.

Questions

1. What is AD DS?
2. What are DNS zones?
3. Explain DORA in DHCP.
4. What is Hyper-V?
5. What is IIS?
6. Name the PDS role services.
7. List network access technologies of RA.
8. What is needed to set up RDS?
9. Which are WSUS connection modes?

Join our book's Discord space
Join the book's Discord Workspace for Latest updates, Offers, Tech happenings around the world, New Release and Sessions with the Authors:

https://discord.bpbonline.com

CHAPTER 6
Service Management with GUI and PowerShell

Introduction

This chapter provides a comprehensive step-by-step installation guide on configuring client/server network services in Windows Server 2022 using Windows PowerShell cmdlets. Readers will learn how to leverage the power of Windows PowerShell to configure various network services in Windows Server 2022 efficiently. The topics covered include promoting a server to a **Domain Controller (DC)**, adding an A record in a DNS server, configuring a DHCP server, configuring a virtual machine, establishing a Web server, setting up a print server, configuring Remote Desktop users, and setting up a WSUS server. By following the detailed instructions and using the provided cmdlets, readers will gain the necessary skills to successfully configure and manage these essential network services in Windows Server 2022.

Structure

In this chapter, we will cover the following topics:

- Promoting server to a domain controller
- Adding an A record in the DNS server

- Configuring a DHCP server

- Configuring a virtual machine

- Configuring a website

- Configuring the print server

- Configuring Remote Desktop users

- Configuring the WSUS server

Objectives

This chapter provides a comprehensive guide on configuring client/server network services in Windows Server 2022 using Windows PowerShell. Readers will learn to efficiently configure various network services, including DHCP, AD DS, virtual machines, Web servers, DNS, print servers, WDS, VPN, Remote Desktop users, and WSUS. By following the step-by-step instructions and using the provided PowerShell cmdlets, readers will gain the necessary skills to successfully manage these network services in Windows Server 2022 successfully.

Promoting the server to a domain controller

Promoting a server to a DC is crucial in establishing a centralized authentication, authorization, and resource management system within a Windows Server environment. Organizations can enjoy the advantages of centralized user account management, security policies, and access controls by promoting a server to a domain controller. That results in a unified security framework throughout the network, enabling users to log in using a single set of credentials. The domain controller hosts the **Active Directory** database, facilitating efficient user information management, group policies, and directory-based services like DNS and LDAP. Moreover, promoting multiple servers to domain controllers ensures redundancy and fault tolerance, guaranteeing the availability of authentication and directory services. This approach supports scalability and accommodates expansion by distributing the workload. Trust relationships between domains can also be established and administered, enabling collaboration

and resource sharing. In summary, promoting a server to a domain controller provides a resilient and scalable infrastructure for user authentication, resource management, and centralized administration.

Having initiated the installation of AD DS on the server in *Chapter 5, Installing roles in Windows Server 2022 Using Server Manager and PowerShell*, we are now ready to progress toward promoting the server to a domain DC. It is the opportune moment to transition into this next phase. Therefore, let us embark on this exciting journey as we embrace the challenges and rewards of promoting the server to a domain controller.

Exercise 6.1—Configuring domain controller

This exercise outlines the procedure for configuring the **Domain Controller** (**DC**) using Server Manager and PowerShell.

Configuring domain controller using Server Manager

To begin the process of configuring DC in Windows Server 2022 using Server Manager, follow the following steps:

1. Open **Server Manager** from the **Start** menu.
2. Click on the **Notifications** icon, then select **Promote this server to become a domain controller**, as shown in *Figure 6.1:*
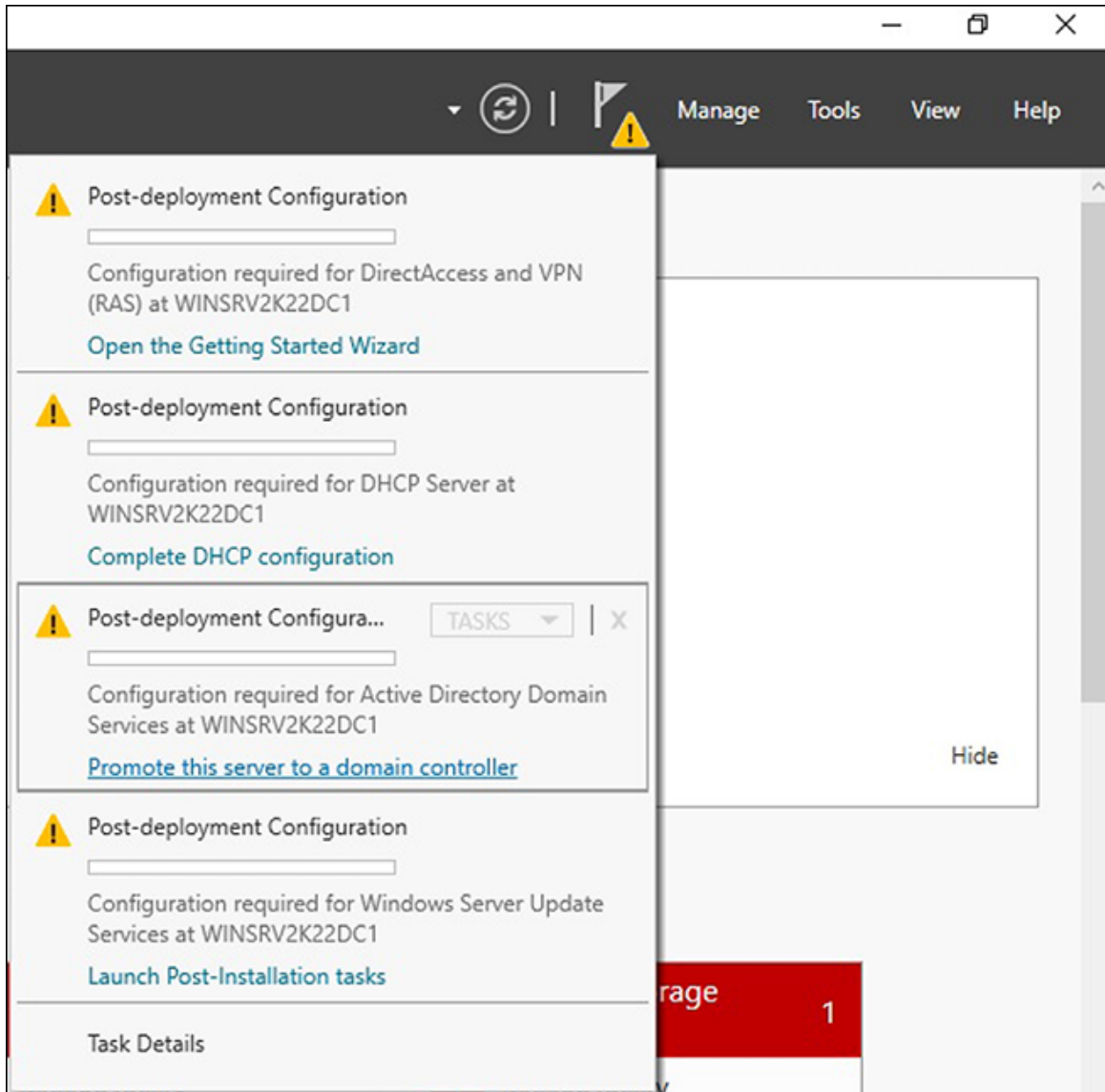
Figure 6.1: *Initiating the configuration of the domain controller in Windows Server 2022 using Server Manager*

3. On the **Deployment configuration** page, choose **Add a new forest**. Enter **bpb.local** as the **Root domain name**. Click on the **Next** button to proceed.

4. Select the functional level for the new forest and root domain on the **Domain Controller Options** page. Enter the **Directory Services Restore Mode (DSRM)** password. Click on the **Next** button.

5. Accept the default settings on the **DNS options** page. Click on the **Next** button to continue.

6. Accept the default settings on the **Additional Options** page. Click on the **Next** button to continue.

7. On the **Paths** page, keep the default settings and click on the **Next** button.

8. Review the settings on the **Review Options** page, as shown in *Figure 6.2*, and click on **Next**:
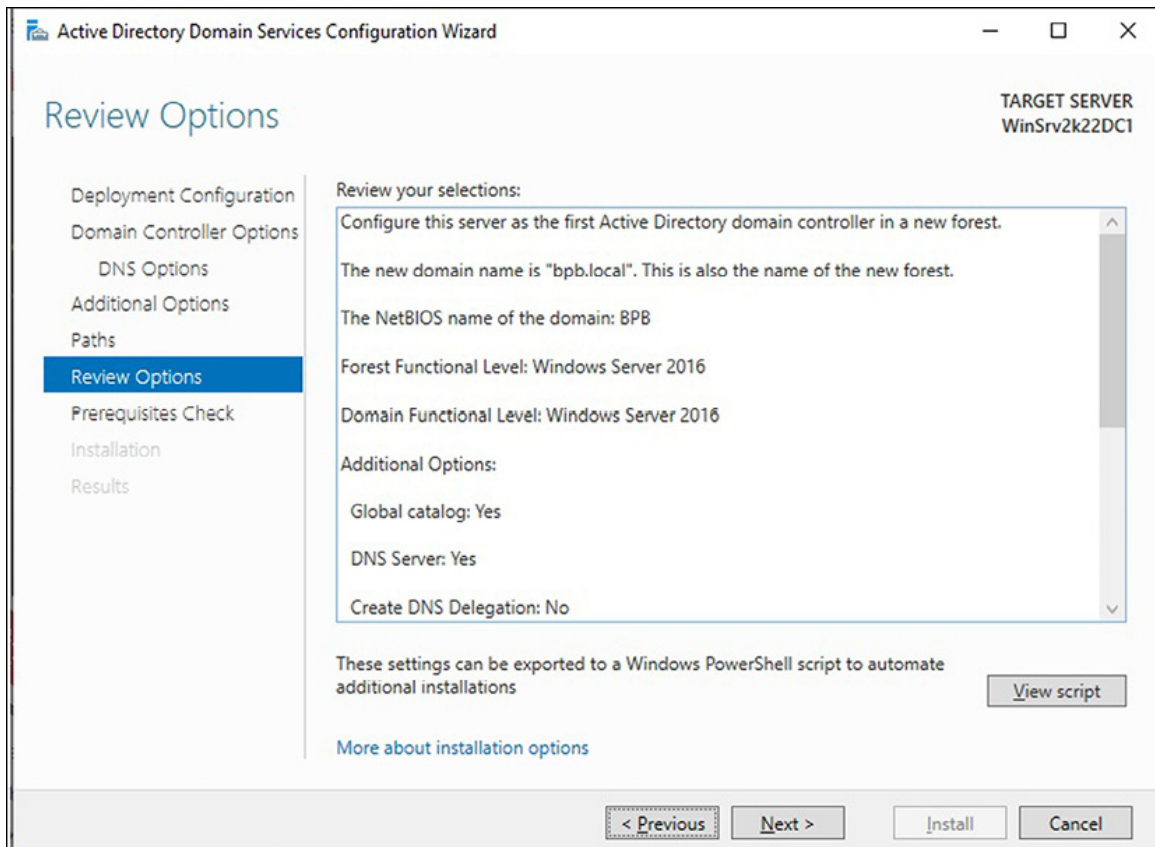
Figure 6.2: *Reviewing the settings of configuring domain controller in Windows Server 2022 using Server Manager*

9. On the **Prerequisites Check** page, validate the prerequisites. Then, click the **Install** button, as shown in *Figure 6.3*, to proceed with the DC configuration. Take a look at the following figure:
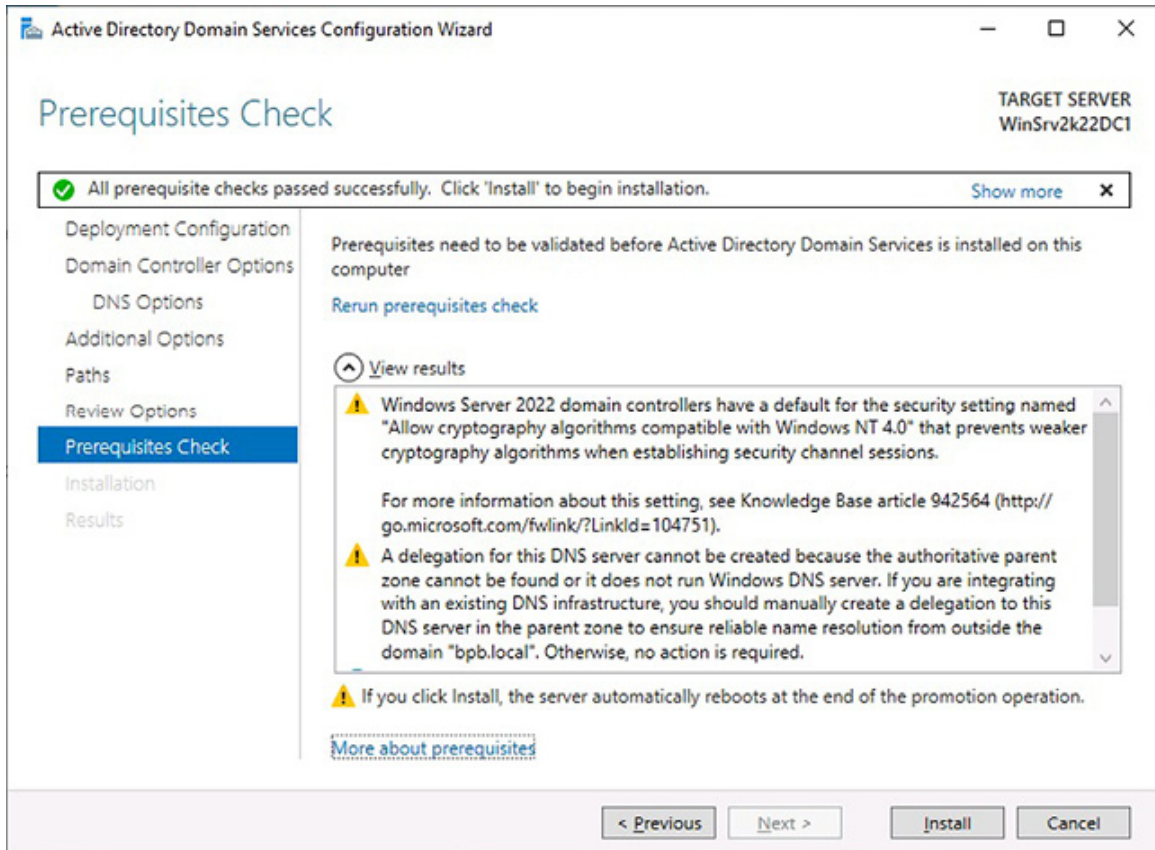
Figure 6.3: *Validation of prerequisites in Windows Server 2022 using Server Manager*

10. On the **Installation** page, the **DC** configuration occurs, *Figure 6.4*. This process restarts the server automatically. Upon restart, the server boots up with an installed **Active Directory Domain Services (AD DS)** and a configured **domain controller (DC)**. Take a look at the following figure:
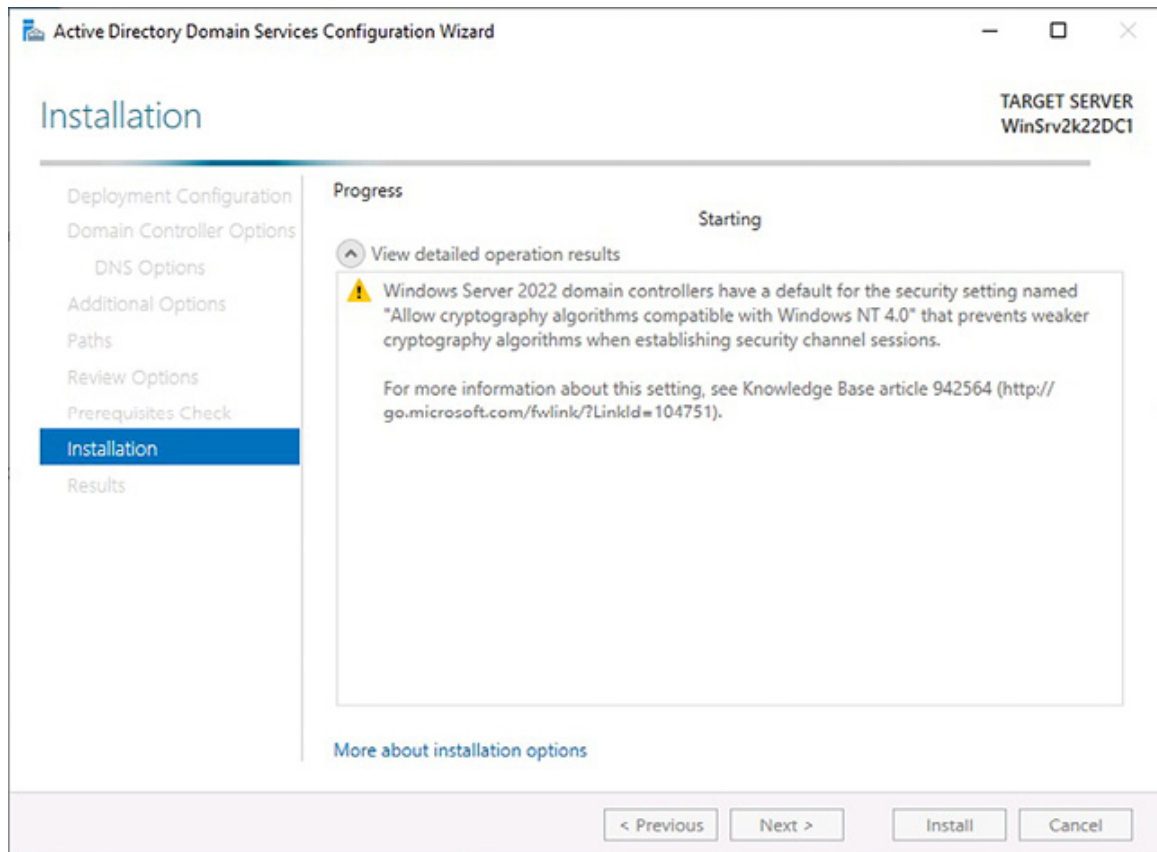
Figure 6.4: *Configuring domain controller in Windows Server 2022 using Server Manager*

Configuring domain controller using Windows PowerShell

To begin the process of configuring DC in Windows Server 2022 using Windows PowerShell, follow the following steps:

1. Launch **Windows PowerShell (Admin)** by right-clicking the **Start** button.

2. Within the **Windows PowerShell** interface, input the provided cmdlets and then press *Enter*:

   Import-Module ADDSDeployment

   Install-ADDSForest

3. Provide the name for the **domain** and press *Enter*.

4. Provide the **safe mode administrator** password and press *Enter*.

5. Confirm the **safe mode administrator** password and press *Enter*.

6. Type the letter `A` for All, and press `Enter`. The **DC** configuration occurs. This process restarts the server automatically. Upon restart, the server boots up with an installed `Active Directory Domain Services (AD DS)` and a configured *DC,* as shown in *Figure 6.5:*

Figure 6.5: Configuring domain controller (DC) in Windows Server 2022 using Windows PowerShell

Adding an A Record in the DNS manager

The A Record, or the Address record, is vital to the **Domain Name System (DNS)** infrastructure. It aims to link a hostname or subdomain with its corresponding IPv4 address. A Records are necessary because domain names in human-readable format, for example, example.com, are more user-friendly than numerical IP addresses such as 192.168.0.1. By associating a domain name with its respective IP address, A Records enable computers and devices to locate and connect to specific servers or resources on the internet. When a user enters a domain name or tries to access a particular server, the DNS system translates the domain name into its associated IP address. The A record is critical in this process by supplying the necessary IP address information to establish the connection.

Exercise 6.2—Configuring an A Record in the DNS server

This exercise outlines configuring an A Record in a DNS server using a DNS manager and PowerShell.

Configuring an A record using the DNS manager

To begin the process of configuring an A Record in Windows Server 2022 using DNS Manager, follow the following steps:

1. Open the **DNS Manager** console by clicking on the **Start** button and then clicking on **Windows Administrative Tools**. Then, double-click on **DNS**. As shown in the following figure:
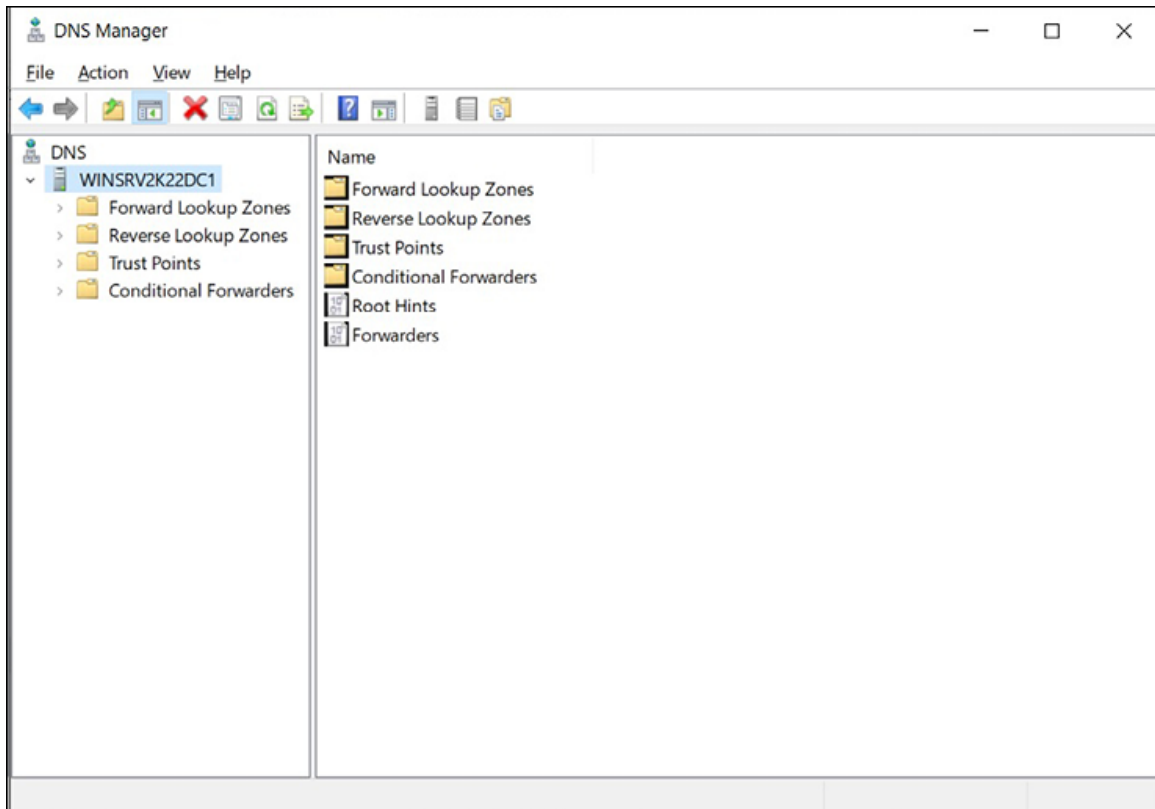
Figure 6.6: DNS Manager console in Windows Server 2022

2. Expand the **server** by selecting it from the tree on the console's left side.

3. Expand the **Forward Lookup Zone** by selecting it from the tree on the left side of the console.

4. Click **bpb.local**, then choose the **New Alias (CNAME)** option from the **Action** menu.

5. Enter a **Name** and **an IP address** for the new host, and then click on **Add host,** as shown in *Figure 6.7:*

Figure 6.7: Adding an A record of a new host in Windows Server 2022

6. A dialog box states that the **host record has been created successfully**. Click on **OK** and then click on the **Done** button to close the **New Host** window. Also, you will notice that an **A record** you added recently is listed in the right panel of the **DNS Manager** console.

Configuring an A Record using Windows PowerShell
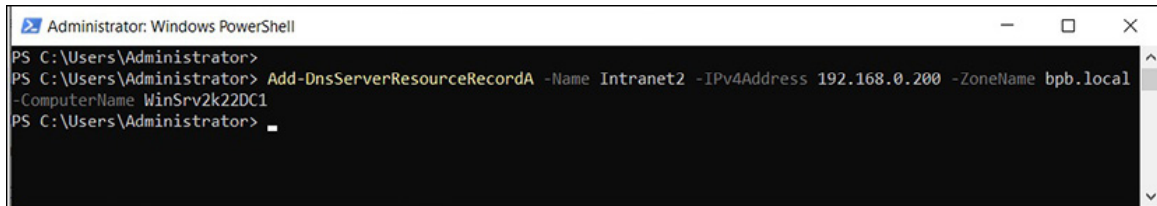
To begin the process of configuring an A record in Windows Server 2022 using Windows PowerShell, follow these steps:

1. Launch **Windows PowerShell (Admin)** by right-clicking the **Start** button.

2. Within the **Windows PowerShell** interface, input the provided cmdlet and then press *Enter*:

   Add-DnsServerResourceRecordA -Name Intranet2 -
   IPv4Address 192.168.0.200 -ZoneName bpb.local -

```
ComputerName WinSrv2k22DC1
```

3. The entered cmdlet will get executed, as shown in *Figure 6.8*:

Figure 6.8: *Configuring an A record in Windows Server 2022 using Windows PowerShell*

Configuring a DHCP server

Configuring a DHCP server in Windows Server 2022 presents several compelling reasons for implementation as follows:

- It simplifies the management of IP addresses by automating the assignment process for client devices on the network. That eliminates the need for manual address assignment, reducing administrative workload and minimizing the risk of address conflicts.

- DHCP facilitates efficient network scaling by dynamically allocating IP addresses to new devices joining the network, eliminating the labor-intensive task of manual assignment. Moreover, configuring a DHCP server ensures consistent network configuration across all connected devices by distributing additional network parameters like default gateways and DNS servers. This standardized network environment simplifies troubleshooting and promotes operational efficiency.

- DHCP servers enable effective management of the IP address pool, allowing specific address ranges to be allocated for different purposes or departments within an organization. That promotes resource efficiency and facilitates network segmentation. Another notable advantage is the time and cost savings associated with DHCP, as manual IP address assignments are eliminated,

enabling IT administrators to focus on other critical tasks and boosting productivity.

- DHCP enhances network security by offering options to configure secure DNS server addresses and enabling network access control by assigning specific IP addresses to known devices. In summary, the configuration of a DHCP server in Windows Server 2022 brings centralized IP address management, network scalability, configuration consistency, cost savings, and improved network security, making it an indispensable component for efficient and effective network administration.

Exercise 6.3—Configuring a DHCP Scope

This exercise outlines the procedure for configuring a DHCP Scope using a DHCP console and PowerShell.

Configuring a DHCP scope using a DHCP console

To begin the process of configuring a DHCP scope in Windows Server 2022 using the DHCP console, follow the following steps:

1. Open **Server Manager** from the **Start** menu.
2. Click on the **Notifications** icon, then select **Complete DHCP configuration**, as shown in *Figure 6.9:*
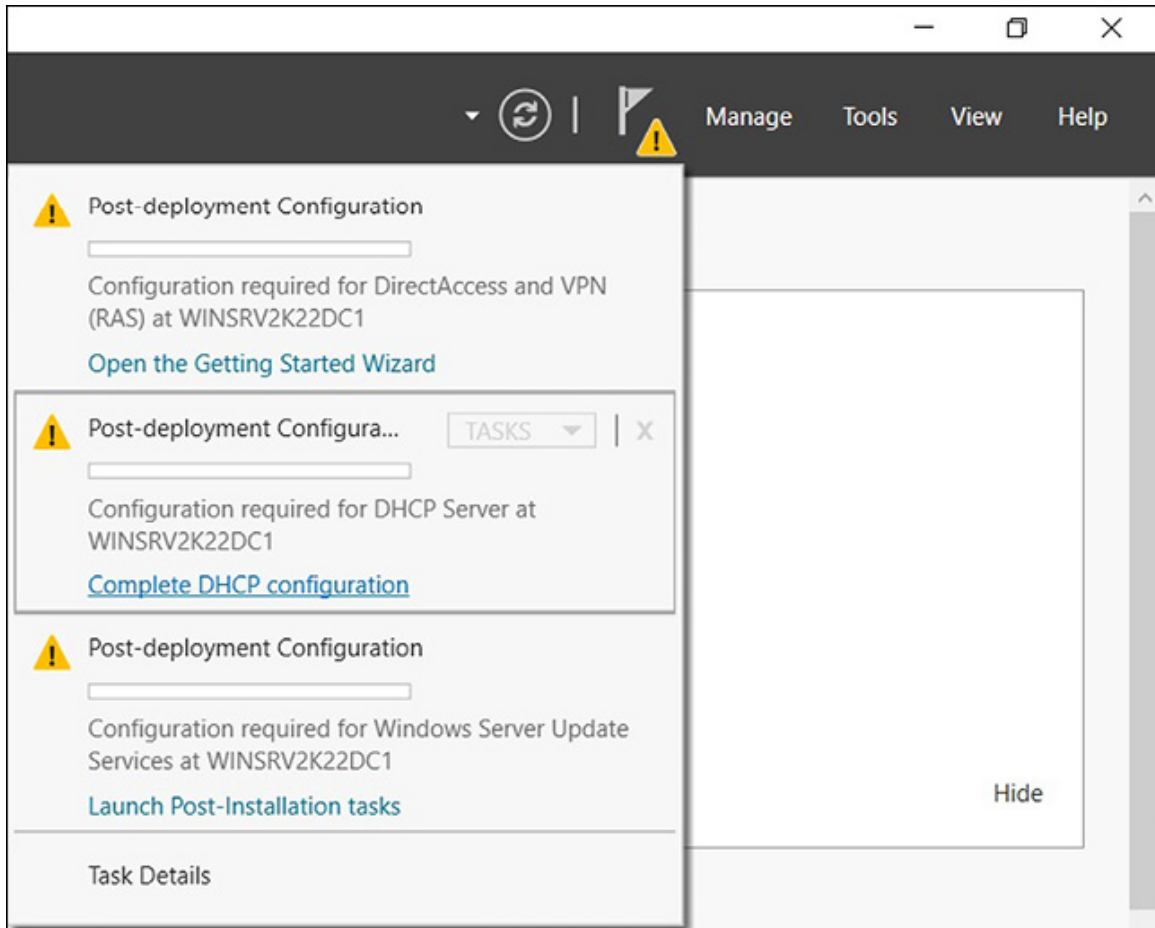
Figure 6.9: *Initiating the configuration of the DHCP Server in Windows Server 2022 using Server Manager*

3. Accept the **Description** page's default settings on the and click **Next**.

4. On the **Authorization** page, specify the credentials to authorize *DHCP Server* and click the **Commit** button.

5. On the **Summary** page, verify that **Creating security groups** and **Authorizing DHCP server** have **Done** status. Then, click the **Close** button. Take a look at the following figure:
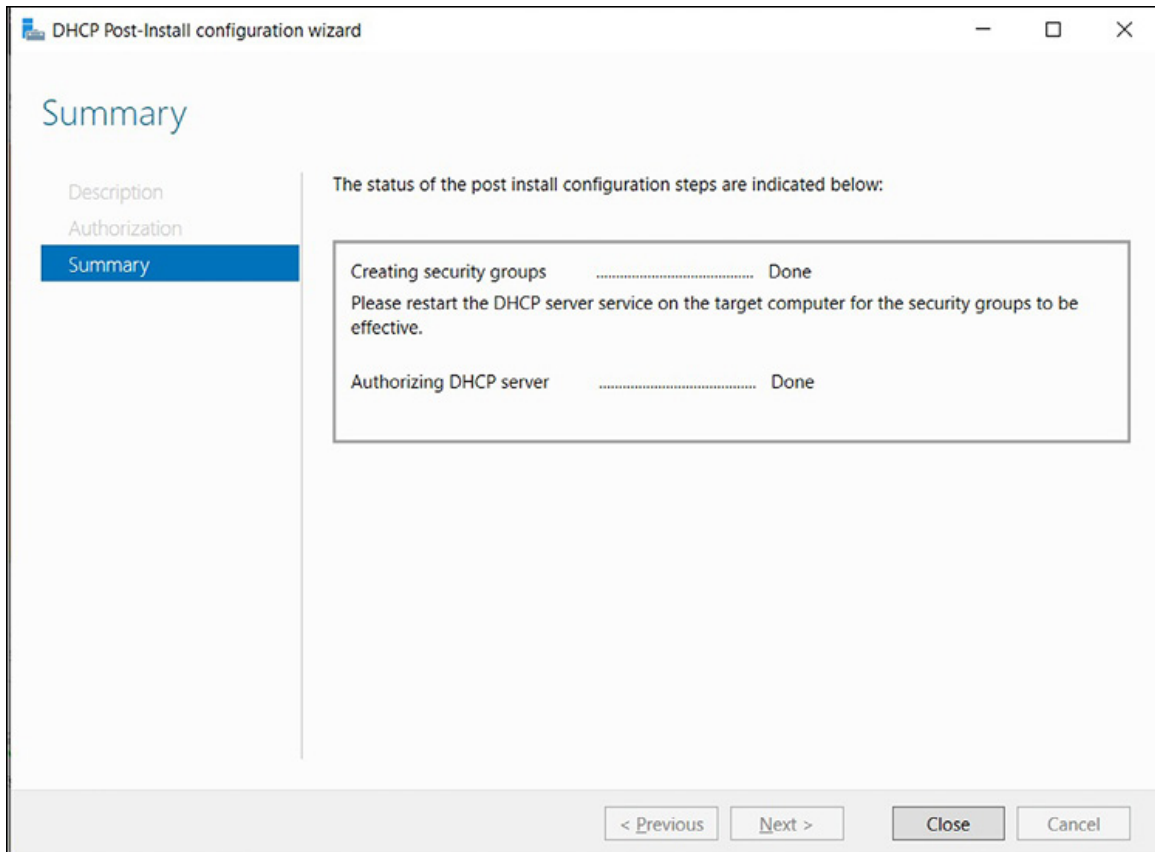
Figure 6.10: Authorizing DHCP Server in Windows Server 2022 using Server Manager

6. Open the **DHCP Manager** console by clicking on the **Start** button and then clicking on **Windows Administrative Tools**. Then, double-click on **DHCP**.

7. Expand the **DHCP server** from the tree on the left side of the window, as shown in *Figure 6.11*:
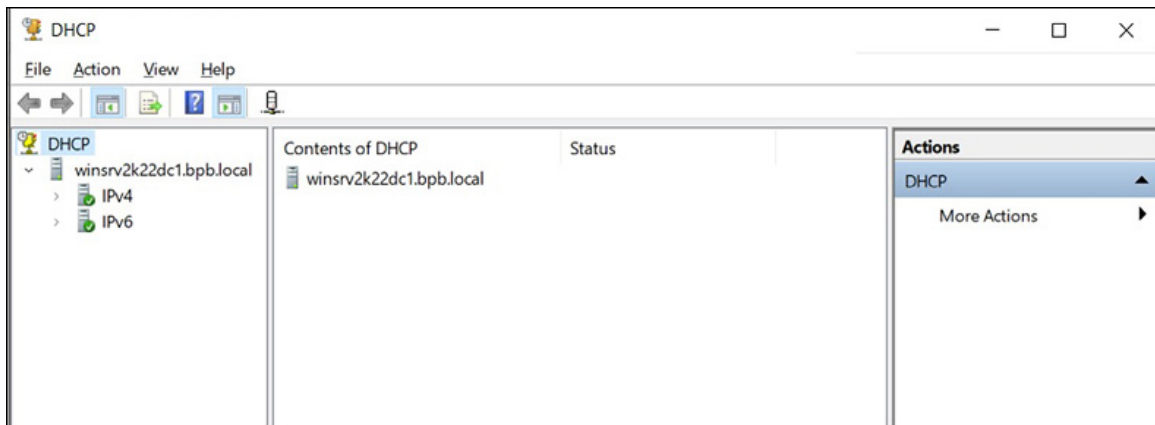
Figure 6.11: DHCP Manager in Windows Server 2022

8. Select the **IPv4 option**.

9. From the **More Actions** menu on the right side of the window, click on **New Scope**.

10. Click the **Next** button on the **Welcome to the New Scope Wizard**.

11. On the **Scope Name** page, provide the name and description for this scope, then click **Next**.

12. On the **IP address range** page, define the address range for the scope and specify the **Subnet mask**, as shown in *Figure 6.12*:
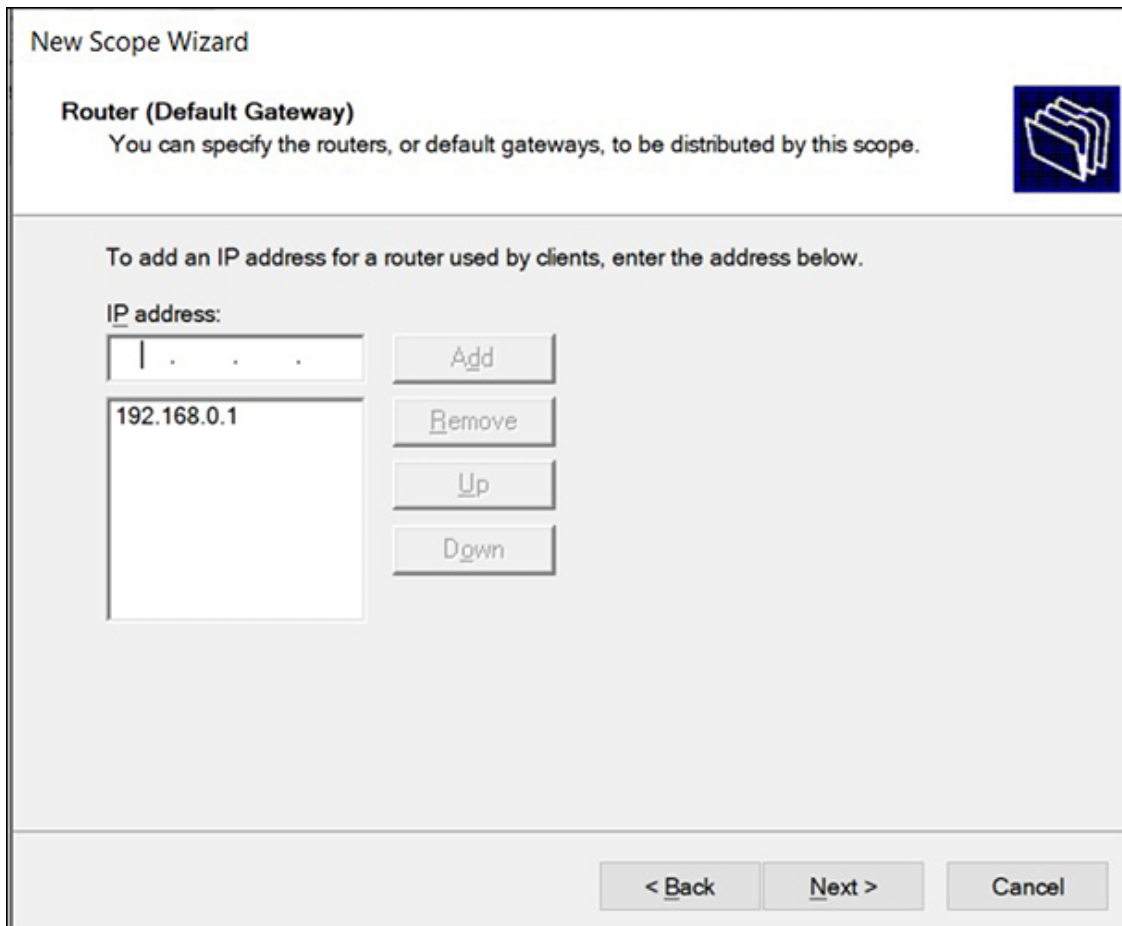
Figure 6.12: *Specifying IP Address range in Windows Server 2022 using DHCP Manager*

13. On the **Add exclusions and delay** page, if needed, **exclude** specific IP addresses from the defined range, if needed.

14. On the **Lease duration** page, specify the **lease duration** for the assigned IP addresses and click **Next**.

15. On the **Configure DHCP options** page, accept defaults and proceed by clicking **Next**.

16. On the *Router* **(default gateway)** page, add the **IP address** of your default gateway and click on **Next**, as shown in the following figure:

Figure 6.13: Specifying default gateway in Windows Server 2022 using DHCP Manager

17. On the **Domain name and DNS servers** page, specify your network's **parent domain and DNS server(s),** as shown in *Figure 6.14*:

Figure 6.14: *Specifying domain name and DNS server in Windows Server 2022 using DHCP Manager*

18. On the **WINS servers** page, if applicable, enter the information for the **WINS** server on your network.

19. On the **Activate scope** page, confirm that you want to **activate this scope** now and click **Next**.

20. Click the **Finish** button to close the **Completing the New Scope Wizard**.

21. Your scope is now marked as ****Active**** in the **DHCP Manager**, as shown in *Figure 6.15:*
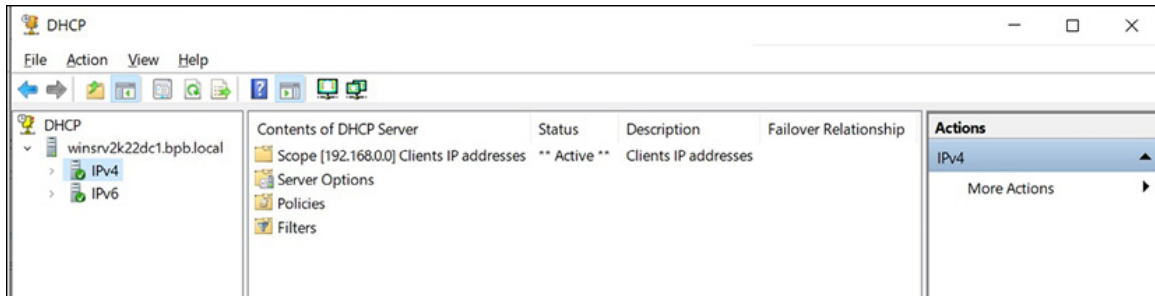
Figure 6.15: *An **Active** IPv4 scope in Windows Server 2022 using DHCP Manager*
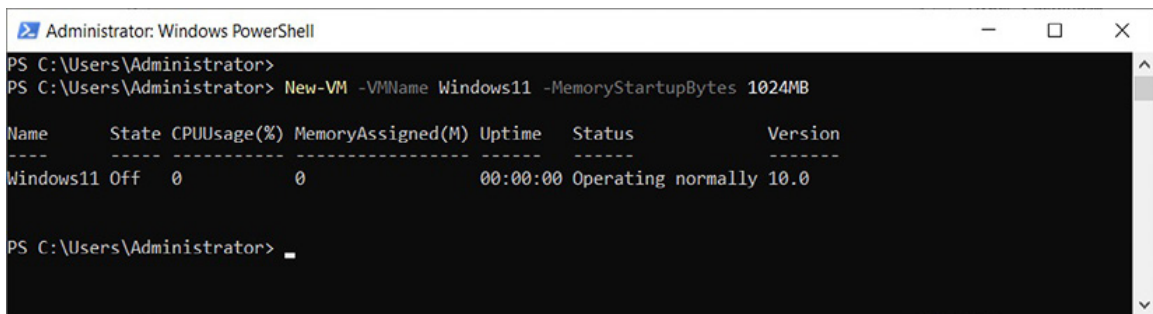
Configuring a DHCP scope using Windows PowerShell

To begin the process of configuring a DHCP Scope in Windows Server 2022 using Windows PowerShell, follow the following steps:

1. Launch **Windows PowerShell** by right-clicking on the **Start** button.

2. Within the **Windows PowerShell** interface, to authorize your DHCP Server in **Active Directory** (**AD**), input the provided cmdlet and then press *Enter*:

   Add-DhcpServerInDC -DNSName bpb.local

3. To create a DHCP Scope, input the provided cmdlet, and then press *Enter*:

   Add-DhcpServerv4Scope -Name "Clients IP addresses" -StartRange 192.168.0.2 -EndRange 192.168.0.99 -SubnetMask 255.255.255.0 -Description "Clients IP addresses" -State Active

4. The entered cmdlet will get executed, as shown in *Figure 6.16*:
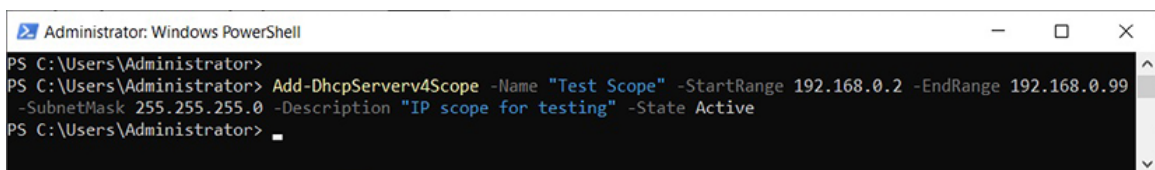
Figure 6.16: *Configuring an IPv4 scope in Windows Server 2022 using Windows PowerShell*

5. To exclude a range within an IP scope, input the provided cmdlet and then press *Enter*:

```
Add-Dhcpserverv4ExclusionRange -ComputerName
WinSrv2k22DC1 -ScopeId 192.168.0.0 -StartRange
192.168.0.10 -EndRange 192.168.0.20
```

6. To view the newly added scope, input the provided cmdlet and then press *Enter*:

```
Get-DHCPServerv4Scope
```

Configuring a virtual machine

Configuring a **Virtual Machine** (**VM**) using Hyper-V in Windows Server 2022 provides numerous advantages. Virtual machines offer high isolation, enabling the independent operation of multiple operating systems and applications within their respective virtual environments. This isolation ensures that issues or reboots in one virtual machine do not impact others. Hyper-V facilitates efficient resource management by allocating CPU cores, memory, storage, and network bandwidth to each virtual machine based on its specific requirements, optimizing performance and scalability, and benefits as follows:

- Virtualization supports server consolidation, reducing hardware costs, power consumption, and data center space needs. It simplifies management and maintenance through centralized control of multiple virtual machines. Virtual machines also create a secure and isolated testing and development environment, which can capture snapshots and quickly revert to previous states. Hyper-V includes replication and high availability features, ensuring disaster recovery and uninterrupted business operations.

- Virtual machines are highly scalable and flexible, swiftly adapting to change demands by adjusting resource allocations and migrating between hosts. With comprehensive management tools like PowerShell integration and performance monitoring, Hyper-V streamlines administration tasks and enhances overall

efficiency. Configuring virtual machines with Hyper-V in Windows Server 2022 optimizes resource utilization, improves security and isolation, simplifies management procedures, and provides robust availability and disaster recovery capabilities for your IT infrastructure.

Exercise 6.4—Configuring a virtual machine

This exercise outlines the procedure for configuring a **Virtual Machine** (**VM**) in Windows Server 2022 using Hyper-V Manager and PowerShell.

Configuring a virtual machine using Hyper-V manager

To begin the process of configuring a **Virtual Machine** (**VM**) in Windows Server 2022, using Hyper-V Manager, follow the following steps:

1. Open the **Hyper-V Manager** by clicking on the **Start** button and then clicking on **Windows Administrative Tools**. Then, double-click on **Hyper-V Manager**. Take a look at the following figure:
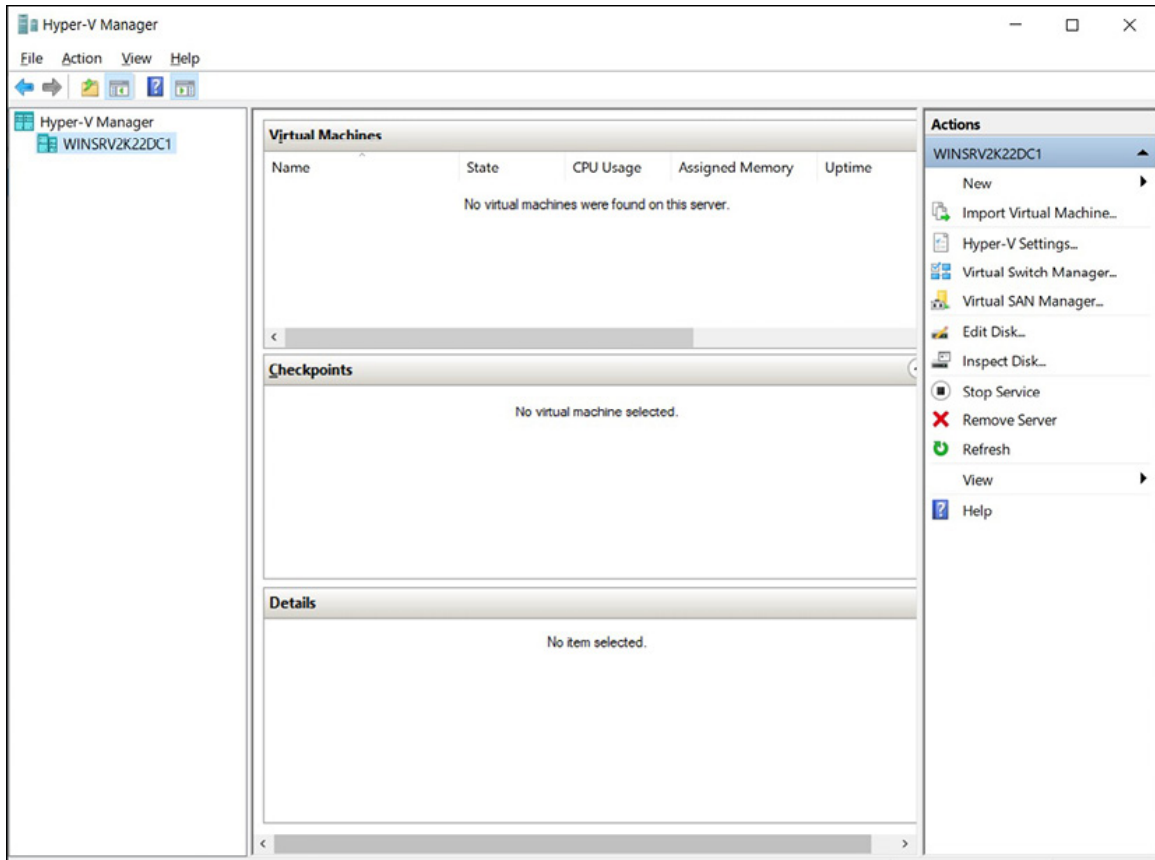
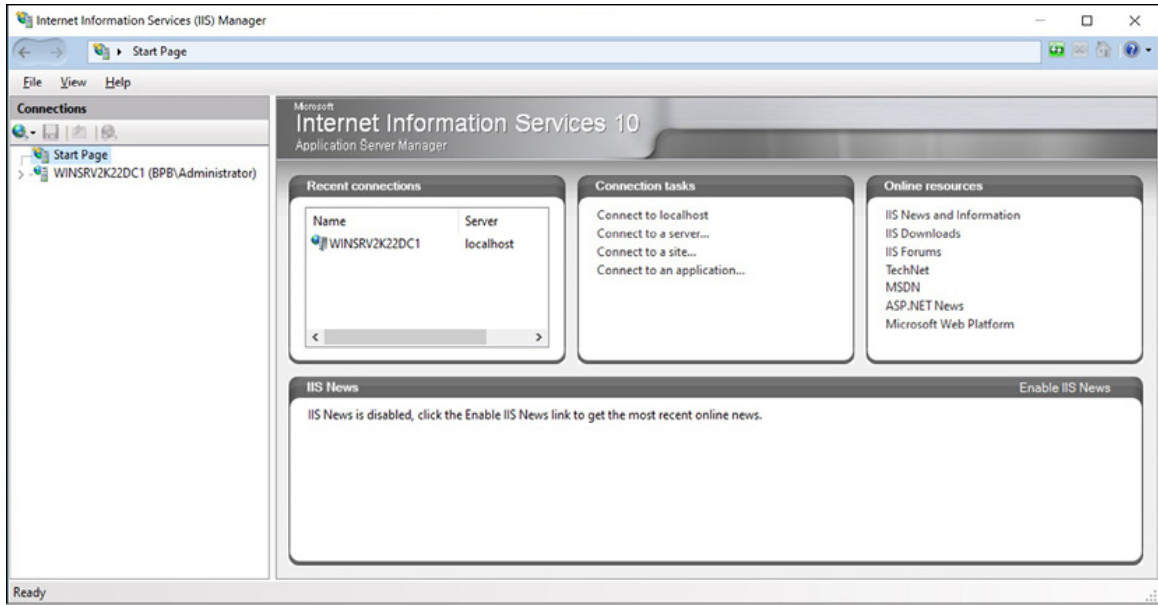***Figure 6.17:*** *Hyper-V Manager in Windows Server 2022*

2. On the left pane of the **Hyper-V Manager**, click on **Server**.

3. From the **Actions menu** on the right pane of **Hyper-V Manager**, select **New |Virtual Machine.**

4. A **New Virtual Machine Wizard** window will open, displaying preliminary information on the **Before You Begin** page. Click on **Next** to proceed.

5. On the **Specify the name and location** page, enter the **name and specify the virtual machine's location, then click Next**.

6. On the **Specify Generation** page, choose the **generation** for the virtual machine and click **Next**.

7. On the **Assign Memory** page, allocate **memory** for the virtual machine and check the box labeled **Use Dynamic Memory.** Click on the **Next** button to continue, as shown in the following figure:
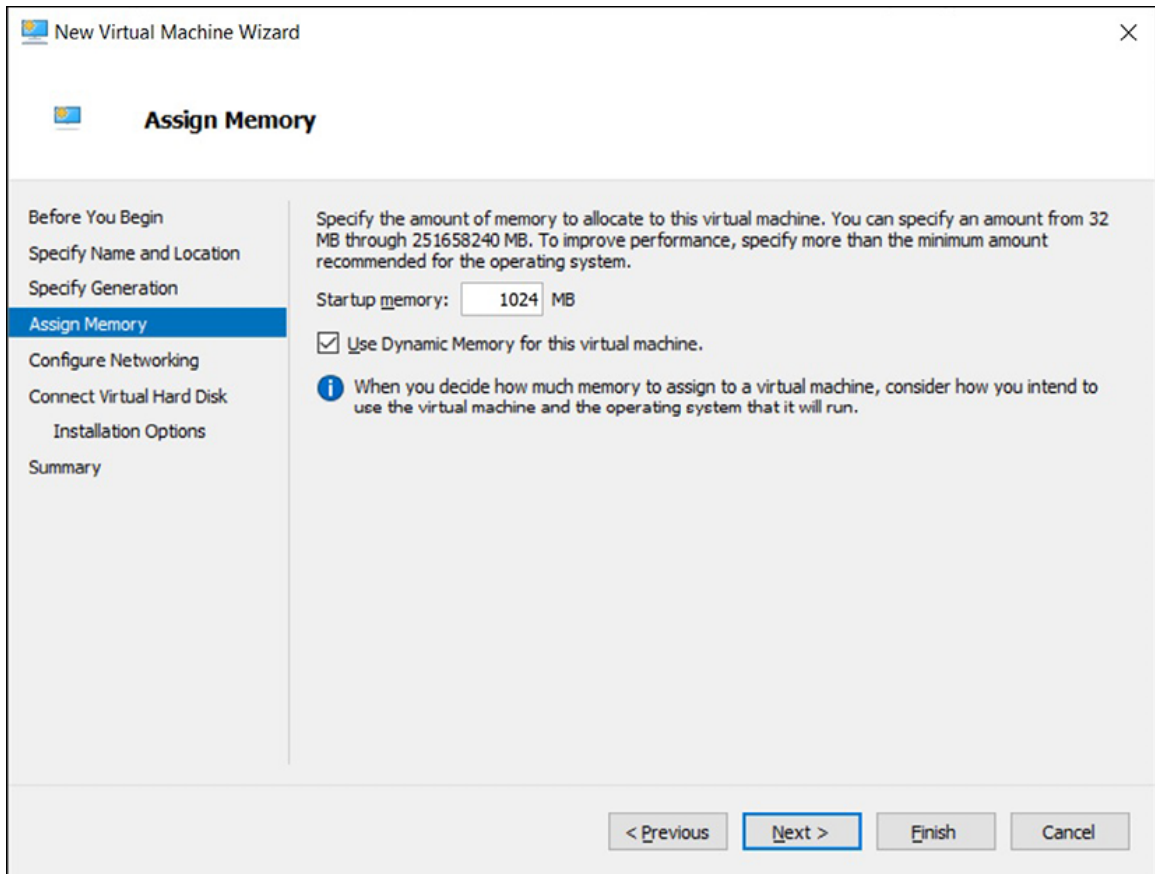
Figure 6.18: *Assigning memory for the virtual machine in Windows Server 2022 using Hyper-V Manager*

8. If no virtual switch is available on the **Configure network** page, accept the defaults and click **Next**.

9. On the **Connect virtual complex disk** page, specify the virtual machine's **storage configuration** and click **Next** to proceed.

10. On the **Installation option** page, choose the **installation option** for the virtual machine and click on the **Next** button to continue.

11. On the **Summary** page, click on **Finish** to create the virtual machine and close the **New Virtual Machine Wizard.**

Configuring a virtual machine using Windows PowerShell

To begin the process of configuring a VM in Windows Server 2022 using Windows PowerShell, follow the following steps:

1. Launch **Windows PowerShell** by right-clicking on the **Start** button.

2. Within the **Windows PowerShell** interface, to configure a virtual machine, input the provided cmdlet and then press *Enter*:

```
New-VM -VMName Windows11 -MemoryStartupBytes
1024MB
```

Take a look at the following figure:

Figure 6.19: *Configuring a virtual machine in Windows Server 2022 using Windows PowerShell*

3. To create a virtual hard drive, input the provided cmdlet and then press *Enter*:

```
New-VHD -Path "C:\users\Public\Documents\Hyper-
v\Virtual Hard Disks\Windows11.vhdx" -Sizebytes
50GB -Fixed
```

4. To attach a virtual hard drive, input the provided cmdlet and then press *Enter*:

```
Add-VMHardDiskDrive -VMName Windows11 -Path
"C:\Users\Public\Documents\Hyper-V\Virtual Hard
Disks\Windows11.vhdx" -ControllerType IDE -
ControllerNumber 0 -ControllerLocation 1
```
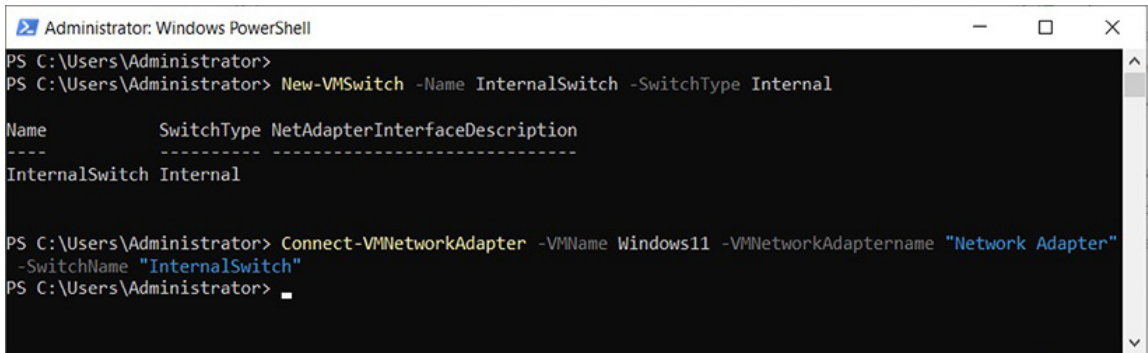
5. To configure an internal virtual switch, input the provided cmdlet and then press *Enter*, as shown in *Figure 6.20*:

```
New-VMSwitch -Name InternalSwitch -SwitchType
Internal
```

6. To connect a network adapter to an internal virtual switch, as shown in *Figure 6.20,* input the provided cmdlet and then

press *Enter*:

```
Connect-VMNetworkAdapter -VMName Windows11 -
VMNetworkAdaptername "Network Adapter" -SwitchName
"InternalSwitch"
```


Figure 6.20: *Configuring an internal virtual switch and connecting a network adapter*

7. To specify a path to an ISO file, input the provided cmdlet and then press *Enter*:

```
Set-VMDvdDrive -VMName Windows11 -ControllerNumber
1 -Path "C:\ISO Images\Windows11.ISO"
```

Configuring a website

Setting up a website using **Internet Information Services (IIS)** presents numerous benefits and is a widely adopted method for hosting Web applications. Some benefits are as follows:

- IIS is a robust and reliable platform, ensuring consistent performance and efficient resource utilization for hosted websites. It boasts many features and configuration options that allow website functionality and security customization.

- IIS seamlessly integrates with the Windows operating system, providing a familiar and user-friendly interface for website management. Its centralized management capabilities enable effortless creation, configuration, and monitoring of multiple websites from a single location.

- IIS supports various Web technologies and protocols, such as HTTP, HTTPS, and FTP, offering flexibility and

adaptability to accommodate diverse Web applications. IIS optimizes website performance and responsiveness by leveraging advanced features like load balancing, caching, and compression.

- IIS incorporates robust security measures, including SSL/TLS encryption, authentication choices, and access control, safeguarding websites and sensitive data. Opting for IIS to configure a website delivers a stable, customizable, and secure hosting environment, making it a popular choice for web applications on Windows servers.

Exercise 6.5—Configuring a Website

This exercise outlines the procedure for configuring a website using Internet IIS Manager and PowerShell.

Configuring a website using IIS manager

To begin the process of configuring a website in Windows Server 2022 using IIS Manager, follow the following steps:

1. Open the **IIS Manager** by clicking on the **Start** button and then clicking on **Windows Administrative Tools**. Then, double-click on **Internet Information Services (IIS) Manager.** Take a look at the following figure:

Figure 6.21: *Internet Information Services Manager in Windows Server 2022*

2. Expand the **Webserver** from the tree on the left side of the **IIS Manager**.

3. Click on **Sites** on the left side of the console. From the **Actions** on the right pane of the **IIS Manager**, select **Add Website...**

4. The **Add Website** window opens. Enter a **Name** for the site and specify the **Physical path** of the **Content Directory** section.

5. On the **Binding** section, if **Port 80** is already in use, change the **Port to 8080**, as in Click **OK** to close the **Add Website** dialog box. Take a look at the following figure:
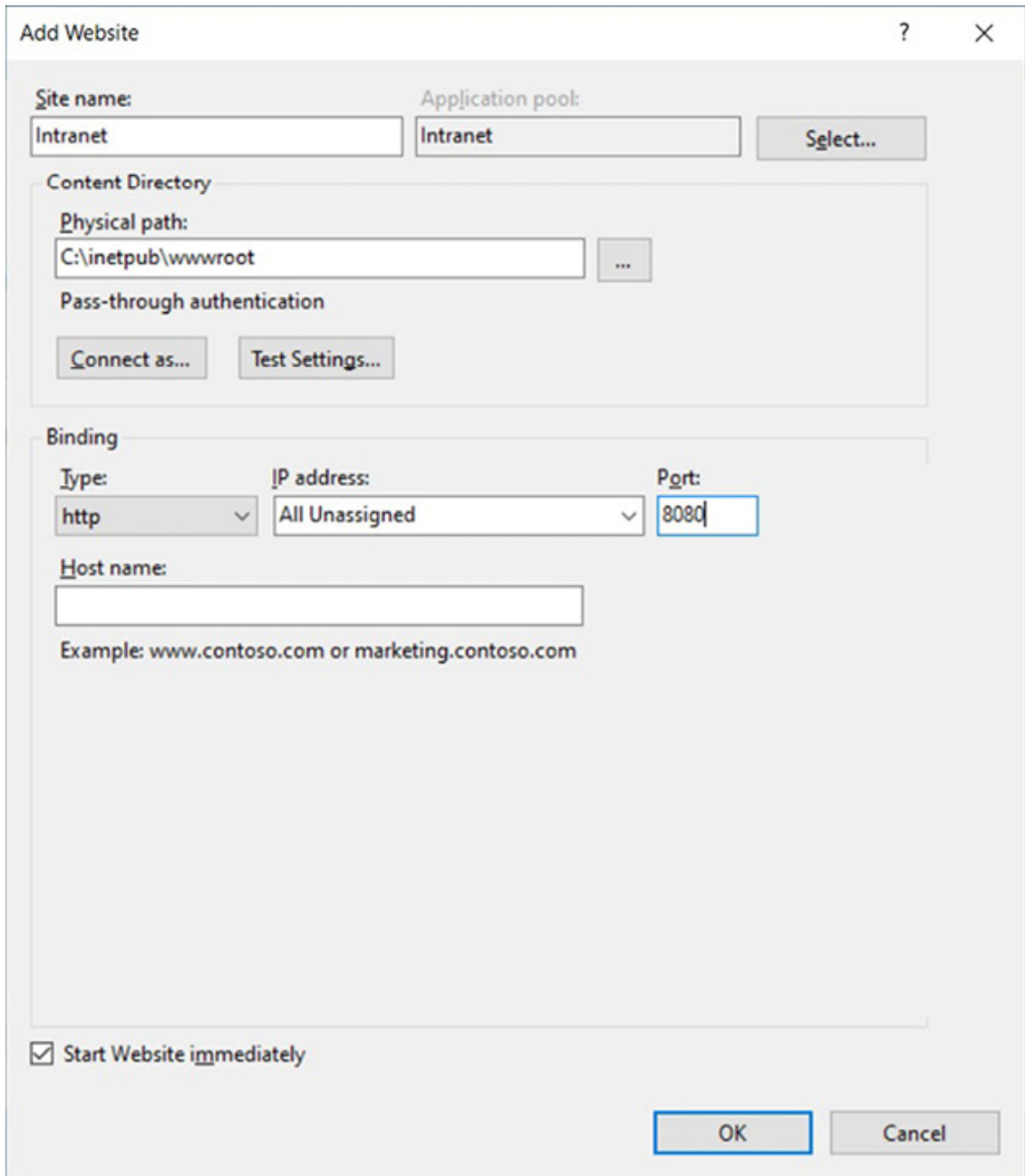
Figure 6.22: Configuring a Website in Windows Server 2022 using IIS Manager

6. The recently added website will be listed in the middle pane of the **IIS Manager** console.

7. From the **Actions** on the right side of the **IIS Manager**, click on **Browse *.8080 (HTTP)** to open the newly added website.

Configuring a website using Windows PowerShell

To begin the process of configuring a website in Windows Server 2022 using Windows PowerShell, follow the following steps:

1. Launch **Windows PowerShell** by right-clicking on the **Start** button.

2. Within the **Windows PowerShell** interface, to create a website, input the provided cmdlet and then press *Enter*:

   ```
   New-Website —Name Intranet —PhysicalPath
   C:\Intranet
   ```

   Take a look at the following figure:
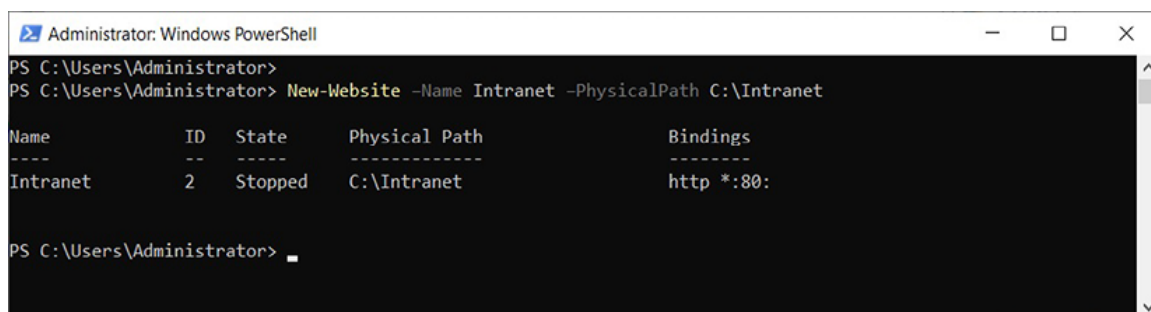
Figure 6.23: Creating a Website in Windows Server 2022 using Windows PowerShell

3. To copy the `index.htm` from the Share folder to the Intranet folder, input the provided cmdlet and then press *Enter*:

   ```
   C:\Share\*.* C:\Intranet
   ```

4. To stop the default website, input the provided cmdlet and then press *Enter*:

   ```
   Get-Website —Name 'Default Web Site› | Stop-
   Website
   ```

5. To start the intranet website, input the provided cmdlet and then press *Enter*:

   ```
   Get-Website —Name 'Intranet' | Start-Website
   ```

   Take a look at the following figure:
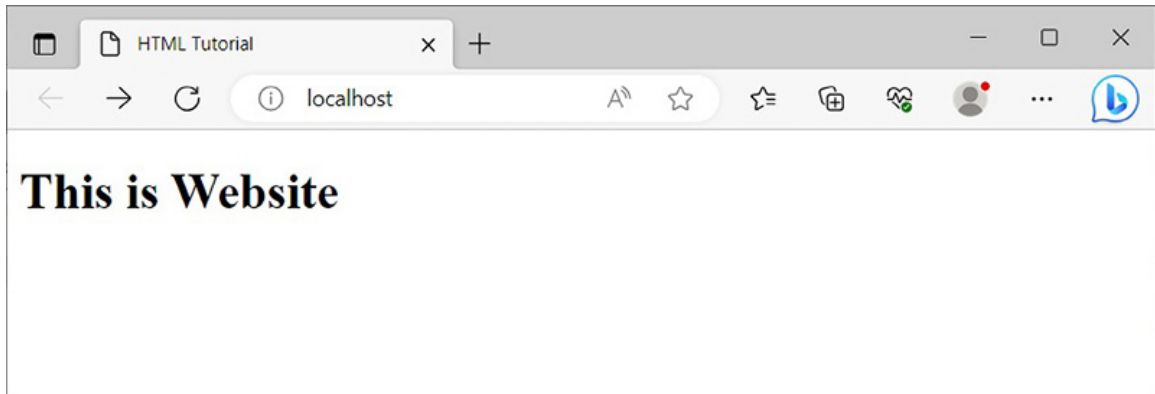
Figure 6.24: *Browsing the newly created Website in Windows Server 2022 using Windows PowerShell*

Note: To perform a test, I have generated a Web page named index.htm within a folder named Intranet on disk C. Once the website is started, browse it through a Web browser, as illustrated in *Figure 6.24*.

Configuring the print server

Configuring the print server on Windows Server using the **Print Management console** (**PDS**) is essential for efficient and centralized printer management in a networked environment. It provides numerous benefits, including centralized printer control, simplified printer deployment, effective driver management, improved printer sharing capabilities, centralized monitoring and control of printers, enhanced print job efficiency, and potential cost savings. By configuring a print server, administrators can manage printers from a single location, easily add or remove printers, distribute printer drivers to client machines, enable printer sharing, monitor printer status, control print queues, prioritize print jobs, and optimize resource allocation. This centralized approach streamlines printer management, boosts productivity, and reduces printer deployment and maintenance expenses.

Exercise 6.6—Configuring the print server

This exercise outlines the procedure for configuring a print server print management and PowerShell.

Configuring print server using print management

To begin the process of configuring the print server in Windows Server 2022 using Print Management, follow the following steps:

1. Open **Print Management** by clicking on the **Start** button and then clicking on **Windows Administrative Tools**. Then, double-click on **Print Management**. The window appears as shown in the following figure:
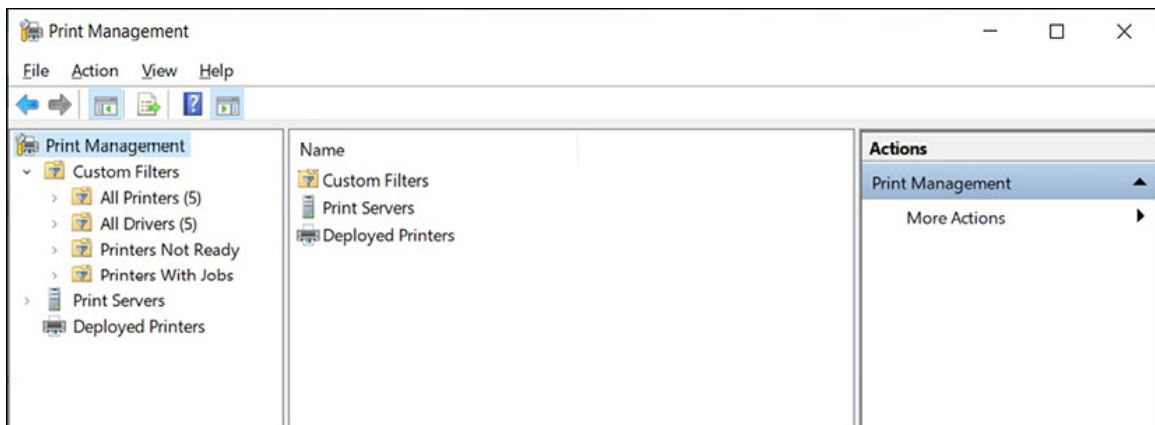
Figure 6.25: Print management console in Windows Server 2022

2. Expand **Print Servers** from a tree structure pane, then expand the **server**. Right-click on **Printers** and select **Add Printer...**

3. The **Network Printer Installation Wizard** opens up to help you install a network printer.

4. Specify the **installation method** on the **Printer installation** page and click the **Next** button. Based on a chosen installation method, you will search for a network printer, add an IP address, and use an existing port to add a new printer or create a new port to add a new printer. Click on the **Next** button to proceed.

5. After completing the **printer installation**, look at the right pane of the **Print Management** console to find your newly added printer.

6. Select the **printer** and click on the **Action** menu. From the expanded menu, select **Manage Sharing...**

7. Ensure the **Share this printer** and **List in the directory** checkboxes are checked, as shown in *Figure 6.26:*
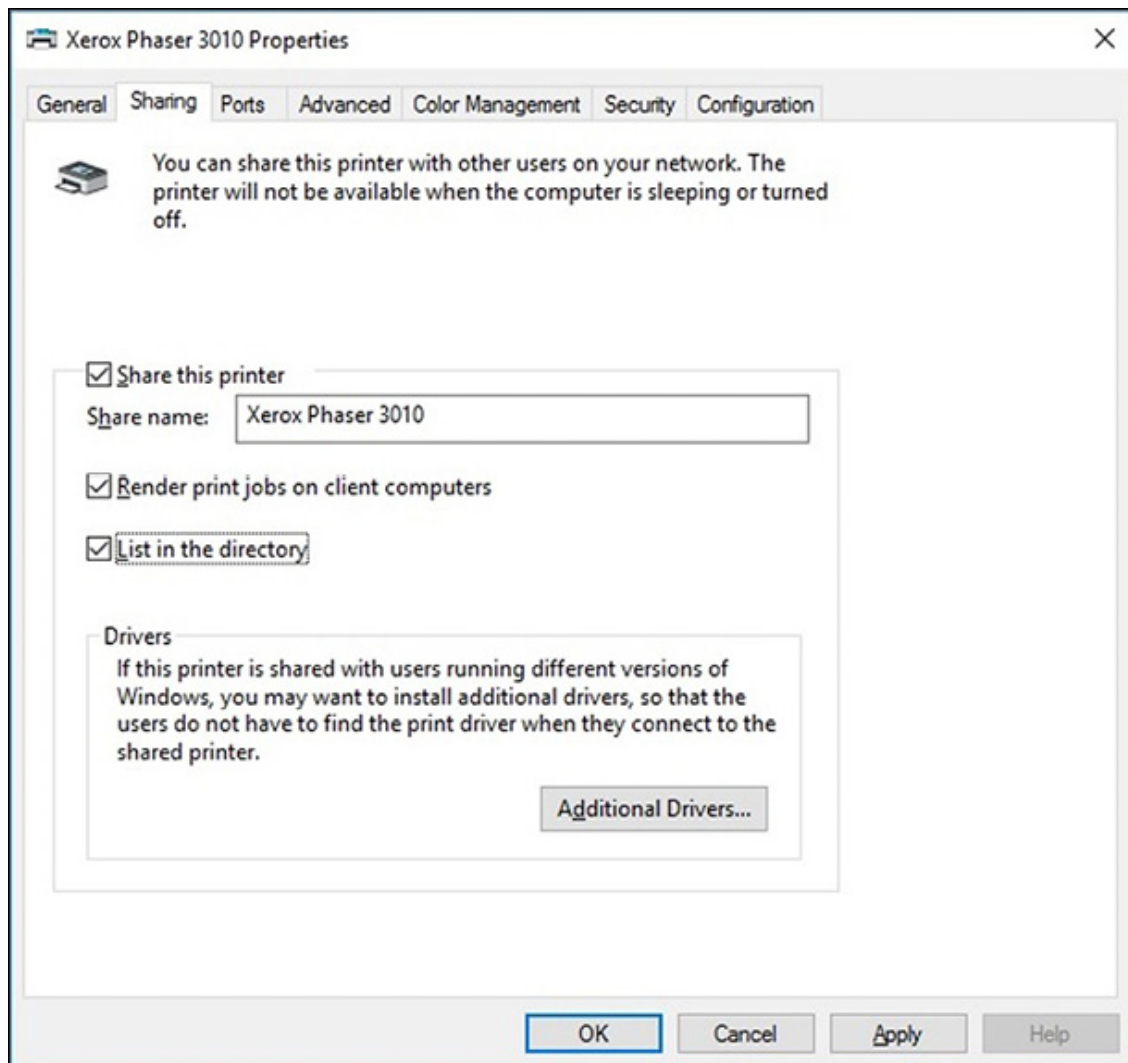
Figure 6.26: *Sharing a printer in Windows Server 2022 using print management*

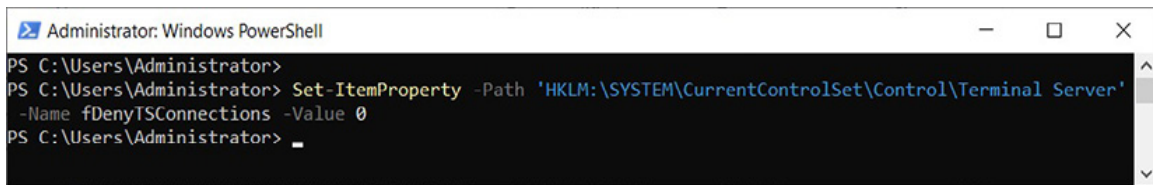8. Once the **sharing options** are maintained, click the **OK** button to close the dialog box.
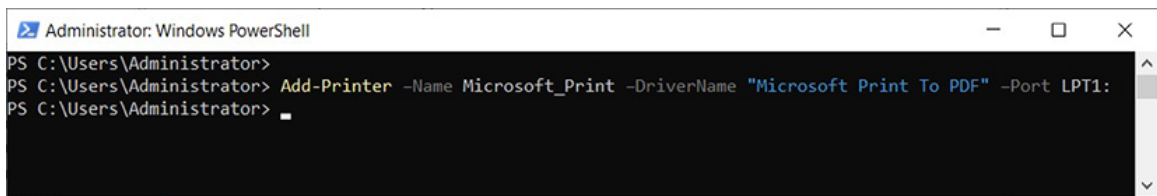
Configuring print server using Windows PowerShell

To begin the process of configuring the print server in Windows Server 2022 using Windows PowerShell, follow the following steps:

1. Launch **Windows PowerShell** by right-clicking on the **Start** button.

2. Within the **Windows PowerShell** interface, to install a printer, input the provided cmdlet and then press *Enter*:

   Add-Printer –Name Microsoft_Print –DriverName "Microsoft Print To PDF" –Port LPT1:

   Take a look at the following figure:

Figure 6.27: *Installing a printer in Windows Server 2022 using Windows PowerShell*

3. To share the printer, input the provided cmdlet and then press *Enter*:

   Set-Printer -Name Microsoft_Print -Shared $True -Published $True -ShareName MicrosoftPrint

Note: It is recommended to install the driver before installing a printer. To do so, use the Add-PrinterDriver cmdlet.

Configuring Remote Desktop users

Configuring Remote Desktop users in Windows Server 2022 is vital for enabling remote access and facilitating effective server management and administration. It provides numerous advantages, such as remote administration capabilities, flexibility, and convenience for administrators to connect to the server from anywhere. With Remote Desktop, multiple administrators can connect simultaneously, promoting centralized management and collaboration. It also allows for remote troubleshooting and maintenance, reducing downtime and improving system availability. Moreover, using Remote Desktop eliminates the need for dedicated physical consoles,

potentially resulting in cost savings for hardware and infrastructure.

Furthermore, it enhances security by enabling access control and restricted connections for authorized individuals or groups. In addition, Remote Desktop ensures business continuity by allowing the administrators to manage the server during unforeseen events or emergencies when physical access is impossible. Configuring Remote Desktop users in Windows Server 2022 enhances server management and administration efficiency, security, and flexibility.

Exercise 6.7—Configuring Remote Desktop Users

This exercise outlines the procedure for configuring Remote Desktop users using Active Directory Users and Computers and PowerShell.

Configuring Remote Desktop users using Active Directory users and computers

To begin the process of configuring Remote Desktop users in Windows Server 2022 using Active Directory Users and Computers, follow the following steps:

1. Open **Active Directory Users and Computers** by clicking on the **Start** button and then clicking on **Windows Administrative Tools**. Then, double-click on **Active Directory Users and Computers.** Take a look at the following figure:
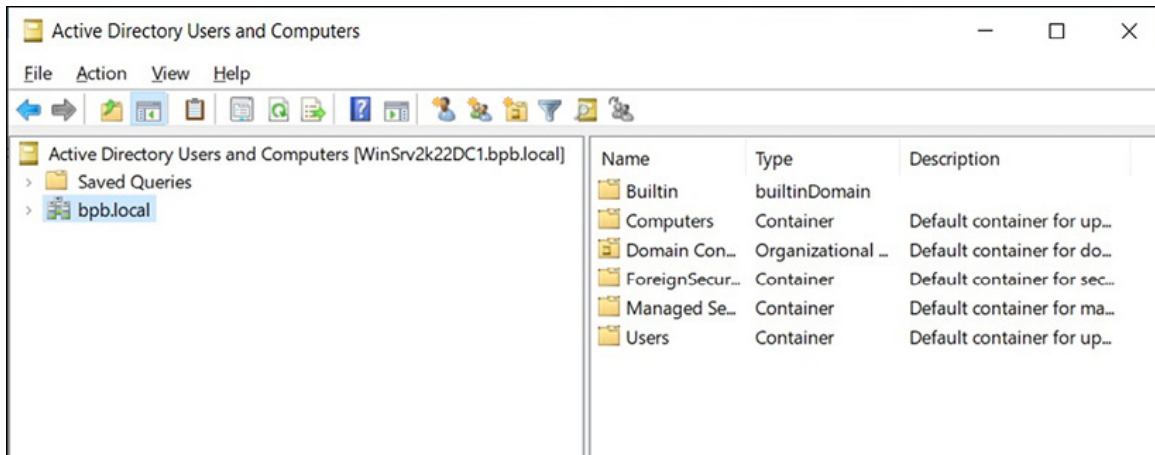
Figure 6.28: *Active Directory Users and Computers Console in Windows Server 2022*

2. Expand the **Server** on the left pane of the **Active Directory Users and Computers** console.

3. Click on **Users** in the tree view on the left pane of the **Active Directory Users and Computers** console.

4. Locate the **Test User** on the right pane of the **Active Directory Users and Computers** console and right-click it.

5. Select the **Add to a group…** option from the context menu.

6. In the Select Groups dialog box, enter the Remote Desktop user in the provided field and click the **Check Names** button to verify the group name. Click on **OK** to close the dialog box. Take a look at the following figure:
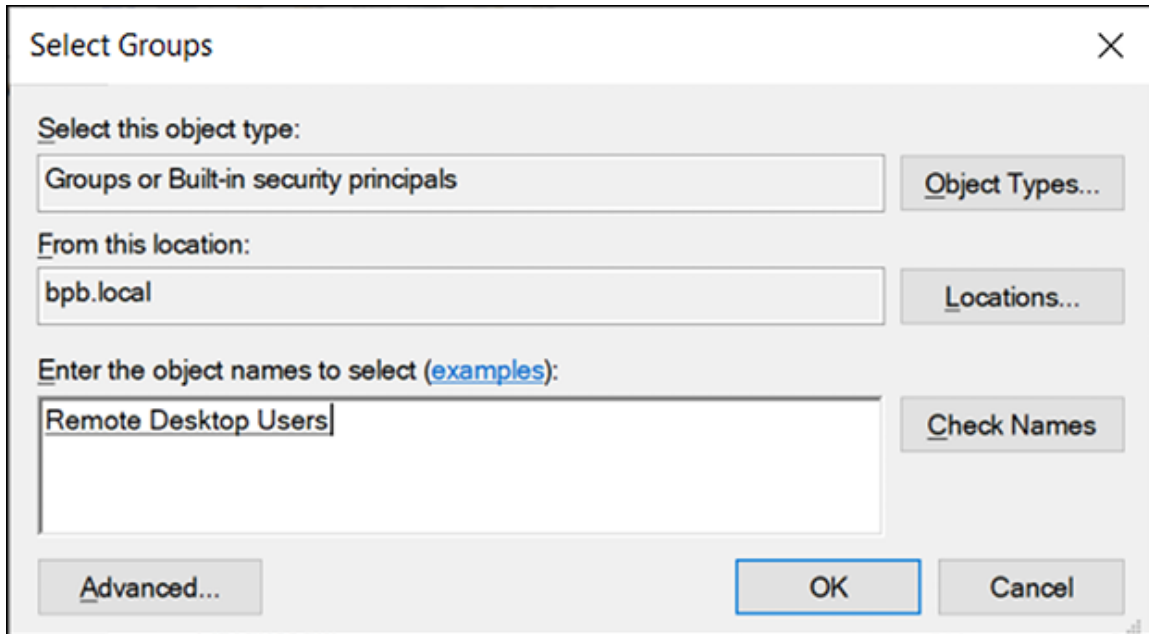
Figure 6.29: Adding a user into the Remote Desktop Users group in Windows Server 2022

7. Click on **OK** to close the **Add to group operation was successfully completed** dialog box.

Note: The Test User used for this practical demonstration has been pre-created beforehand.

Configuring Remote Desktop users using Windows PowerShell

To begin the process of configuring Remote Desktop users in Windows Server 2022 using Windows PowerShell, follow the following steps:

1. Launch **Windows PowerShell** by right-clicking on the **Start** button.

2. Within the **Windows PowerShell** interface, to allow RDP connections on a server, input the provided cmdlet and then press *Enter*:

```
Set-ItemProperty -Path
'HKLM:\SYSTEM\CurrentControlSet\Control\Terminal
Server' -Name fDenyTSConnections -Value 0
```

Take a look at the following figure:

Figure 6.30: Allowing RDP connection on a server in Windows Server 2022 using Windows PowerShell

3. To configure Network Level Authentication, input the provided cmdlet and then press *Enter*:
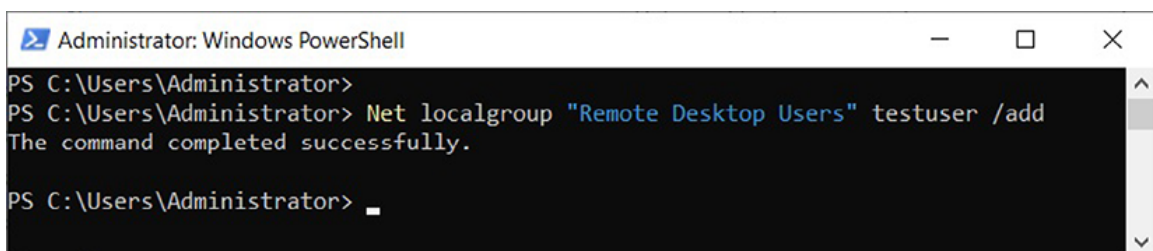
```
Set-ItemProperty -Path
'HKLM:\SYSTEM\CurrentControlSet\Control\Terminal
Server\WinStations\RDP-Tcp' -Name
UserAuthentication -Value 1
```

4. To allow the Remote Desktop firewall exception, input the provided cmdlet and then press *Enter*:

```
Set-NetFirewallRule -DisplayGroup 'Remote Desktop'
-Enabled True
```

5. To add a user to the Remote Desktop Users group, as shown in *Figure 6.31*, input the provided cmdlet and then press *Enter*:

```
Net localgroup "Remote Desktop Users" testuser
/add
```


Figure 6.31: Adding a user to the Remote Desktop Users group in Windows Server 2022 using Windows PowerShell

Configuring the WSUS server

Configuring **Windows Server Update Services (WSUS)** is crucial for effectively managing and regulating the distribution of Windows updates in a networked environment. It establishes a centralized platform that empowers administrators to handle and deploy updates efficiently, ensuring uniformity and productivity throughout the network. Using WSUS allows administrators to optimize network bandwidth by downloading updates once from the WSUS server and internally distributing them, reducing the need for redundant internet downloads.

Moreover, WSUS facilitates improved control and testing of updates, enabling administrators to thoroughly assess and approve updates for compatibility and stability before deployment. WSUS significantly enhances compliance and security by guaranteeing that all network machines stay updated with the latest security patches and fixes, mitigating potential vulnerabilities. With WSUS's comprehensive reporting and monitoring capabilities, administrators gain valuable insights into the updated status of machines, facilitating effective tracking of installations and timely resolution of any issues that may arise.

Furthermore, WSUS offers customization features that empower administrators to target updates based on specific criteria, ensuring that critical updates are prioritized and deployments are efficiently managed. Configuring WSUS is pivotal in achieving centralized update management, optimizing bandwidth utilization, maintaining update control and testing, reinforcing compliance and security, facilitating robust reporting and monitoring, and enabling customization, all contributing to establishing a secure and well-maintained network environment.

Exercise 6.8—Configuring the WSUS Server

This exercise outlines the procedure for configuring the WSUS Server using WSUS Manager.

Configuring the WSUS server using the WSUS manager

To begin the process of configuring the WSUS Server in Windows Server 2022 using WSUS Manager, follow the following steps:

1. Open **Server Manager** from the **Start** menu.
2. Click on the **Notifications** icon, then select **Launch Post-Installation tasks,** as shown in *Figure 6.32:*
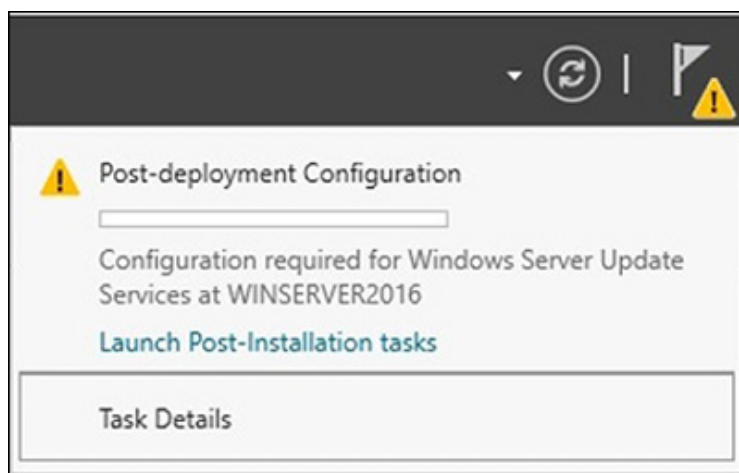
Figure 6.32: Finalizing WSUS post-installation tasks in Windows Server 2022 using Server Manager

3. Open **Windows Server Update Services (WSUS) Manager** by clicking on the **Start** button and then clicking on **Windows Administrative Tools**. Then, double-click on **Windows Server Update Services**.
4. The **Complete WSUS Installation** window will open shortly, as in *Figure 6.33*. Verify that the **Content directory path** is correct and click on **Run**. Keep the dialog box open during the **WSUS post-installation task**, although it may take a few minutes. Take a look at the following figure:
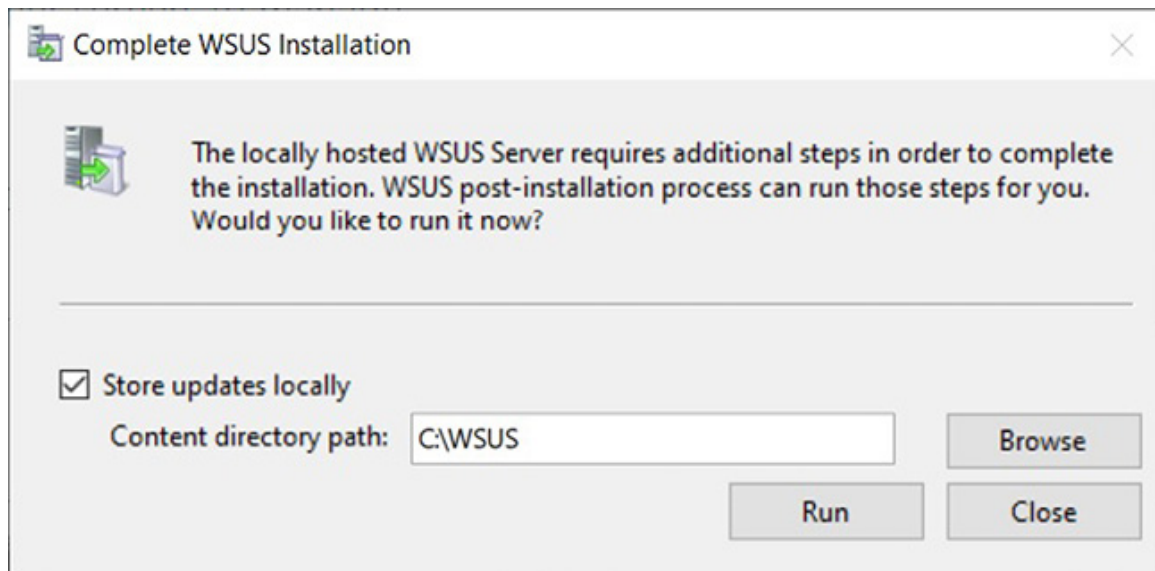
Figure 6.33: Running the WSUS post-installation task in Windows Server 2022

5. Once the **WSUS post-installation task** is completed, click on **Close**.

6. The **WSUS Configuration Wizard** will open. Read the content on the **Before You Begin** page and click **Next**.

7. On the **Microsoft Update Improvement Program** page, optionally, choose to join the **Microsoft Update Improvement Program** and click on **Nex**t.

8. On the **Choose upstream server** page, specify the **upstream server** and click **Next**.

9. Enter the proxy server settings on the **Specify proxy server** page and click **Next** if applicable.

10. On the **Connect to Upstream server** page, click **Start Connection**, then click on **Next**.

11. On the **Choose the Products** page, specify the **products needed for updates** and click **Next**.

12. On the **Choose classifications** page, you must choose the **update classification to synchronize** and click on **Next**.

13. Configure the **synchronization schedule** between the **WSUS server** and **Microsoft Update on the Set sync schedule** page. Click on **Next** to proceed.

14. Launch the **WSUS Administration** console on the **Finished** page or start the **initial synchronization**. Click on **Next**.

15. Explore **additional topics** for fully configuring the **WSUS server** on the **What's Next** page.

16. After closing the **WSUS Configuration Wizard**, the **WSUS Manager** console will open, as shown in *Figure 6.34*:
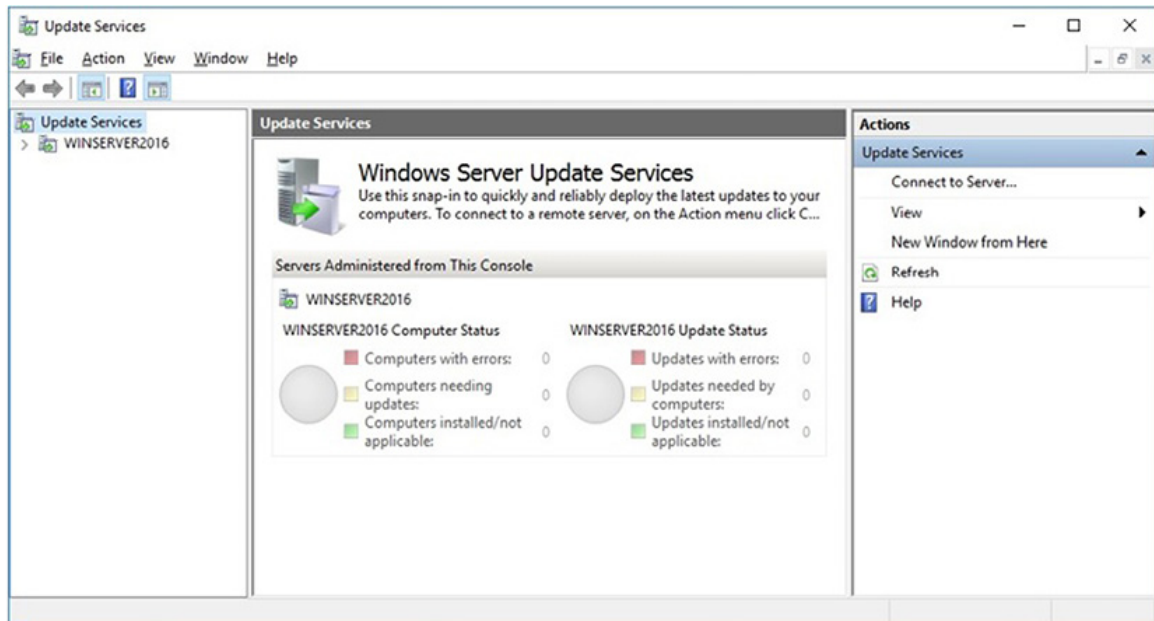
Figure 6.34: *WSUS Manager in Windows Server 2022*

Conclusion

This chapter provided a comprehensive step-by-step installation guide on configuring client/server network services in Windows Server 2022 using Windows PowerShell cmdlets. By leveraging the power of Windows PowerShell, you have discovered efficient methods to configure various network services in Windows Server 2022. The covered topics have included configuring a domain controller, managing DNS records, configuring an IPv4 scope in a DHCP server, configuring a virtual machine, establishing a Web server, setting up a print server, configuring Remote Desktop users, and setting up a WSUS server. Through the detailed instructions and utilization of the provided cmdlets, you have gained the necessary skills to successfully configure

and manage these essential network services in Windows Server 2022. The upcoming chapter will focus on enhancing the performance of Windows Server 2022 through optimization techniques.

Questions

1. What is a domain controller (DC)?
2. What is an A record?
3. What is an IPv4 scope?
4. What is a virtual machine (VM)?
5. What is a website?
6. What is a print server?
7. What is a Remote Desktop user?
8. What are WSUS benefits?

Join our book's Discord space

Join the book's Discord Workspace for Latest updates, Offers, Tech happenings around the world, New Release and Sessions with the Authors:

https://discord.bpbonline.com

CHAPTER 7
Tuning Windows Server 2022 for Peak Performance

Introduction

This chapter provides comprehensive guidance on optimizing the performance of Windows Server 2022. First, system administrators must deeply understand server hardware components and their roles in a computer network. With this knowledge, system administrators can make informed decisions when selecting server hardware, ensuring their servers perform at their best. Next, this chapter goes over performance monitoring, which is essential for maintaining optimal server performance, and troubleshooting issues as they arise. The Windows Admin Center is a crucial tool that enables system administrators to monitor server performance effectively. This chapter also introduces Performance Monitor, Resource Monitor, and Task Manager for effective server performance monitoring. Finally, this chapter emphasizes the importance of logs and alerts in maintaining optimal server performance. It guides logging collected information and setting up alerts to identify and resolve issues that may arise quickly. By incorporating all these best practices and techniques, readers can ensure that their Windows Server 2022 systems are performing at peak efficiency while being able to monitor and maintain their servers effectively.

Structure

In this chapter, we will cover the following topics:

- Server hardware components and their roles
- Performance monitoring basics
- Best practices for server maintenance
- Overview of Windows Admin Center
- Logs and alerts for server performance

Objectives

This chapter aims to guide system administrators in optimizing the performance of Windows Server 2022. This chapter will cover topics such as understanding server hardware components, selecting the best hardware, and monitoring server performance with Windows Admin Center and Performance Monitor tools. This chapter also emphasizes the importance of logs and alerts in maintaining optimal server performance and guides the reader in setting them up. By following these best practices and techniques, the readers can ensure that their Windows Server 2022 systems are performing at peak efficiency while being able to monitor and maintain their servers effectively.

Server hardware components and their roles

When it comes to technology, a server is essentially just a computer. If you open up the case of a server, you will see a variety of components that make up the internal hardware. These components are often referred to as hardware components in tech terminology. When it comes to servers, it is essential to understand what they are and how they impact a server's performance.

You may be wondering why understanding server hardware components is so important. After all, a server's primary role is not necessarily data processing. Instead, as discussed in *Chapter 5, Using the Add Roles and Features Wizard in Windows Server 2022*, servers are responsible for providing network services and

handling user requests to access those services. However, the hardware a server is built with can significantly impact how effectively it performs its tasks.

To that end, it is essential to take the time to understand server hardware components and how they function within a server. That includes the processor, memory, storage, and network interface cards. Each of these components plays a crucial role in how a server operates, and by understanding how they work, you can make informed decisions when selecting server hardware. Let us learn more about the components as follows:

- **Processor:** Speed is essential when selecting a suitable processor, measured in Hertz (Hz), with modern processors reaching Gigahertz (GHz). However, speed is not the only determining factor, as other essential components must be considered. The cache is one such component, referring to the processor's memory. The larger the cache capacity, the more data can be retrieved from memory for processing. As shown in *Figure 7.1*, modern processors have L1, L2, and L3 cache types, with their speed determined by the number of caches. The core is the processor's processing unit, with modern processors having up to dozens of cores, allowing for more multiprocessing. Word size refers to the processor's internal architecture, with modern processors using either 32-bit or 64-bit word size. Registers are the processor's high-speed memory and are considered the fastest component in the computer system. Finally, virtualization technology enables multiple operating systems to share processor resources, making it essential to consider when selecting a processor that meets a server's performance needs. Please refer to the following figure:

Figure 7.1: Intel's Xeon processor powers modern servers

- **Memory:** The primary storage of a computer consists of hardware that temporarily stores data and allows the processor to access it quickly. RAM and ROM are two types of primary storage, with the former being volatile and the latter being non-volatile. RAM is working memory and loads the operating system and apps, whereas ROM is hardware initialization memory and runs the Power-On Self-Test. Servers typically use ECC memory, as shown in *Figure 7.2*, which has one more chip than the RAM modules in PCs and enables the detection and correction of memory errors. Although advanced types of RAM, such as **Single Device Data Correction** (**SDDC**) and **Double Device Data Correction** (**DDDC**), exist, RAM for servers is generally expensive due to its features. Therefore, understanding the characteristics of primary storage is crucial in selecting suitable RAM for servers. Please refer to the following figure:
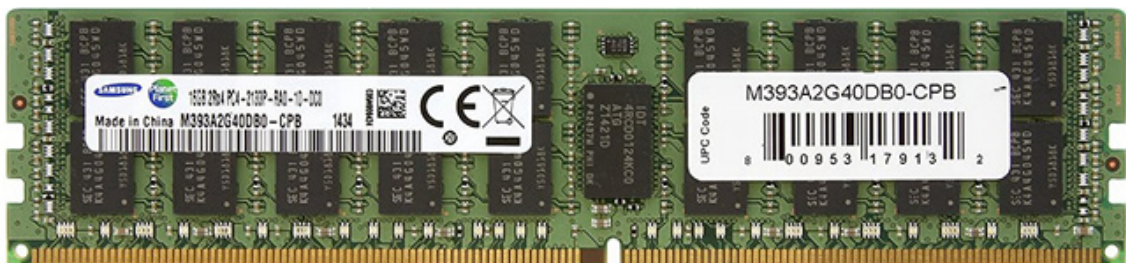
Figure 7.2: ECC RAM is standard for servers

- **Disk:** Servers are critical machines of modern information systems and must always be operational. To achieve this, servers must have the hardware to support continuous uptime and ensure that data and services are available to users. **Direct-attached storage** (**DAS**) is a group of disks connected to the server, and servers are equipped with this type of storage to ensure data availability. Hot-swappable technology, which replaces damaged disks without interrupting the server's operation, is also a common feature of DAS. With these features and more, servers can provide high availability of data and services, making them an essential part of modern IT infrastructure. Refer to the following figure:

Figure 7.3: SAS disks are used in modern servers

- **Network interface:** A network interface serves as the connection point between a computer and a network, which can be physical or logical, with virtual machines represented by software. Servers typically have multiple network interfaces, as shown in *Figure 7.4*, and adding **Network Interface Cards** (**NIC**) can offer tremendous benefits. For instance, numerous NICs enable NIC teaming, increasing the server's bandwidth. In addition, **Network Load Balancing** (**NLB**) helps distribute the network load across servers, whereas network separation allows you to separate intranet traffic from internet traffic. Therefore,

adding NICs to servers can enhance network performance, security, and reliability. Please refer to the following figure:
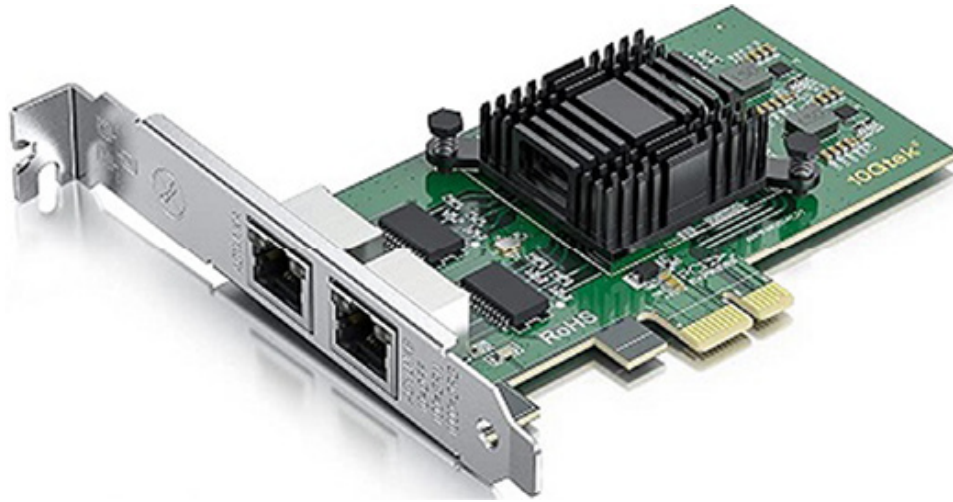
Figure 7.4: A server's NIC with dual network interfaces

Server's miscellaneous hardware

Servers are essential in modern computing, requiring various components to function efficiently. One such component is the processor, and the difference between 32-bit and 64-bit processors is significant. The 32-bit processors are considered a legacy technology, whereas 64-bit processors are modern and much faster. The RAM capabilities of these processors also differ, with 32-bit processors accessing up to 232 data from RAM and 64-bit processors accessing up to 264 data from RAM.

Another essential component of servers is removable drives, which offer external and portable storage. These drives can be plugged into and unplugged from servers using USB and IEEE 1,394 ports, and they include technologies such as CDs, DVDs, USB flash drives, and backup drives.

Regarding graphics cards, servers do not typically require advanced graphics cards, but it ultimately depends on the server's purpose. For example, servers that deal with graphics and video processing may require advanced graphics cards, which are necessary for tasks such as 3D animation and Auto CAD.

Servers generate significant thermal heat, mainly from their processors and hard disk drives. To maintain an optimum temperature, servers require a processor's coolers and case coolers (case fans), which draw thermal heat out of the computer case by blowing it. In addition, air conditioners maintain the optimal temperature in the server room and data centers.

Power supplies are another crucial component of servers. They convert **Alternative Current** (**AC**) to **Direct Current** (**DC**) and supply power to the motherboard, adapters, and peripheral devices. Redundant power supplies are essential because they prevent single points of failure. Servers generally have two or more **Power Supply Units** (**PSU**s) with hot plugs, allowing them to be replaced while the server works.

Finally, servers have multiple physical ports, which allow communication points for connecting cables to the computer. These ports include AC power connectors, Ethernet ports, PCIe ports, USB ports, HD-15 video connectors, management ports, and legacy ports such as serial, parallel, and PS/2 ports.

Note: ServeTheHome (**https://www.servethehome.com/**) is a comprehensive online resource that provides guidance and information for IT professionals on servers, storage, networking, and high-end workstation hardware. The website also features various excellent open-source projects.

Performance monitoring basics

The importance of performance monitoring in server maintenance cannot be overstated. As the saying goes, "Prevention is better than cure." Early identification of server problems is crucial in preventing them from becoming costly in both time and business. An effective performance monitoring plan requires a clear strategy and the right tools. It also involves setting up a metric to measure performance monitoring, which requires baseline information to evaluate the actual performance of servers, determine when upgrades are needed, and assess the effectiveness of upgraded systems. Without a clear plan, performance monitoring results will be based on assumptions, leading to bad business decisions.

To prevent this from happening, a performance monitoring methodology is used to conduct research and model a questionnaire that includes questions about the server's purpose, the services it provides, the components to monitor, the metric of component performance, and the tool to use for system analysis and data collection. By following this approach, businesses can ensure that performance monitoring is based on facts, not assumptions, and that they can make informed decisions about their server systems.

Overview of performance monitoring procedures

The performance monitoring methodology helps develop well-structured procedures; in the case of server performance monitoring, it is essential to follow specific guidelines, such as:

- Documenting the server's hardware, software, and configuration is crucial.

- Establishing the server's baseline helps to set performance standards.

- Upgrading the server's hardware and software is necessary to keep up with evolving technology.

- After any changes, performing a baseline check and comparing it with the previous ones is essential. Doing this can identify server bottlenecks that must be resolved to ensure the server runs efficiently.

- Finally, concrete steps must be taken to fine-tune the server's performance, ensuring optimal operation. Following these guidelines will help in developing structured procedures for monitoring server performance.

Importance of server baselines

The overall performance of a server needs to be monitored regularly, and as a system administrator, it is vital to ask some key questions to ensure the process is effective. For example, you may want to know how to identify when servers are overloaded and whether you have a benchmark to compare their performance against before discussing how to establish a

baseline and when to create one. A server baseline is a report that captures the implementation of various server components under normal working conditions. That includes the following:

- Processor and memory utilization
- Disk read-and-write operations
- Network connection utilization

It is important to note that performance monitoring is not limited to hardware components, and different networks may require monitoring of other parameters. Therefore, establishing a baseline to understand a server's expected performance and making accurate comparisons to identify any issues is essential.

Note: The TechRepublic article (**https://www.techrepublic.com/article/pro-tip-using-server-manager-to-baseline-your-windows-hardware/**) provides a pro tip for using the Server Manager tool in Windows to establish a server baseline, which is a snapshot of a server's performance under normal workload conditions. In addition, the article explains the steps involved in creating a baseline and how to analyze the performance data to identify potential issues and optimize the server's performance.

Understanding performance monitor

The performance monitor is an essential tool for server administrators that provides detailed insights into the server's performance. By monitoring the server's performance, administrators can detect and resolve any potential issues or bottlenecks affecting the server's availability or performance. The performance monitor tool visually represents real-time performance data, allowing administrators to monitor the server's performance in real-time or from a log file. In addition, the information gathered by the performance monitor is displayed in various formats, including line graphs, histogram bars, or report formats, which provides administrators with a comprehensive view of the server's performance. To launch the Performance Monitor in Windows Server 2022, complete the following steps:

1. Open the `Run` dialog box by pressing the *Windows key + R* on your keyboard.
2. Type in `perfmon.exe` in the `Run` dialog box and hit *Enter*.

3. The **Performance Monitor** tool, shown in *Figure 7.5*, will quickly open and display the current performance data of the server in real-time:
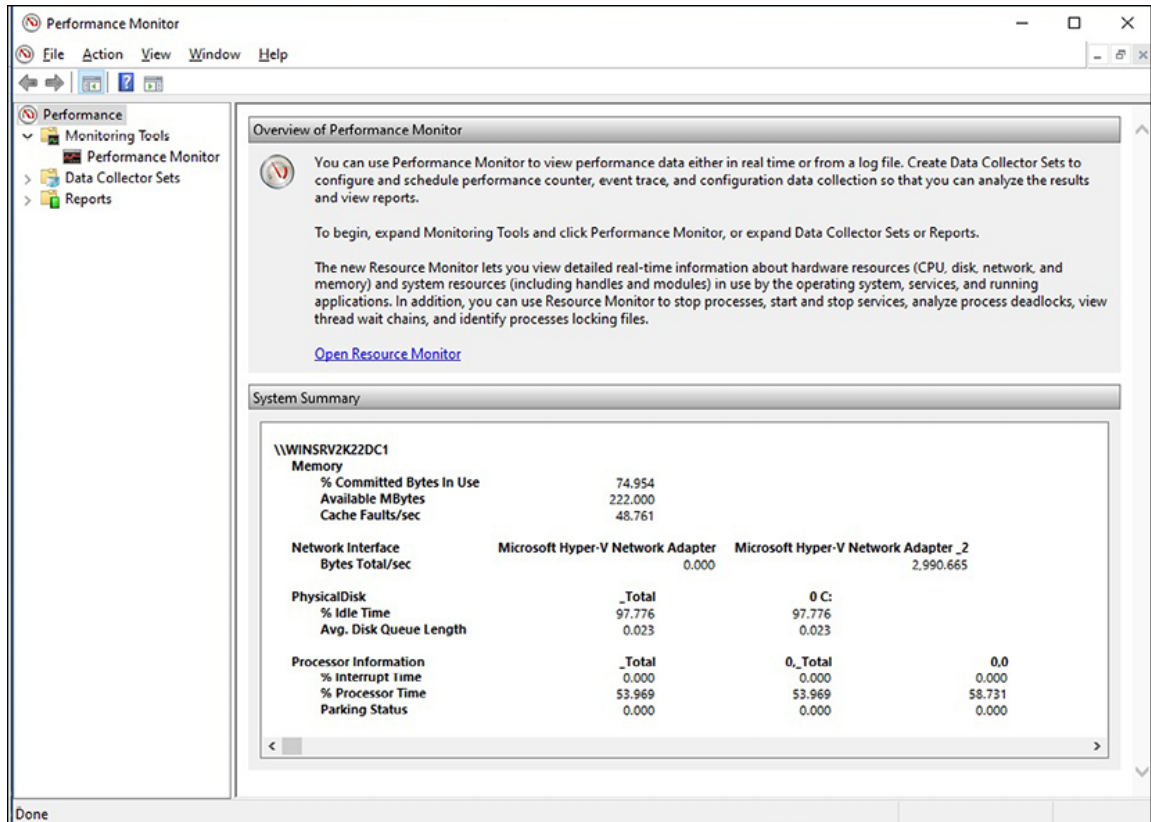
Figure 7.5: *Performance Monitor in Windows Server 2022*

In the performance monitor, you can use counters and instances of selected objects to gather data for the server hardware you are monitoring. Counters provide performance information on the operation of an operating system, application, service, or driver. Objects have counters to measure different aspects of performance, and each object has at least one instance representing an individual copy of a specific type of object. This feature enables you to identify server bottlenecks and quickly take action to avoid further degradation of server performance. After identifying the bottlenecks, you can fine-tune the server's performance by undertaking appropriate measures.

Exercise 7.1—Setting up data collector sets for Windows Server performance monitoring

This exercise concerns setting up a Data Collector Set in Windows Server 2022 performance monitor. Follow the given steps:

1. Open **Performance Monitor** and expand **Monitoring Tools**.
2. Select **Performance Monitor** and right-click to select **New | Data Collector Set**.
3. Name your **Data Collector Set** and click on **Next**.
4. Please specify the location to save it by clicking **Browse** and **Next**.
5. Set the user in **Run** and select either **Start this data collector set now** or **Save and Close**.
6. Click on **Finish**.
7. Right-click on **Graph** and select **Add Counters...**
8. Choose counters from the **Available Counters** section and click on the **Add** button to add them to the **Added Counters** section.
9. Repeat Step 8 to add more counters. Refer to *Figure 7.6.*
10. Click on **OK** to close the window.
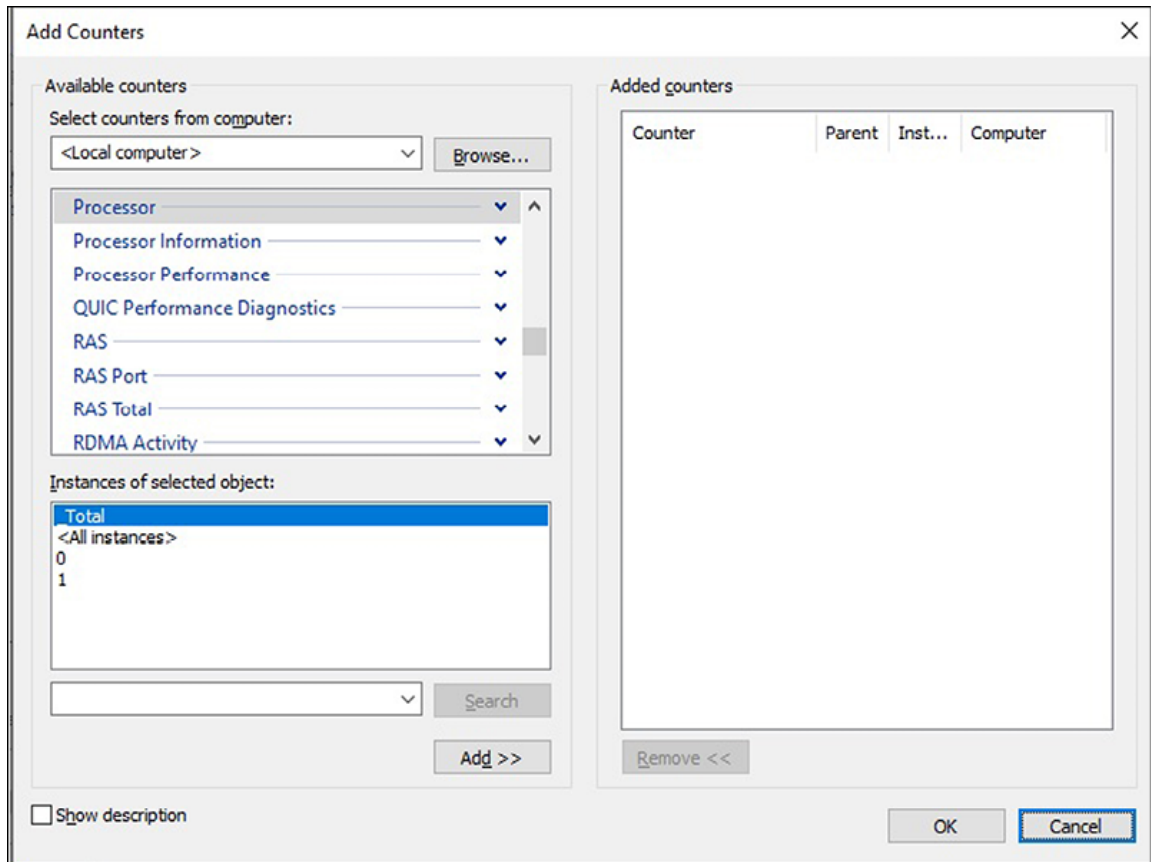
Figure 7.6: *Adding counters in the performance monitor of Windows Server 2022*

Getting to know resource monitor

Resource monitor is a tool in Windows Server 2022 that allows you to diagnose the cause of slow performance on your computer or server. It provides real-time monitoring of hardware and software resources, enabling you to identify the components responsible for the slow version. To run Resource Monitor, you can follow these simple steps:

1. Press the *Windows key + R*.

2. Enter `resmon.exe` and press *Enter*.

3. The Resource Monitor will appear shortly after, allowing you to view the real-time usage of hardware and software resources.

Refer to *Figure 7.7:*
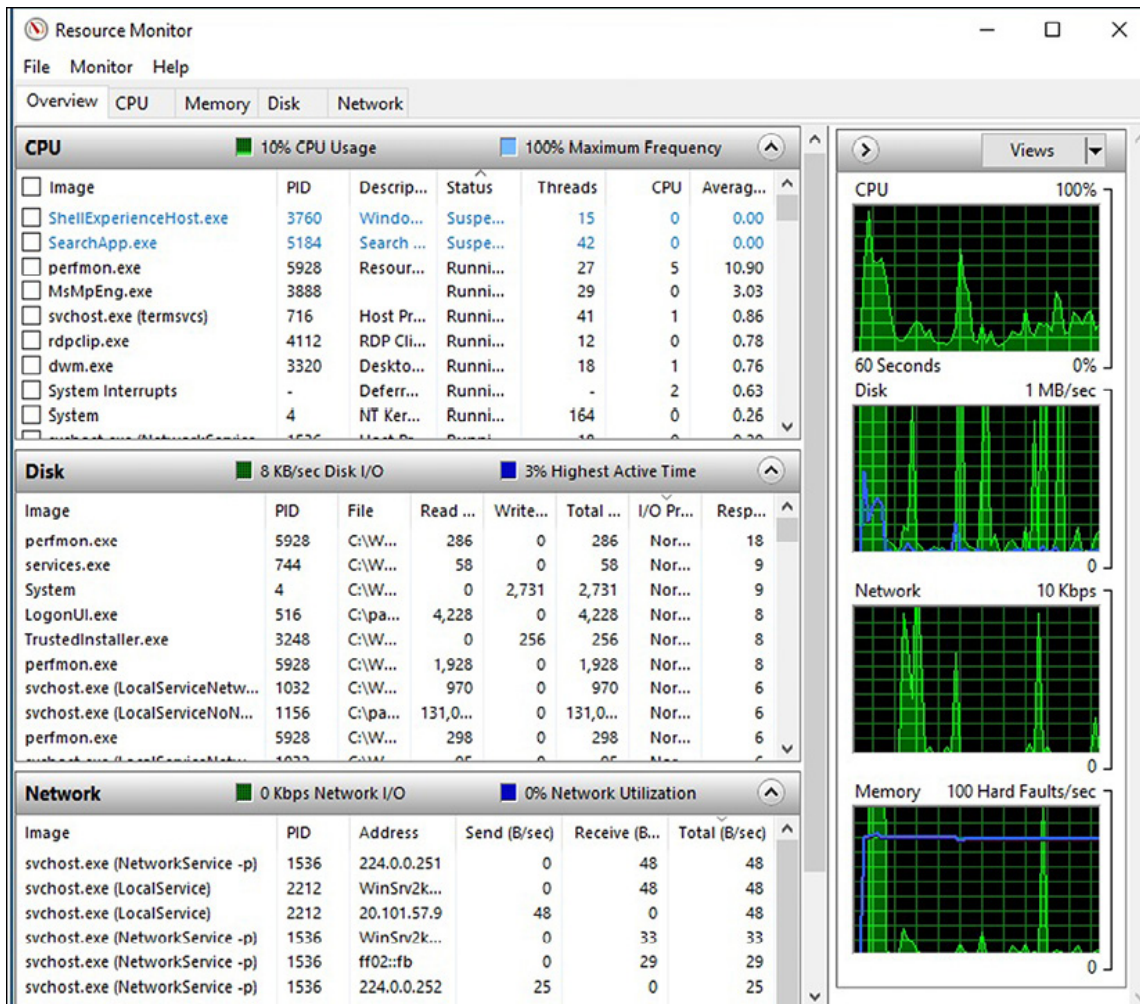
Figure 7.7: Resource monitor in Windows Server 2022

You can use the overview tab to get a quick summary of the system's resource usage or the other tabs to get more detailed information about the CPU, memory, disk, and network usage of specific processes and services. With resource monitor, you can track down performance issues and optimize your system for better performance.

Overviewing task manager

Task manager is a built-in Windows utility that allows users to monitor and manage running processes, performance, and services on a server. It provides a graphical representation in both summary and graph views, making it easy for users to understand the server's current state. In addition, Task Manager allows users

to start or stop applications and background processes. To run Task Manager on Windows Server 2022, complete the following steps:

1. Right-click the taskbar and select **Task Manager** from the **Context** menu.
2. Once launched, **the Task Manager** will display the *real-time status* of processes and services and provide various performance metrics in an easy-to-understand format, as shown in *Figure 7.8*:
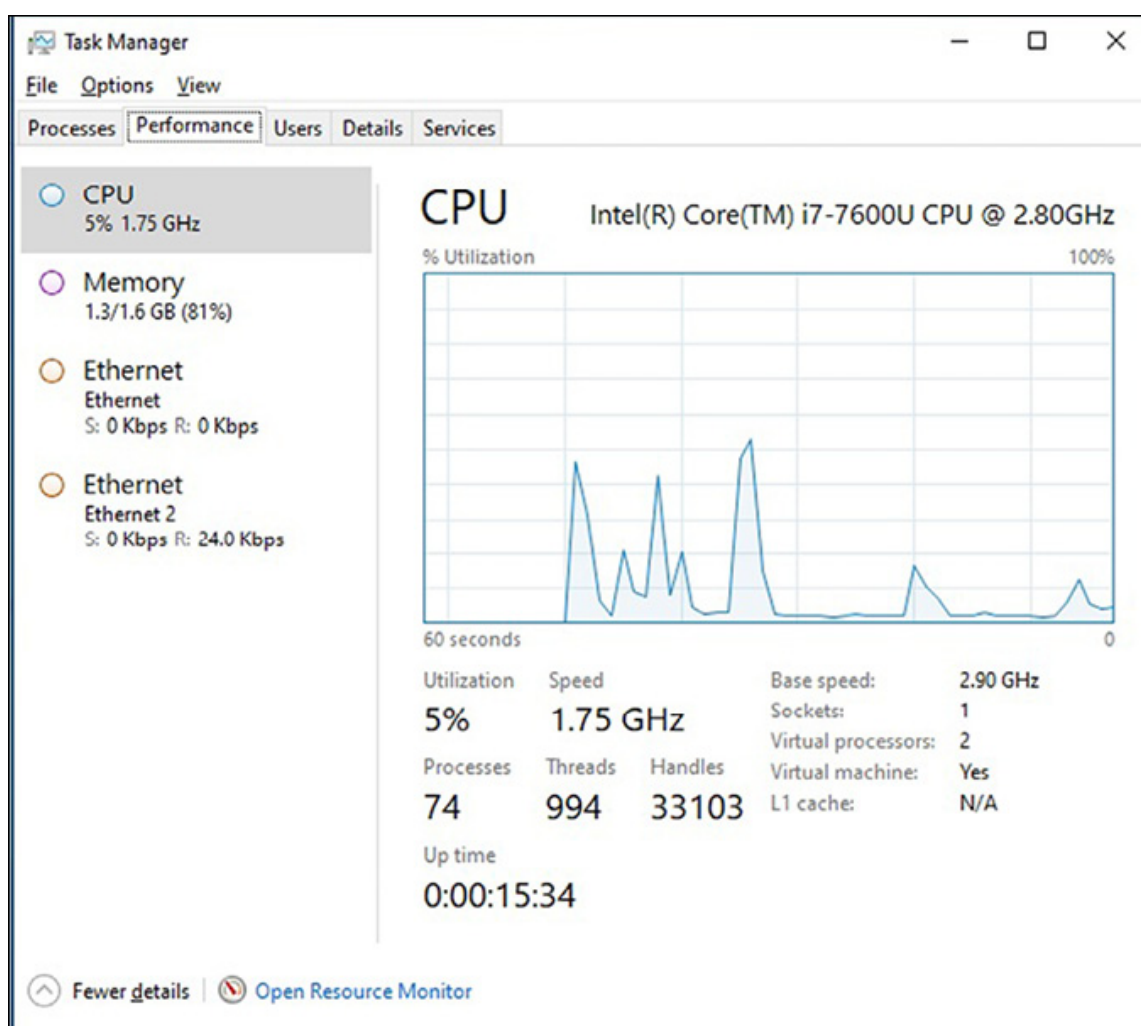
Figure 7.8: *Task Manager in Windows Server 2022*

Best practices for server maintenance

In information technology, best practices are the most effective and efficient methods for solving problems and managing policies and procedures. Therefore, accredited management standards such as ISO 9000 and ISO 14001 consider best practices a crucial feature. By following these practices, organizations can ensure that their servers run efficiently, network services are reliable, client/server applications are secure, and network infrastructures are scalable. Guidelines, in contrast, are recommendations for meeting policy standards, whereas procedures are step-by-step instructions for implementing policy components.

Note: ISO 9000 (**https://www.iso.org/iso-9001-quality-management.html**) is a set of international standards that outline the requirements for a Quality Management System (QMS). The ISO 9000 family of standards is designed to help organizations meet the needs of customers and other stakeholders while meeting statutory and regulatory requirements related to the product or service.

Note: ISO 14001 (**https://www.iso.org/iso-14001-environmental-management.html**) is a set of international standards that provide Environmental Management Systems (EMS) guidelines. The ISO 14000 family of standards is designed to help organizations minimize their environmental impact while maintaining profitability. In addition, this standard provides a framework for an organization to manage its ecological responsibilities systematically, contributing to the environmental pillar of sustainability.

Information Technology Infrastructure Library

The growing use of computer technology and networking in businesses, information, and communication technology departments in the 1980s became increasingly critical in improving productivity and efficiency. This recognition led to the development of the **Information Technology Infrastructure Library** (**ITIL**), a framework that guides IT organizations in designing, implementing, operating, and managing IT services. ITIL's best practices are presented in publications, with the latest version being ITIL v4, released in 2019 and 2020. In addition, the ITIL core books cover the fundamental concepts of ITIL, including the following:

- Service Strategy
- Service Design

- Service Transition

- Service Operation and Continual

- Service Improvement

By using ITIL, organizations can tailor their IT services to meet their business needs and become a driving force in today's economy.

Overview of Windows Admin Center

Windows Admin Center is an advanced tool designed to manage servers, which was initially known as Project Honolulu and was introduced in 2018. The tool has been continuously improved and is now available in Windows Server 2022. The software allows system administrators to manage Windows Servers on-premises and in the cloud using a Web-based interface. Windows Admin Center is a locally installed application that replaces older tools like Server Manager and Computer Management and is free to download from Microsoft's website. It is compatible with Windows Server 2022, Windows 11/10, and earlier versions of Windows Client and Windows Server.

WAC provides various tools for managing Windows servers, hyper-converged infrastructure, Windows 10 and 11 PCs, and clusters. The interface of WAC is similar to Azure cloud management, making it easier for administrators to switch between the two tools. The tools in WAC include features for managing and monitoring virtual machines, storage, networking, and security. In addition, the application allows administrators to manage on-premises and cloud servers, providing a consistent experience across different environments.

Windows Admin Center tools and features

WAC is a comprehensive solution for managing Windows servers and other devices. The application can be used remotely, and administrators can manage their Windows servers from a Web-based interface. WAC also offers various tools and features for managing and monitoring different aspects of the server infrastructure, making it easier for administrators to maintain and improve the efficiency of their systems. Some of these tools are as follows:

- **Azure Hybrid Center** is a tool that bridges on-premises infrastructure and the cloud, allowing organizations to take advantage of the cloud's benefits while maintaining their existing investments in on-premises infrastructure. It provides improved connections between on-premises servers and cloud services, including Azure Automanage, Azure Arc, Azure Backup, File Sync, Disaster Recovery, and other cloud services.

- **Azure Kubernetes Service** is a control panel for configuring a local Kubernetes group. It provides a platform that supports applications running in a cluster of containers, making it easier to work with at scale.

- **Azure Monitor** is a tool that provides a centralized platform for monitoring Azure resources and applications running on-premises or in the cloud. It offers a dashboard that displays various resources' health and performance and alerts for critical events and performance anomalies.

- **Microsoft Defender for Cloud** is a security tool that provides unified visibility, protection, and response capabilities for cloud workloads. It helps to identify and block threats across multiple platforms, including Azure, AWS, and Google Cloud.

- **Remote Desktop** is a tool that allows administrators to remotely access and manage Windows servers and desktops from a central location. It provides a secure and easy-to-use remote desktop experience for managing servers and workstations without physically being on the device.

- The **secured-core server** is a security-related feature that provides multi-layered security across hardware, firmware, and operating systems. It uses **Trusted Platform Module** (**TPM**) 2.0 and System Guard to boot Windows Server safely and minimizes the risks of firmware vulnerabilities.

- **Storage Migration Service** is a tool that simplifies the process of migrating servers to a newer version by utilizing a GUI interface and Windows PowerShell to inventory server data and transfer the configuration to the new servers.

Exercise 7.2—How to download Windows Admin Center

This exercise will guide you on how to download Windows Admin Center. Follow the given steps:

1. Open your internet browser and visit the website **https://www.microsoft.com/en-us/windows-server/windows-admin-center**.

2. On the download site, you will find a button for downloading **Windows Admin Center**, as shown in *Figure 7.9*. Click on that button to start the download process:
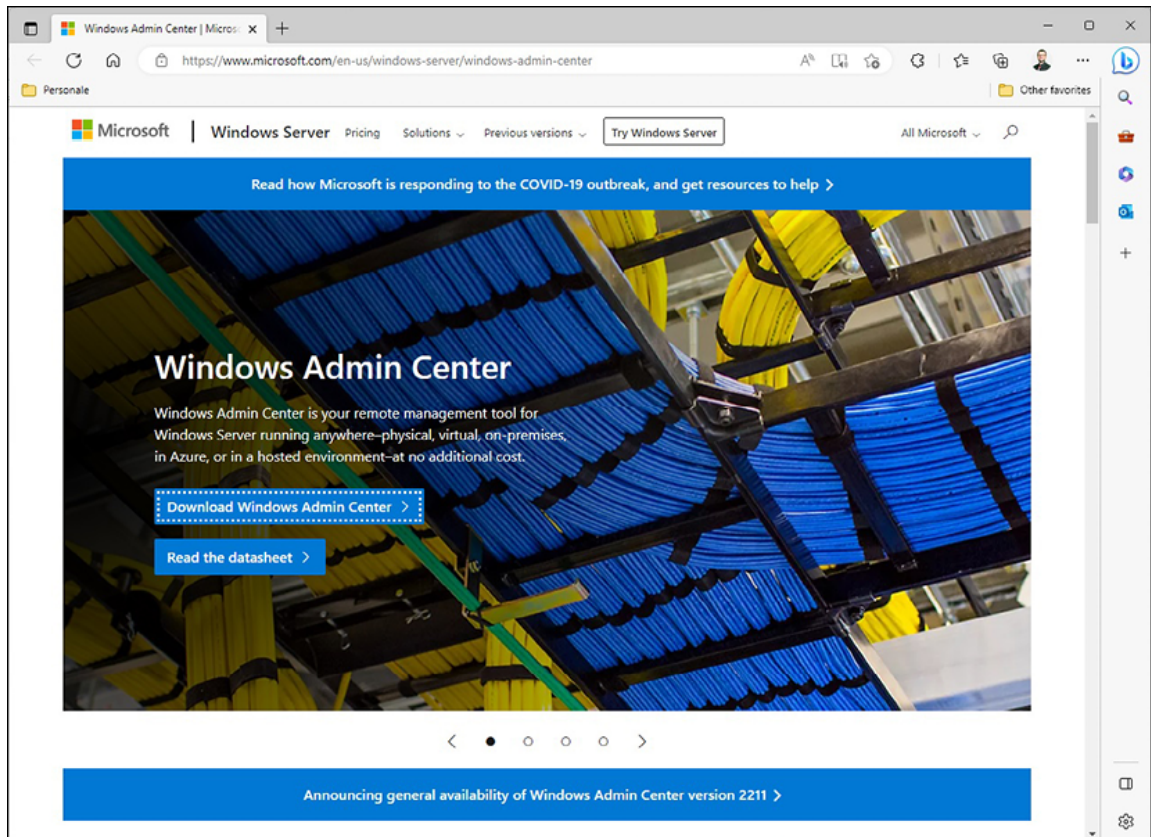
Figure 7.9: *Downloading Windows Admin Center*

Exercise 7.3—How to Install Windows Admin Center

This exercise provides instructions for installing Windows Admin Center. To do so, complete the following steps:

1. Open the downloaded file `WindowsAdminCenter2211.msi` by double-clicking on it to launch the installer.

2. Click the `Next` button in the `Windows Admin Center Setup wizard` to install.

3. Examine and approve the license terms, as shown in *Figure 7.10*, and click `Next`.
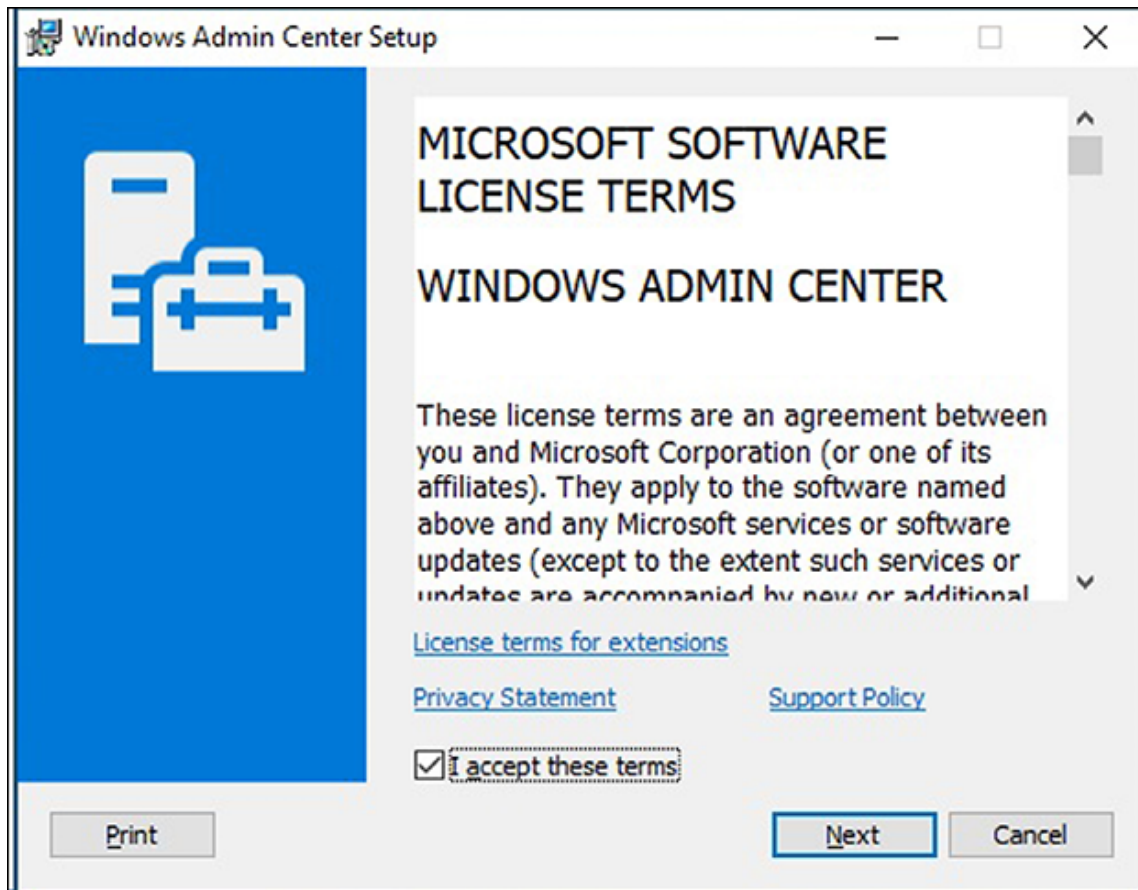
Figure 7.10: Installing Windows Admin Center

4. Choose the installation location and select **Next**.

5. Choose the **most appropriate** option on the *Send diagnostic data to Microsoft* page.

6. Select **Use Microsoft Update when I check for updates**, then click **Next**.

7. Accept the Install Windows Admin Center defaults on the **Windows Server page** and click **Next**.

8. Select the features you want to install, then click **Next**.

9. Choose between a self-signed certificate or a certificate from a certificate authority, then click **Next**.

10. Review the installation summary and click on **Install** to begin the installation process.

11. Wait for the installation to complete, then click on **Finish** to exit the setup wizard.

12. To access **Windows Admin Center**, open your Web browser and go to `https://localhost:6516`.

Exercise 7.4—How to connect to a server from the Windows Admin Center

This exercise provides instructions for connecting with a server using Windows Admin Center. To do so, complete the following steps:

1. Open **Windows Admin Center** and click the **Add** button in the top-left corner.

2. Within the **Servers** section, select the **Add** button, as shown in *Figure 7.11*:
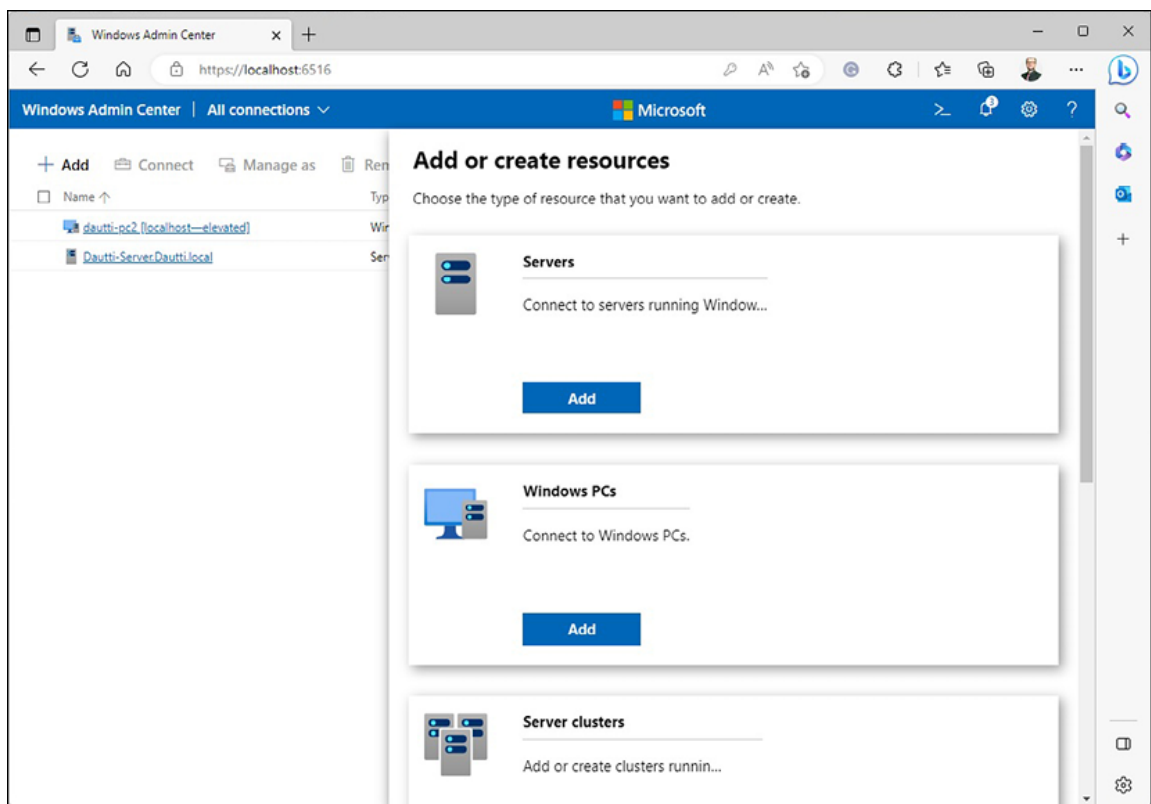
Figure 7.11: *Connecting to a server over Windows Admin Center*

3. In the **Server name** field, enter the IP address or hostname of the server you want to connect to.

4. Enter the credentials for the server you want to connect to.

5. Click the **Add** button to add the server to your list of connections.
6. Please select the server from the connections list to manage it using the **Windows Admin Center**.

Logs and alerts for server performance

The section discusses the importance of performance monitoring in maintaining the ongoing operations of a server and the dedication and patience it requires from system administrators. The correct tools, such as logs and alerts, are crucial to keeping the server running. Logs are useful for detailed analysis and record archiving, whereas alerts enable system administrators to be informed on time about occurrences, allowing them to take appropriate actions.

Performance Monitor is a tool that allows system administrators to collect performance information, log that information automatically, and set up alerts. The logged performance information can be used for analysis or exported to a spreadsheet or a more advanced analytical program for further analysis and reporting.

The recommended approach is outlined in the following section to configure performance logs and alerts in Windows Server 2022.

Exercise 7.5—Enabling performance logs and alerts service

This exercise explains starting the performance logs and alerts service in Windows Server 2022. To do so, complete the following steps:

1. Press the *Windows key + R*.
2. Type in `services.msc` and hit *Enter*.
3. Locate the **Performance Logs & Alerts** service from the list of services and check its status, as shown in *Figure 7.12*.
4. If the service is stopped, right-click on it and choose **Start**.

5. Close the `Services` window. Please refer to the following figure:
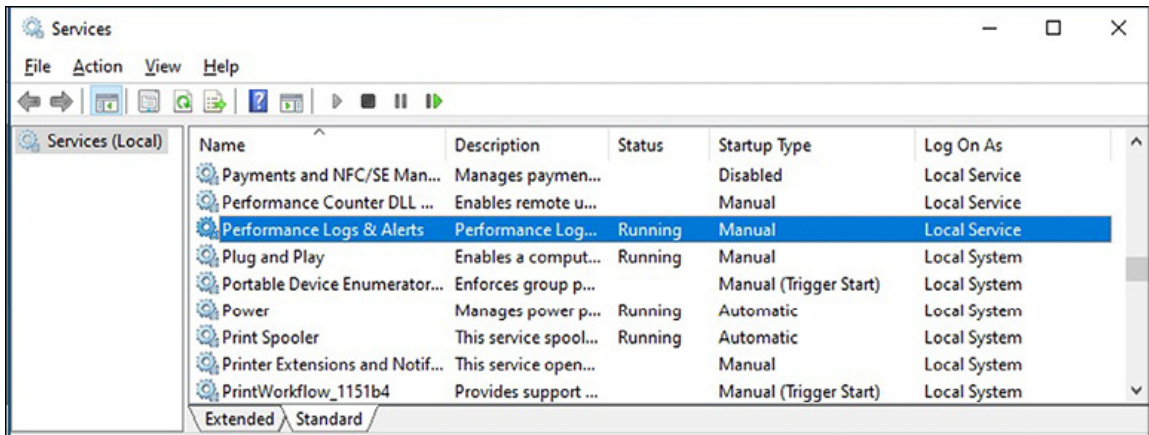
Figure 7.12: *Performance logs and alerts service in Windows Server 2022*

Exercise 7.6—Exploring the PerfLogs folder

This exercise provides steps to help you access the PerfLogs folder containing the Performance Monitor logs in Windows Server 2022. To do so, complete the following steps:

1. Press the *Windows key + R*.

2. Type `c:` and press *Enter*.

3. The `PerfLogs folder` will be displayed, as seen in *Figure 7.13*:
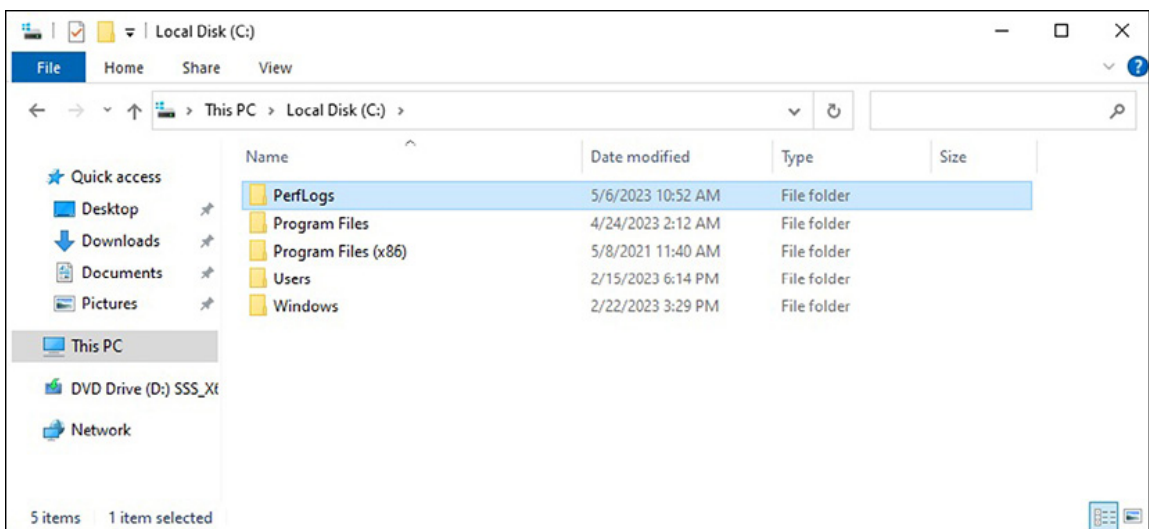
Figure 7.13: *PerfLogs folder in File Explorer of Windows Server 2022*

Exercise 7.7—Creating and configuring performance data logs

This exercise explains how to create performance data logs in Windows Server 2022. To do so, complete the following steps:

1. Expand **Data Collector Sets** and select **User Defined** in **Performance Monitor**.

2. Right-click on **User Defined** and select **New | Data Collector Set**.

3. Enter a name for the Data Collector Set.

4. Select the **Create manually (Advanced)** option and click **Next**.

5. Choose the **Create data logs** option and the performance counter sub-option, then click **Next**.

6. Click the **Add** button to add counters, as shown in *Figure 7.14*. Specify the time interval and click on **Next**.

7. Ensure that the default folder for saving data logs is the **PerfLogs folder**, and click **Next**.

8. Set the User in **Run** and select the **Start Now data collector set** option.

9. Finally, click on **Finish** to complete the process.
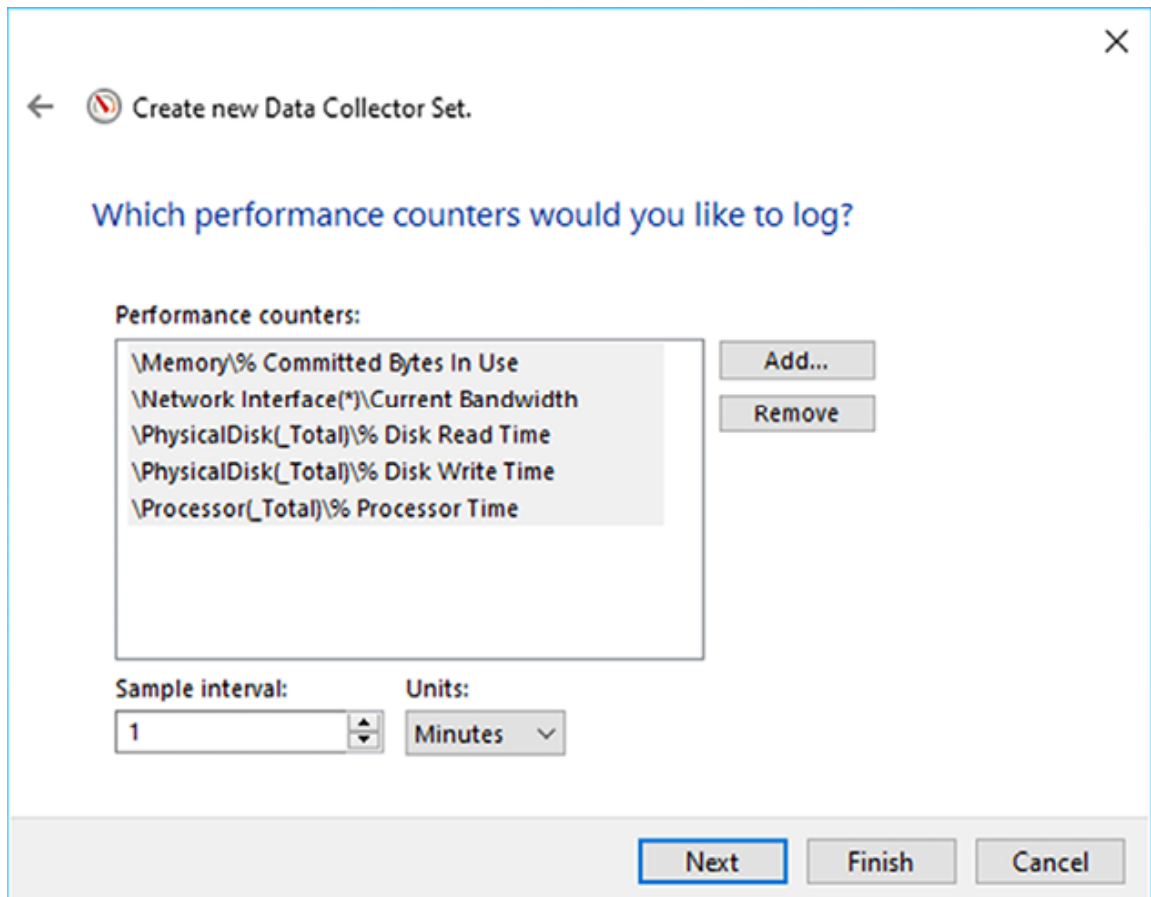
Figure 7.14: *Logging the performance counters*

Exercise 7.8—Performance counter alert configuration

This exercise provides steps to explain how to set up a performance counter alert in Windows Server 2022. To do so, complete the following steps:

1. Repeat steps 1–4 from the *Creating Performance Data Logs* section.

2. Choose **Performance Counter Alert** and click on **Next**.

3. Click on the **Add** button to add counters, specify the limit for the alert, and click on **Next**. *Figure 7.15* shows how to do this.

4. Set the User in **Run as** and select the **Start Now data collector set** option.

5. Click on **Finish** to complete the setup.

Refer to *Figure 7.15:*
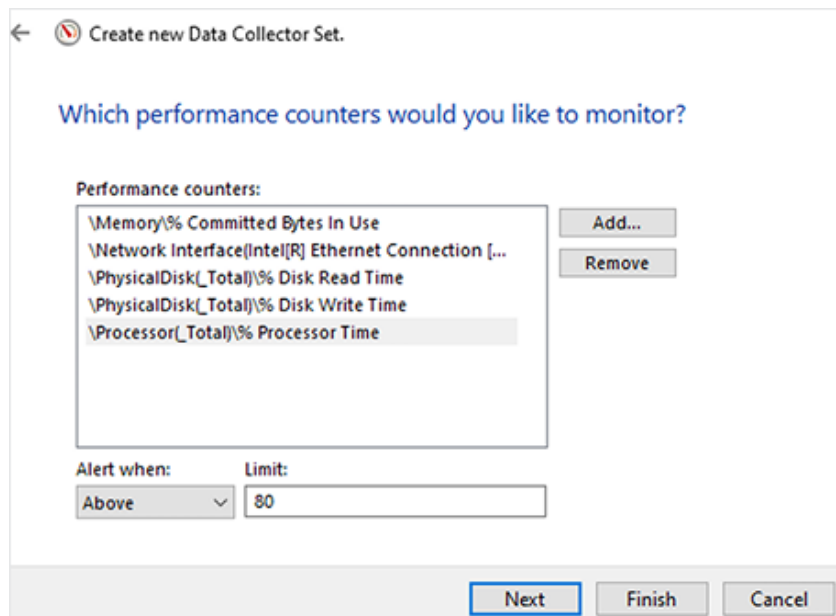
Figure 7.15: *Joining a domain using server configuration*

Conclusion

This chapter has provided detailed information about the hardware components of a server and how to maintain and monitor its performance using the native tools and utilities of Windows Server 2022. You have learned about the crucial elements of a server, such as the processor, memory, disk, and network, and how they impact the server's performance. In addition, you have been introduced to various performance monitoring tools such as Performance Monitor, Resource Monitor, Task Manager, and Performance Counters, which enable system administrators to keep track of server performance, especially hardware performance. In addition to these native tools, Windows Admin Center is another powerful tool that allows system administrators to manage and monitor servers remotely through a Web-based interface. This chapter concludes with an exercise that provides step-by-step instructions on running the performance logs and alerts service. This exercise covers starting the service, accessing the Performance Monitor logs folder, creating performance data logs, and setting up performance

counter alerts. The upcoming chapter will focus on updating and troubleshooting Windows Server 2022.

Questions

1. Which are the four main hardware components?
2. What is a Performance Monitor?
3. What is a Resource Monitor?
4. What is a Task Manager?
5. What is Windows Admin Center?

CHAPTER 8
Maintaining and Resolving Issues in Windows Server 2022

Introduction

In this chapter, you will learn about the challenging yet crucial tasks of updating and troubleshooting Windows Server 2022. As you progress through this chapter, you will discover that these tasks can be simplified and are manageable with a solid plan and strategy. Understanding the importance of troubleshooting, updating, monitoring, and maintaining servers can significantly increase the business continuity standard, which is critical to the success of any organization in the market. This chapter will cover the server startup process, advanced boot options, Safe Mode, backup and restore disaster recovery plan, and updating the Windows Server 2022, server hardware, and third-party software. It also includes a discussion on the Event Viewer, which allows you to monitor different logs on the Windows Server 2022 and troubleshoot any problems you might experience, thus reducing downtime and minimizing the financial impact on the business. By the end of this chapter, you can apply the knowledge gained to manage and monitor logs using the Event Viewer and keep your Windows Server 2022 up to date, ensuring a high business continuity standard.

Structure

In this chapter, we will cover the following topics:

- Starting up your server
- Maintaining business continuity
- Updating the OS and applications
- Troubleshooting errors and problems
- Understanding the Event Viewer

Objectives

This chapter aims to provide a comprehensive understanding of troubleshooting, updating, monitoring, and maintaining Windows Server 2022 with practical strategies to simplify and manage these essential tasks. This chapter covers server startup processes, advanced boot options, Safe Mode, backup and restore disaster recovery plans, and updating the Windows Server 2022. In addition, the Event Viewer is discussed as a valuable tool for monitoring system logs and troubleshooting errors to minimize downtime and reduce financial losses. As a result, readers will gain a solid foundation in server management and the confidence to apply this knowledge in practical settings.

Starting up your server

Understanding the hardware components and startup process is crucial for troubleshooting hardware-related problems, minimizing downtime, and ensuring a server's smooth operation. Although it may seem entirely technical, knowing how a server starts up is essential for service technicians to diagnose and troubleshoot any issues arising during startup. To grasp the server's startup process, it is necessary to start with the **Basic Input/Output System** (**BIOS**), which is responsible for initializing the hardware components and checking for errors before loading the operating system. By understanding the BIOS and how it interacts with the server's hardware, technicians can quickly diagnose and resolve any startup problems, minimizing downtime and ensuring the

server is always up and running. Therefore, it is essential to comprehensively understand of the server's hardware components and startup process for effective server management and troubleshooting. Let us now go over the various systems to understand the server's startup process:

- **Basic Input/Output System (BIOS):** When a server is turned on, the ROM chip on the motherboard activates the BIOS, as in *Figure 8.1*, to enable users to access and set up the server's hardware. BIOS controls the functionality of the server's hardware and identifies and configures hardware in the server, including identifying boot devices. Please refer to the following figure:
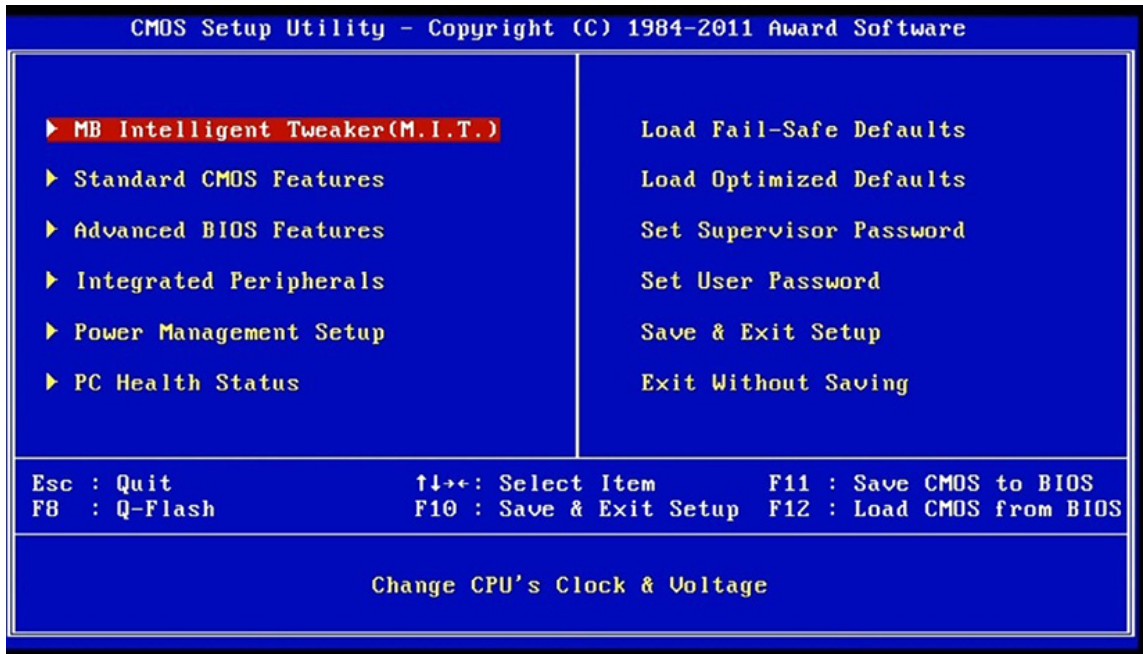
Figure 8.1: BIOS in a computer system

- **Unified Extensible Firmware Interface (UEFI):** Modern computers use UEFI instead of BIOS, as shown in Figure 8.2. UEFI supports 32-bit or 64-bit processor modes, can access the entire computer's memory, and uses **GUID Partition Table** (**GPT**) instead of **Master Boot Record** (**MBR**) to enable support for disks larger than 2 TB. In addition, UEFI can be quickly updated by downloading

firmware updates directly from the manufacturer's website. Please refer to the following figure:
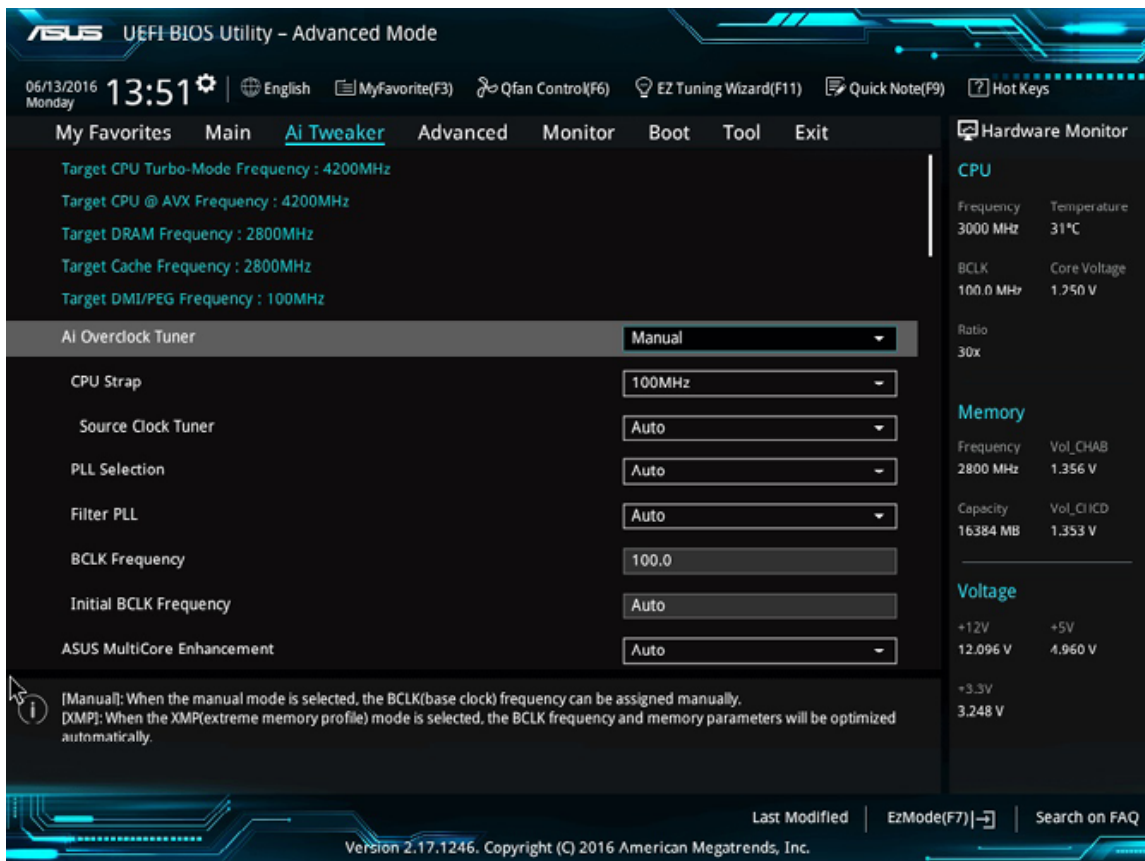
Figure 8.2: UEFI in a computer system

- **Trusted Platform Module (TPM):** As shown in *Figure 8.3*, TPM is a motherboard chip that supports disk encryption by providing hardware security for BitLocker. TPM helps ensure the integrity of early startup components by verifying that no changes were made to the BIOS, boot sector, and boot manager. Once TPM verifies that there are no changes, it releases the decryption key to the Windows OS bootloader. If TPM detects changes, it blocks any volume protected by BitLocker, and the disk will remain protected. Please refer to the following figure:
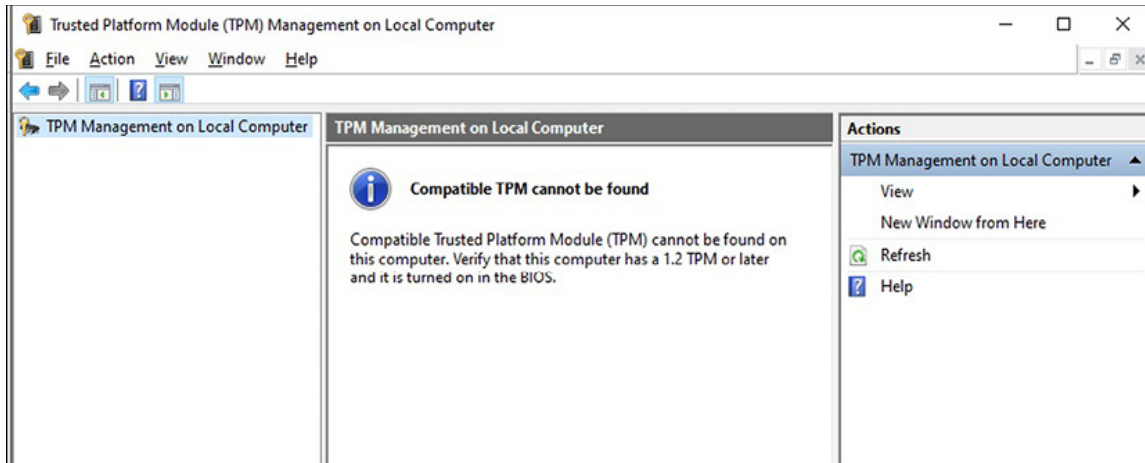
Figure 8.3: *TPM in Windows Server 2022*

- A **Power-On Self-Test** (**POST**) is a diagnostic test by BIOS when booting a server that verifies that the server hardware is working correctly. Users can learn about the POST's beeps during server hardware initialization. It is recommended that users keep an eye on the processors, memory, and graphics cards, as they are the first three components examined by a POST.

- **Master Boot Record (MBR):** BIOS hands control over the first boot device once POST verifies that the server hardware works correctly. The MBR contains the information to identify and boot the OS and is created when disk partitions are made. The MBR resides outside the disk partitions and has either **NT Loader** (**NTLDR**), **Boot Manager** (**BOOTMGR**), or both, depending on the Windows OS installed on the server's disk.

- **Boot Configuration Data** (**BCD**), as shown in *Figure 8.4*, represents a store of specific files that control an OS boot. BCD provides a standard boot option interface for the newest Windows OSes, such as Windows Vista to Windows Server 2022, independent of the firmware. In addition, BCD is more secure than the previous boot option (`Boot.ini`), enabling administrators to assign permissions to manage boot options. Please refer to the following figure:

Figure 8.4: BCDedit.exe in Windows Server 2022

- A **bootloader**, often called a bootstrap loader or boot manager, is a program that boots a computer and appears after POST verifies that the computer hardware is functional. The bootloader loads the Windows OS kernel into memory or disk. There are two types of bootloaders in Windows OSes: NTLDR for Windows NT to Windows Server 2003 and BOOTMGR for Windows Vista to Windows Server 2022.

- The boot sector is a sector on a server's disk containing the information required to boot that server. It is located in the

first disk track's first sector and usually has the MBR, which includes the bootloader. Tracks look like concentric circles on a disk, and there are many on a disk, whereas sectors are the track's divisions, and their size depends on the file system the server's OS is running.

- **Boot menu:** When multiple Windows OSes are running on a computer, it is called multi-booting, and the computer displays a boot list that lists all OSes running on it every time it is turned on. The `boot.ini` file displays the boot menu and is located inside the disk partitions, precisely at the root partition (the C: partition). The path to `boot.ini` is `C:\boot.ini`, containing boot options such as bootloader and the OS. In post-Vista OSes, the equivalent of boot.ini is BCD.

- **Safe Mode:** Safe Mode is a diagnostic mode in Windows OSes that uses a minimal set of drivers and services, and it represents a way to boot the OS when users experience malfunctions. Pressing the *F8* key allows the Windows Advanced Options Menu to be accessed from where the Safe Mode option can be selected. Note that the F8 key option can only be used in pre-Vista Windows OSes. In post-Vista Windows OSes, such as Windows Vista to Windows Server 2022, Advanced Startup Options enables Windows OS recovery, including access to the Safe Mode.

Maintaining business continuity

As a system administrator in today's technology-driven world, it is crucial to recognize that downtime can lead to financial loss for the company. Hence, your primary duty is to minimize potential downtime as much as possible. To achieve this, you must assess the components susceptible to failure and take necessary actions to prevent such losses. By identifying the potential points of failure and taking proactive measures, you can minimize downtime and ensure the system runs smoothly. As a result, you will help the company maximize its productivity and reduce the losses caused by system failures.

Overview of Disaster Recovery Plan

A **Disaster Recovery Plan** (**DRP**) is a well-structured plan that ensures a company can continue to provide services or recover from a disastrous situation as soon as possible. Unexpected events cannot always be prevented, but losses can be minimized if a business is prepared. A DRP is a proactive method for maintaining business continuity in such situations.

To compile a DRP, organizations should consider several factors, including the following:

- Making an inventory of all hardware and software.
- Analyzing potential threats and vulnerabilities.
- Establishing priorities.
- Defining tolerance in case of a disaster.
- Reviewing past disaster handling.
- Acknowledging the importance of staff.
- Executing DRP DRY tests regularly.
- Having management approve the DRP.
- Update the DRP regularly.

By following the preceding steps, organizations can ensure they are adequately prepared for unexpected events, reducing the risk of significant losses in case of a disaster. In addition, system administrators play a vital role in implementing and executing the DRP, as they are responsible for the smooth operation of the organization's IT infrastructure.

Understanding data redundancy

Data redundancy is a method that stores comparable data in several locations and is updated automatically. However, what if these updates do not occur successfully? That can result in data inconsistency problems, leading to even more severe issues, such as data integrity problems. These issues can further exacerbate the situation, potentially harming an organization's extensive data and multiple storage locations. Therefore, it is crucial to ensure data redundancy processes are carefully implemented and monitored to avoid such issues. In addition, organizations should

have contingency plans to handle any potential data consistency or integrity issues that may arise.

Getting to know clustering

Clustering is a technique used to achieve high availability of services by combining the power of multiple servers. By merging processor power, RAM, storage capacity, and network interfaces, a group of servers works together to provide uninterrupted services. There are two common types of clustering given as follows:

- **Failover clustering** is typically used for backend processing environments such as databases and mail servers. It requires a minimum of two servers and works on the active-passive principle, where one server is active, and the other is passive.

- **Load-balancing clustering** is used for front-end processing environments such as Web servers. It also requires a minimum of two servers, but the servers are merged into a virtual server, and loads are distributed between them.

As far as users are concerned, they access a single server, but in reality, the loads are distributed between the servers. Using clustering, businesses can ensure that their services are always available to users, even if one or more servers fail.

What is folder redirection?

Folder redirection is a feature that allows system administrators to move a local computer or shared folder on a network to a new location. This feature can help make the data stored on the server easily accessible to users, just as it would be if kept on a local computer. For example, when a user saves data in a redirected folder, the data is automatically stored in the designated network location rather than the local computer. Folder redirection can also improve data security by storing essential files on a secure network rather than single computers.

Exercise 8.1—Group policy folder redirection setup

This exercise explains setting up a **Group Policy Object** (**GPO**) in Windows Server 2022 to redirect a folder. To do so, complete the following steps:

1. Press the *Windows key + R*, enter `gpmc.msc`, and press *Enter* to access the **Group Policy Management Console**.

2. Expand **User Configuration**, then **Policies**, then **Windows Settings**, and finally, **Folder Redirection**.

3. Right-click on the **Documents** folder and choose **Properties** from the menu.

4. Select the **Basic - Redirect** everyone's folder to the same location setting, as shown in *Figure 8.5*.

5. In the **Target** folder location section, choose **Redirect to the following Location**.

6. Enter the root path to your redirected folder.

7. Click **OK** to close the **Document Properties** window and complete the folder redirection process. Please refer to the following figure:
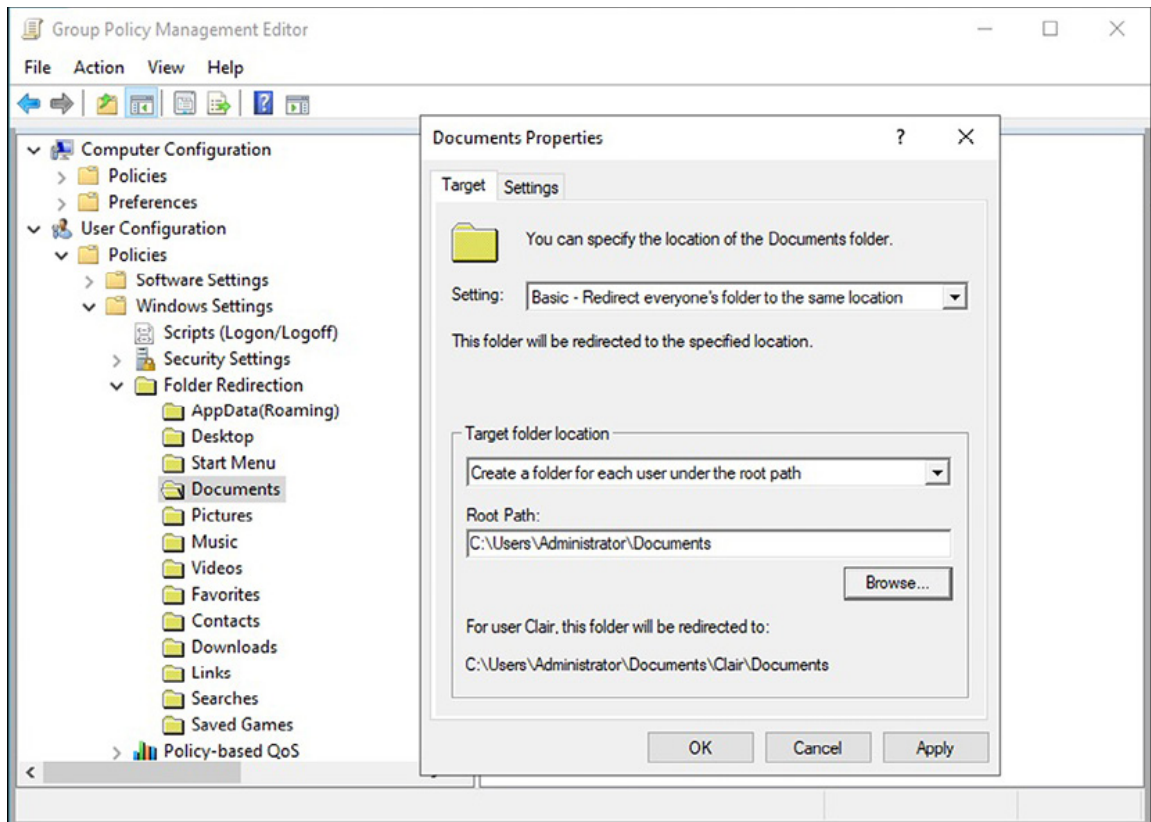
Figure 8.5: *Group Policy folder redirection setup in Windows Server 2022*

Overview of backup and restore

Protecting data on servers from loss is a crucial requirement for system administrators. Backups are the primary way of copying data in case of failure. However, restoring data is recovering lost or corrupted data on a server. Different types of backups that can be used are as follows:

- **Full backup:** This type of backup creates a copy of all data. To restore data, only the last set of complete backups is needed.

- **Incremental backup:** This backup copies data that has changed since the last backup, regardless of type. Typically, incremental backups are performed from Monday to Thursday, with a full backup on Friday. To restore data, the last set of full backups and incremental backups between the full backup and the desired day must be used. This type

of backup takes less time to do but more time to restore data.

- **Differential backup:** This backup copies data that has changed since the last full backup. It is similar to an incremental backup, with differential backups done from Monday to Thursday, followed by a full backup on Friday. The last full and incremental backups must be used to restore data. This type of backup takes more time to do but less time to restore data.

When selecting a backup media, it usually depends on the data's importance and quantity. CDs, DVDs, removable HDDs, backup tapes, **Network-Attached Storage** (**NAS**), and **Storage Area Networks** (**SAN**) are potential backup storage technologies. Online backup services are also used by organizations these days. Convenience, security, and cost are critical factors when selecting online backup services. Finally, the **Grandfather-Father-Son** (**GFS**) backup rotation scheme is the most common. The son backup is performed daily, the father backup is performed weekly, and the grandfather backup is performed monthly.

Exercise 8.2— How to add the Windows Server backup feature?

This exercise explains adding the Windows Server Backup feature to Windows Server 2022 using Server Manager. To do so, complete the following steps:

1. Open the **Run** dialog box by pressing the *Windows key + R*, type in `servermanager.exe`, and press *Enter*.
2. From the **Server Manager** console, select **Add Roles and Features**.
3. In the **Before You Begin** option, click on **Next**.
4. In the **Installation Type** step, select **Role-based or feature-based installation**.
5. Select a server from the server pool in the **Server Selection** option and click **Next**.
6. Skip the **Server Roles** step by clicking on **Next**.

7. In the **Features** step, scroll down the list, select **Windows Server Backup** (refer to *Figure 8.6*), and click **Next**.

8. In the **Confirmation** option, click on **Install**.

9. Click **Close** to exit the **Add Roles and Features Wizard** after the installation.
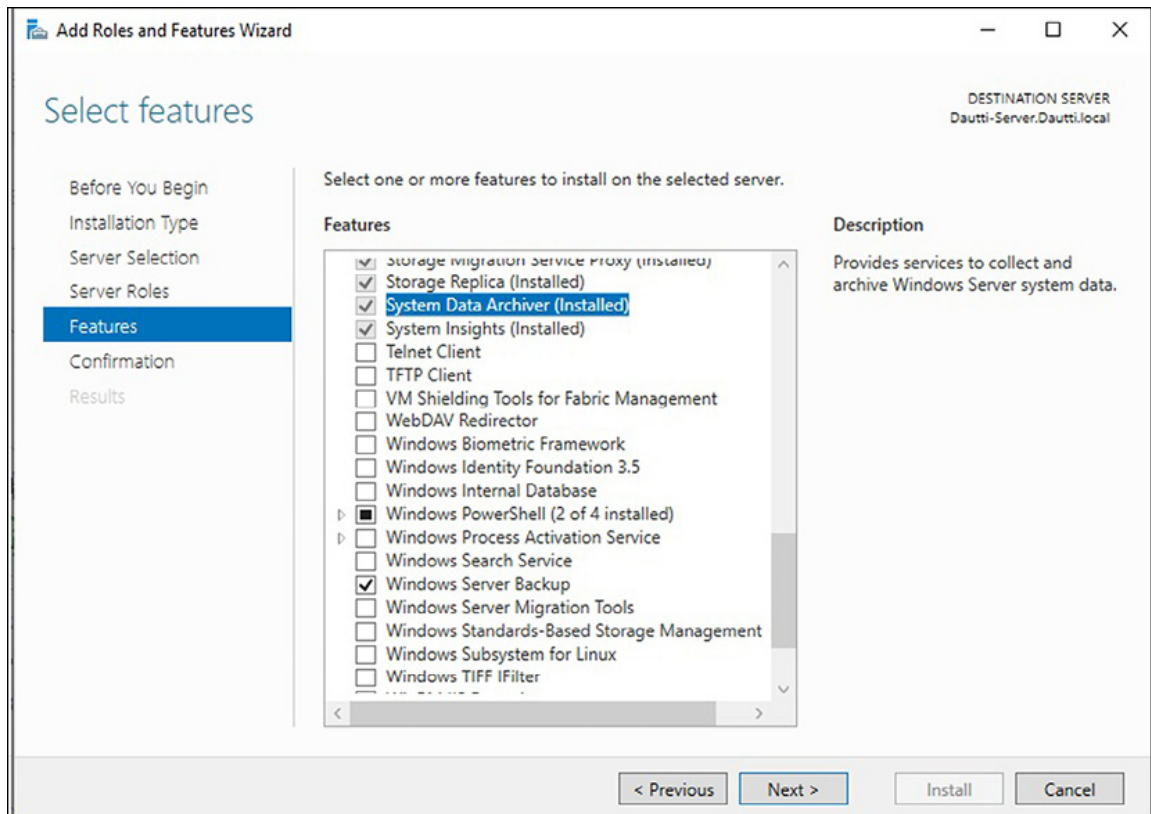
Figure 8.6: Adding Windows Server Backup feature in Windows Server 2022 using Server Manager

Understanding Directory Services Restore Mode

During the AD DS configuration wizard, you will be asked to provide a **Directory Services Restore Mode** (**DSRM)** password required for AD restore. Like Safe Mode in the OS, DSRM is used to restore AD when it fails or needs fixing. The following are the two methods that exist for restoring data replicated on a **Domain Controller** (**DC**):

- The first method involves reinstalling the OS, reconfiguring the DC, and allowing normal replication to populate the DC

from a second DC on the network.

- The second method uses a backup to restore the DC's replicated data.

The replicated data from a backup medium can be restored through either a non-authoritative or authoritative restore.

- A non-authoritative restore is applied when a DC has failed due to hardware or software problems. The AD structure is restored from a backup medium and populated from the second DC on the network through normal replication.

- An authoritative restore occurs after a non-authoritative restore and helps restore the entire system to a state before the AD objects are deleted. This method uses the `Ntdsutil` command to enable an authoritative restore of AD.

Overview of Uninterruptible Power Supply

The power supply is a critical component of any server's infrastructure, regardless of its processing power, memory capacity, or data storage capacity. Without a stable power supply, the server becomes useless. An **Uninterruptible Power Supply (UPS)** device ensures that a server always has a steady power supply. A UPS is a battery-powered device that gives the server power during a power outage. However, UPS devices are not capable of supplying power for extended periods. In such cases, electric generators can be an alternative solution to overcome the issue of power outages. Therefore, having a UPS and a generator for mission-critical servers that cannot afford downtime is crucial.

Updating the OS and applications

After installing Windows OS, it is essential to check for any new updates using the Windows Update service. That is recommended to protect the system from malicious attacks and to resolve any issues and bugs in the operating system. Windows Server 2022 is no exception, and it is necessary to update it to enhance its features, add new ones, and download driver updates for specific hardware. By updating the operating system, users can keep it secure and maintain its stability. Therefore, it is one of the most

critical activities that should be performed after installing the operating system on a new or used server.

What is a Windows update?

Microsoft releases new updates on the second Tuesday of each month, also known as *Patch Tuesday*. These updates include the latest features, security updates, and fixes for Microsoft OSes and programs, including Windows Server 2022. The updates are distributed through Microsoft's Windows update server, accessed via the Windows update feature or their official website. In addition, users will receive notifications about available updates in the system tray and Notification Center.

To access the update and security settings in Windows Server 2022, users can follow the same process as in Windows Server 2019. However, the Windows Update page, as shown in *Figure 8.7*, has slight changes in theme and options. The options include the following:

- Pausing updates for seven days
- Setting up active hours to prevent automatic restarts during operational hours
- Viewing updated history and statuses
- Choosing how updates are installed

Please refer to the following figure:
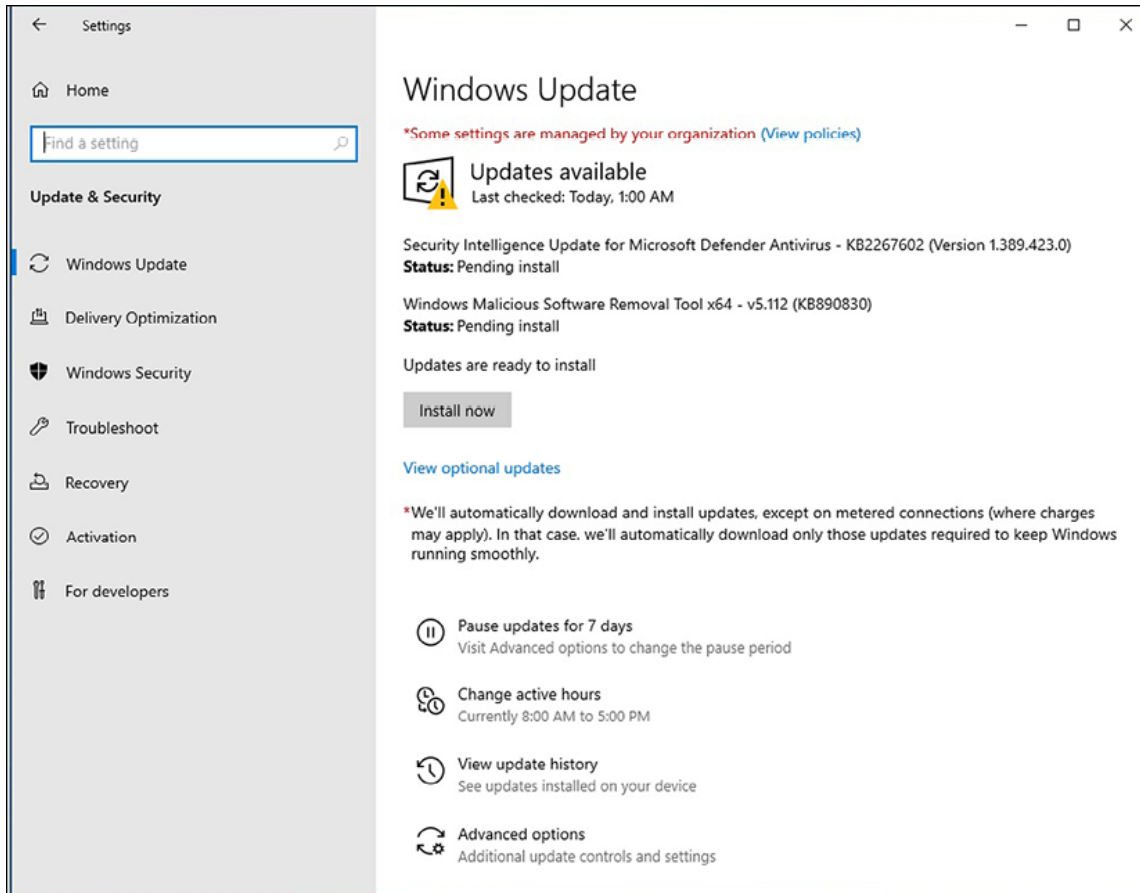
Figure 8.7: *Windows update page in Windows Server 2022*

Users can receive updates for other Microsoft products when updating Windows or defer feature updates. However, it is recommended to install updates regularly to keep the system protected, resolve issues and bugs, and add new features and enhancements.

How do you update Microsoft programs?

Using and updating Microsoft programs, shown in *Figure 8.8*, is typical on a Windows Server 2022-powered server. Some examples of client/server programs include Microsoft Exchange, SQL Server, and SharePoint. These programs are used for specific purposes like e-mail, database, and collaboration servers. Therefore, updating these Microsoft programs regularly is essential to ensure optimal performance and security. Please refer to the following figure:
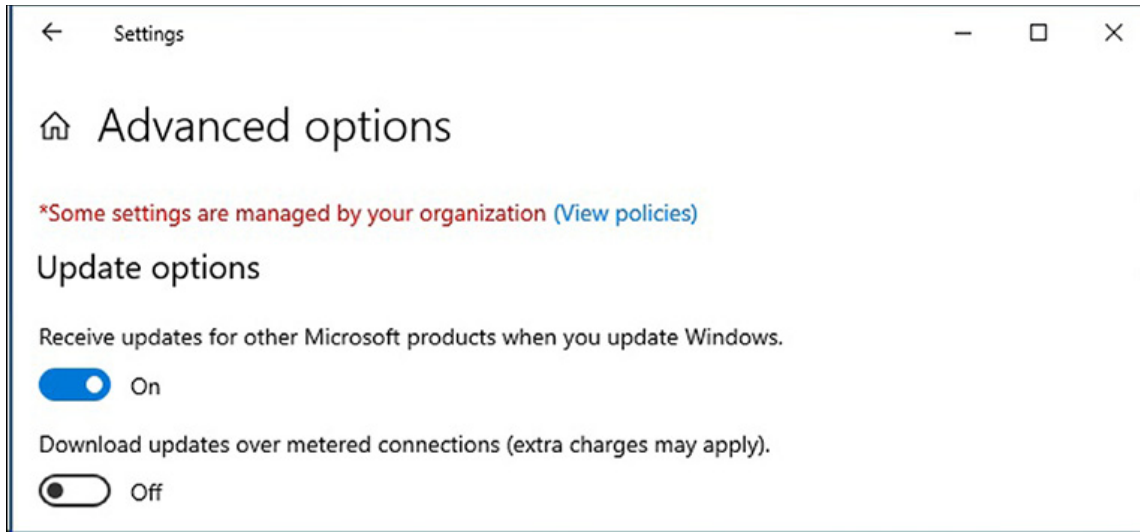
Figure 8.8: *Updating Microsoft programs in Windows Server 2022*

The importance of updating non-Microsoft programs

There is considerable importance in updating third-party programs running on a server powered by Windows Server 2022, in addition to Microsoft programs. Examples of such programs include Oracle database, Apache Web server, and VMware ESXi. The article highlights that while Microsoft programs are usually updated through the Windows update feature, updating third-party programs can differ. That is because each software company has its unique way of developing software, which means the procedure for updating such software can also be unique. As such, system administrators need to understand the differences between updating Microsoft programs and third-party programs to ensure the server runs smoothly and securely. Regular updates to third-party programs can help improve performance, address vulnerabilities, and ensure compatibility with the latest OS updates.

Getting to know Windows Server Update Services

Windows Server Update Services (**WSUS**) is the successor to **Software Update Services** (**SUS**). WSUS, as shown in *Figure 8.9*, enables system administrators to regulate the distribution of Microsoft's product updates to their organization's computers. The infrastructure of WSUS downloads updates, patches, and

fixes to an organization's server, which then approves and distributes the updates to other organizations' computers. Using WSUS, system administrators can approve or cancel updates, schedule the installation of updates on a particular date, and generate reports to determine which updates are required for each computer. Furthermore, the organization's computers no longer need to refer to Microsoft updates because WSUS provides the updates.

Refer to *Figure 8.9:*
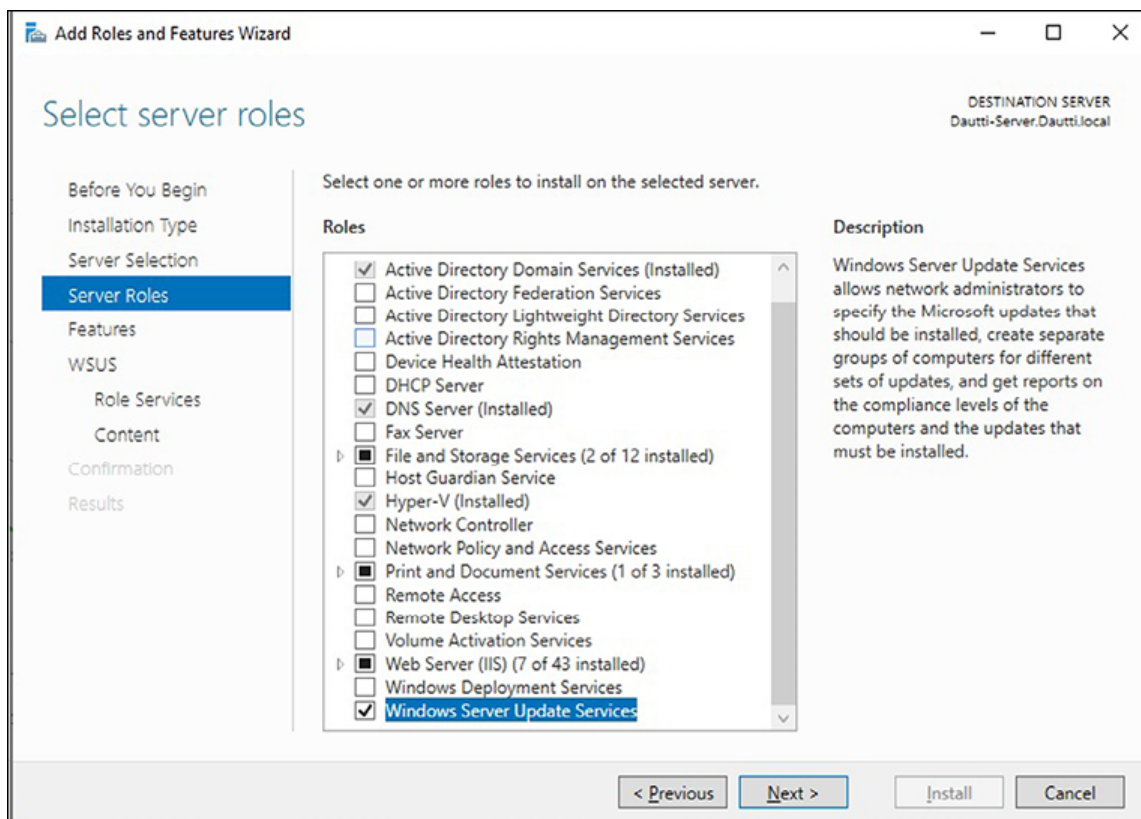
Figure 8.9: *Adding WSUS in Windows Server 2022*

Troubleshooting errors and problems

Troubleshooting is a crucial skill that requires practice and experience to master. Whenever an IT problem is solved, it enhances the problem solver's confidence and knowledge base. Thus, learning and practicing troubleshooting is crucial to building

proficiency. By refining their mastery, IT professionals can increase their chances of effectively solving problems.

Understanding troubleshooting process

As mentioned in the previous section, troubleshooting is an important task that server technicians must master. To help with this, CompTIA has developed a six-step troubleshooting model that is widely used, including by Microsoft product support service engineers. These steps involve the following:

- Discovering the problem by gathering technical information
- Evaluating system configuration by asking questions about recent changes
- Listing and tracking possible solutions
- Executing a plan and having a backup plan
- Checking the results
- Taking a proactive approach by documenting changes made during the troubleshooting process

By following the preceding steps, technicians can effectively and efficiently troubleshoot server problems, increasing their chances of successfully resolving issues.

Understanding troubleshooting approaches

The success of the troubleshooting process relies on the approach taken to solve the problem. Let us go over the two methods of troubleshooting—the systematic approach and the specific approach:

- The systematic approach involves structured steps toward solving the problem. This approach is an effective troubleshooting methodology that can be applied to any situation. The systematic approach consists of identifying the problem, gathering information about the issue, analyzing the data, developing a plan, executing the plan, and verifying the results.

- The specific approach is based on prior knowledge and experience in solving the same or similar problems. This approach involves using guesswork and intuition to diagnose and solve the problem. The specific approach is practical when dealing with issues encountered before or when the technician has expertise within the particular area.

It is important to note that both approaches have advantages and disadvantages, and the chosen approach will depend on the specific problem and the technician's expertise.

Understanding troubleshooting procedures

Troubleshooting requires expertise, experience, and a logical approach to problem-solving. Therefore, server technicians must follow specific guidelines and procedures to troubleshoot issues with computers and servers effectively. Some techniques that need to be considered include the following:

- Checking documentation
- Reviewing logs and event viewer
- Searching through knowledge-based articles
- Using utility programs

These utility programs include the following:

- Advanced Boot Options menu
- Windows Repair
- Memory Diagnostics
- System Information
- Device Manager
- Task Manager
- Performance Monitor
- Resource Monitor
- Event Viewer

These programs can help diagnose and solve issues with the server. Ultimately, the success of the troubleshooting process depends on the technician's ability to be organized, systematic, and efficient in their problem-solving approach.

Understanding the Event Viewer

The Event Viewer is a tool in the Windows operating system that allows system administrators to monitor server events. It is a valuable source of information for troubleshooting software, hardware, and network-related issues that impact the server. However, it is essential to note that even a properly functioning system can show various warnings and errors in the Event Viewer. Experienced system administrators are already aware of this fact. Therefore, the system administrator needs to understand the tool and when it can be helpful. Five types of logs can be monitored with Event Viewer: Application, Security, Setup, System, and Forwarded Events, explained as follows:

- The **Application** log tracks events related to applications or programs.

- The **Security** log tracks security-related events, such as invalid login attempts or denied folder access.

- The **Setup** log tracks application setup events.

- The **System** log tracks events triggered by Windows system components.

- The **Forwarded Events** log tracks events triggered by remote computers. To use the Forwarded Events log, you must create an event subscription.

Exercise 8.3—Central Monitoring Configuration

This exercise explains the steps for centralized monitoring on Windows Server 2022. To do so, complete the following steps:

1. Launch the command prompt as an administrator on a remote server and enter `winrm quickconfig` to grant administrative rights to local users remotely.

2. Right-click on the *Start* button and select **Computer Management**.

3. Expand **Local Users and Groups** and click on **Groups**.

4. Add the **central server** to the **administrator's group**.

5. Launch the command prompt as an administrator on the central server and enter **wecutil qc**.

6. Press **Y** when prompted to confirm the action.

7. Open **Event Viewer** by entering **eventvwr.exe** in the command prompt.

8. Right-click on **Subscriptions** and select **Create Subscription…**

9. Enter the **subscription name** and **description**.

10. Select **Forwarded Events** as the destination log.

11. Click on the **Select Computers** button to choose the remote server.

12. In the **Subscription Properties** window, click **Select Events…** and **Edit**.

13. Set the **event log filtering criteria** in the **Query Filter** window.

14. Click on **Advanced…** to make sure the machine account is selected.

15. Click on **OK** to complete the subscription setup.

    Refer to *Figure 8.10:*
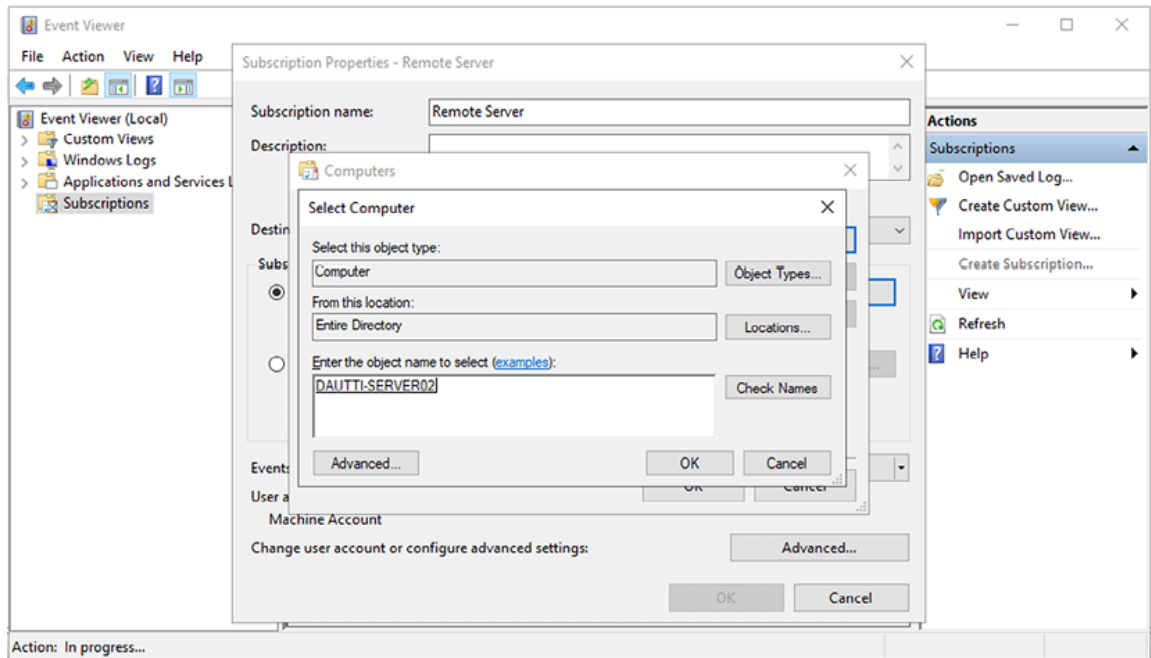
Figure 8.10: *Central monitoring configuration over Event Viewer*

Exercise 8.4—Event Viewer log filtering

This exercise provides steps to filter the Event Viewer logs in Windows Server 2022. To do so, complete the following:

1. Press the *Windows key + R*, type `eventvwr.msc,` and press *Enter*.

2. Choose the type of log you want to filter from the expanded `Windows Logs` section.

3. Click on the `Filter Current Log…` option in the `Actions` pane, as shown in *Figure 8.11*.

4. Set the filtering criteria in the `Filter Current Log` window to get the desired results.

5. Click on `OK` to close the `Filter Current Log` window.
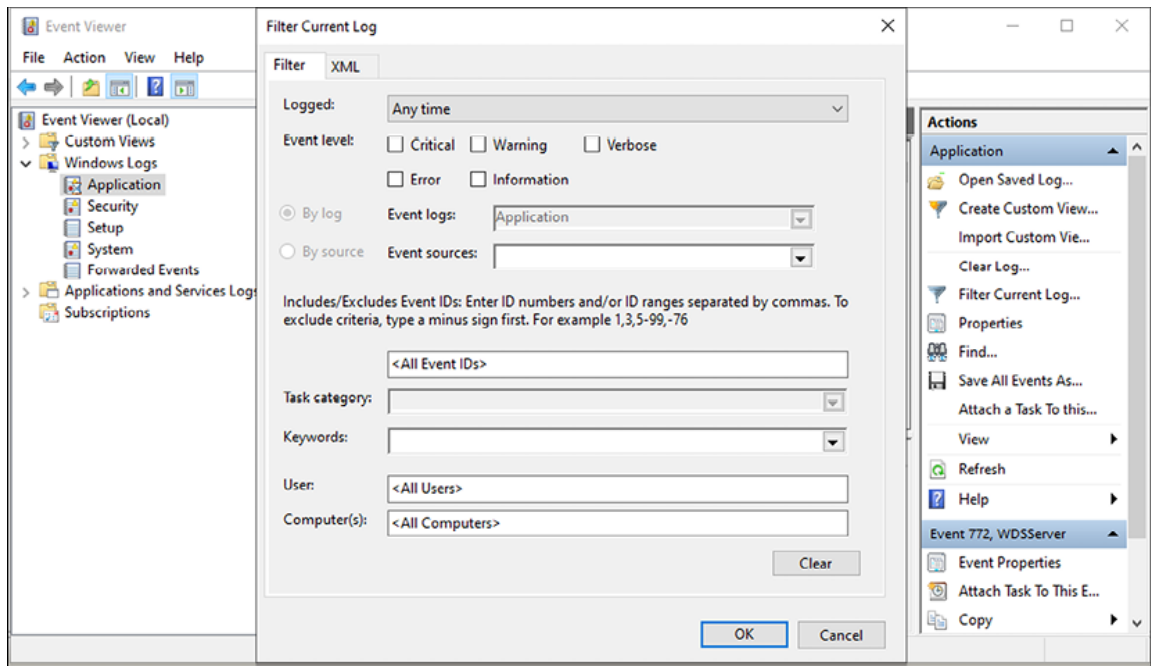
Figure 8.11: *Event Viewer log filtering*

Exercise 8.5—Log location configuration

This exercise provides explanations to change the default location of logs in Windows Server 2022. To do so, complete the following:

1. Press the *Windows key + R*, type `regedit`, and press *Enter* to open the **Registry Editor**.

2. Navigate   to `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EventLog\System.`

3. Double-click on the `File` value, which is located inside the `System` folder.

4. Enter the new path to save the log files in the **Value data** text box, then click `OK`.

5. If you want to change the default location of application logs,   navigate   to `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EventLog\Application.`

6. If you want to change the default location of security logs, navigate   to

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EventLog\Secur
ity.
```

7. After making the desired changes, close the `Registry Editor` window.

Refer to the following figure:
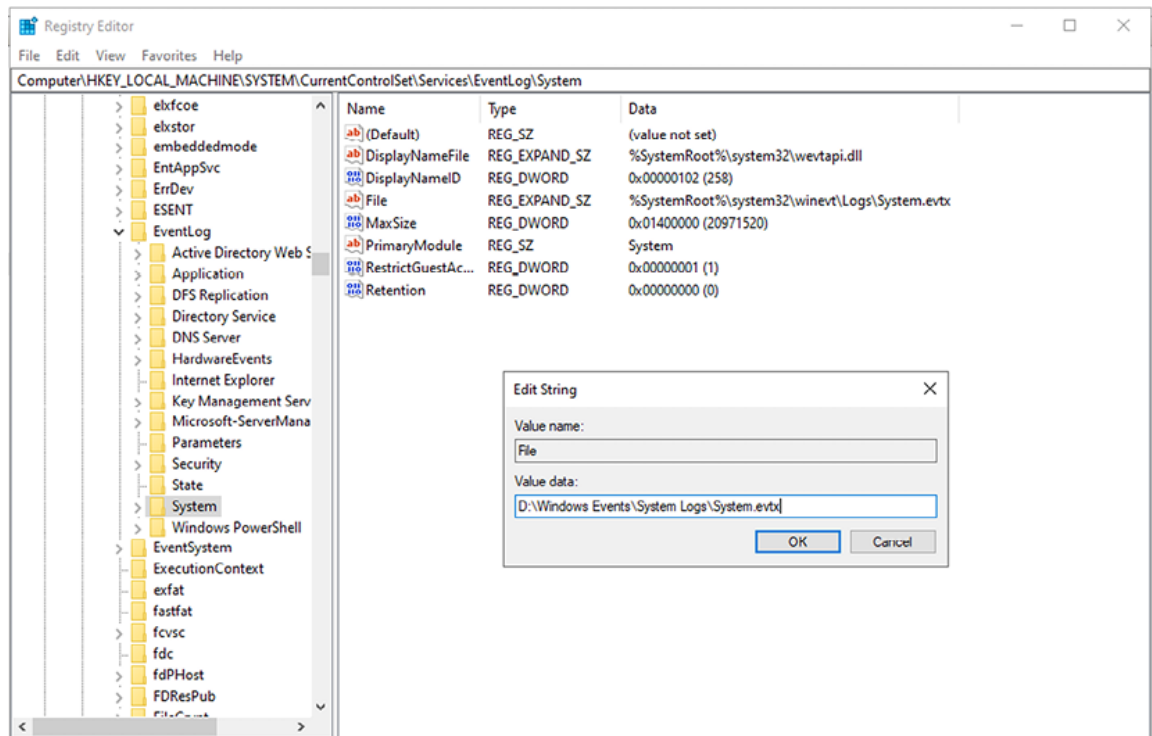
Figure 8.12: Log location configuration

Conclusion

This chapter teaches the reader about updating and troubleshooting Windows Server 2022. First, the chapter provided information on updating the server, including adding new features and enhancing security. It also introduced you to various troubleshooting methodologies that could help resolve issues that may arise. In addition, you learned about the technologies that could add redundancy to the server, ensuring its high availability and reliability. This chapter concluded with an exercise that explained how to use the Event Viewer to monitor and manage logs. This tool could help you identify and diagnose issues that

occurred on the server, making it easier to take corrective actions.

In the upcoming chapter, you will learn about studying and preparing for the Microsoft certification exam. This certification could help validate your skills and knowledge in Windows Server 2022, making you more marketable in the IT industry.

Questions

1. What is the startup process?
2. How is business continuity maintained?
3. What is a Windows Update?
4. What is troubleshooting?
5. What is Event Viewer?

Join our book's Discord space

Join the book's Discord Workspace for Latest updates, Offers, Tech happenings around the world, New Release and Sessions with the Authors:

https://discord.bpbonline.com

Getting Ready for Microsoft Certifications

Introduction

This chapter aims to give you a comprehensive understanding of Microsoft certifications. It covers the basics of certificates and certifications and delves into what it takes to pass the certification exam. You will also find practical tips and advice for preparing for the exam day. By reading this chapter, you will have access to valuable resources to help you get informed about Microsoft certifications and the steps required to succeed in the certification exam. With the proper preparation, you will be equipped with the necessary skills to overcome obstacles and become a **Microsoft Certified Professional** (**MCP**). This certification can open doors to a successful career in the field, and this chapter will help you on your journey to achieving that goal.

Structure

In this chapter, we will cover the following topics:

- What is Microsoft certification?
- Understanding Microsoft role-based certifications
- Who should take the Microsoft certification exam?

- Skills measured in the Microsoft certification exam

- What to expect and how to succeed in the Microsoft certification exam

- Preparing for the Microsoft certification exam

- How to register for the Microsoft certification exam

- On the day of your Microsoft certification exam

- New Microsoft certification validity and renewal requirements

Objectives

This chapter aims to provide readers with a comprehensive understanding of Microsoft certifications, including the basics of certificates and certifications, the specific skills measured in the certification exam, and practical tips for exam preparation. In addition, this chapter aims to equip readers with the necessary resources to succeed in the certification exam and become a **Microsoft Certified Professional** (**MCP**). The ultimate goal is to help readers open doors to a successful career in Microsoft technologies.

What is Microsoft certification?

Microsoft certifications, as shown in *Figure 9.1*, are highly valued in the IT industry and are recognized worldwide to prove one's skills and knowledge in a specific technology area. A Microsoft certificate is a document that showcases the holder's expertise in a particular Microsoft technology. In addition, it proves that the individual has the necessary skills, knowledge, experience, and talent for the technology for which the certificate is issued. Please refer to the following figure:
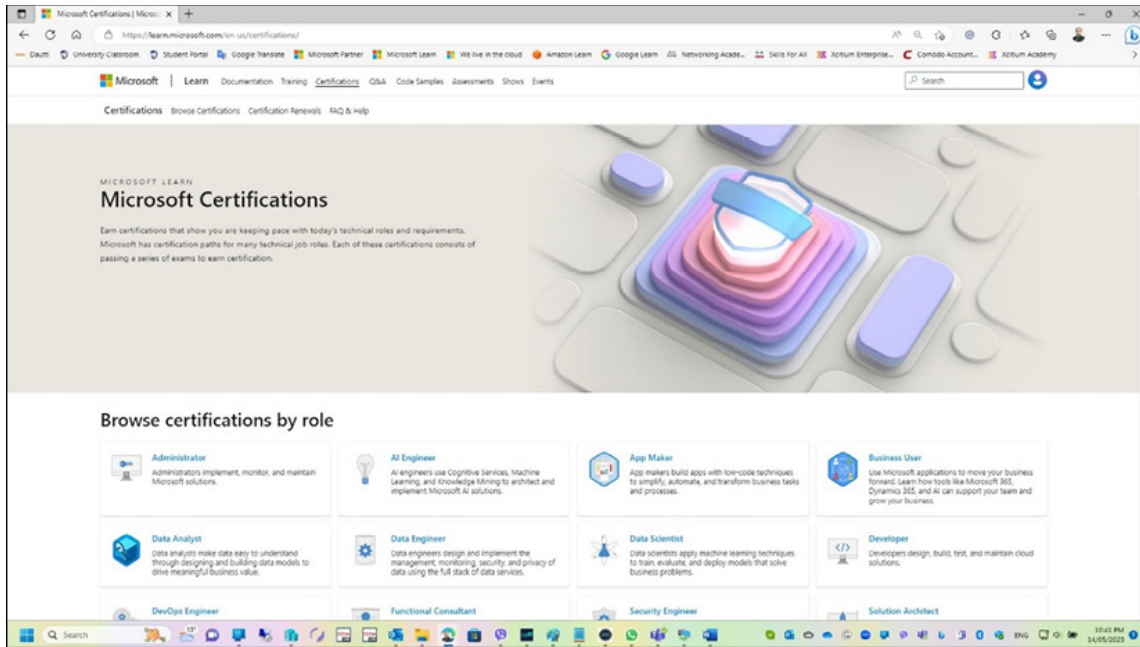
Figure 9.1: *Microsoft certification website*

According to Todd Thibodeaux, president and CEO at CompTIA, "The certificate represents a reliable current and advanced knowledge mechanism." However, only some Microsoft certificates imply the holder has completed a Microsoft certification. For instance, someone who attended Microsoft technologies training at a Microsoft Learning Partner might receive an attendance certificate. Still, the training may not be mapped to a specific Microsoft certification exam. Therefore, the attendance certificate is not considered a Microsoft certification.

The question then arises: What is Microsoft certification? Simply put, it is a process in which a participant attends training to learn technical skills and prepare for the certification exam. Successfully passing the certification exam and obtaining the credential or title offered by the certification exam completes the so-called Microsoft Certification cycle.

In conclusion, attending training and passing the Microsoft certification exam is crucial for receiving a Microsoft certificate and becoming a Microsoft Certified Professional. The certification process ensures that individuals have the necessary skills and knowledge to meet the demands of the IT industry and opens doors to various career opportunities.

Understanding Microsoft role-based certifications

In response to the evolving landscape of the technology industry, Microsoft launched a set of new certifications in early 2019 aimed at providing more career-focused qualifications that align with existing job roles. These certifications are called role-based certifications, as shown in *Figure 9.2*, and they showcase the ability of certified candidates to keep up with the technical requirements of their respective roles. In addition, by becoming certified, individuals can prove their expertise to employers and peers and receive the recognition and opportunities they have earned.
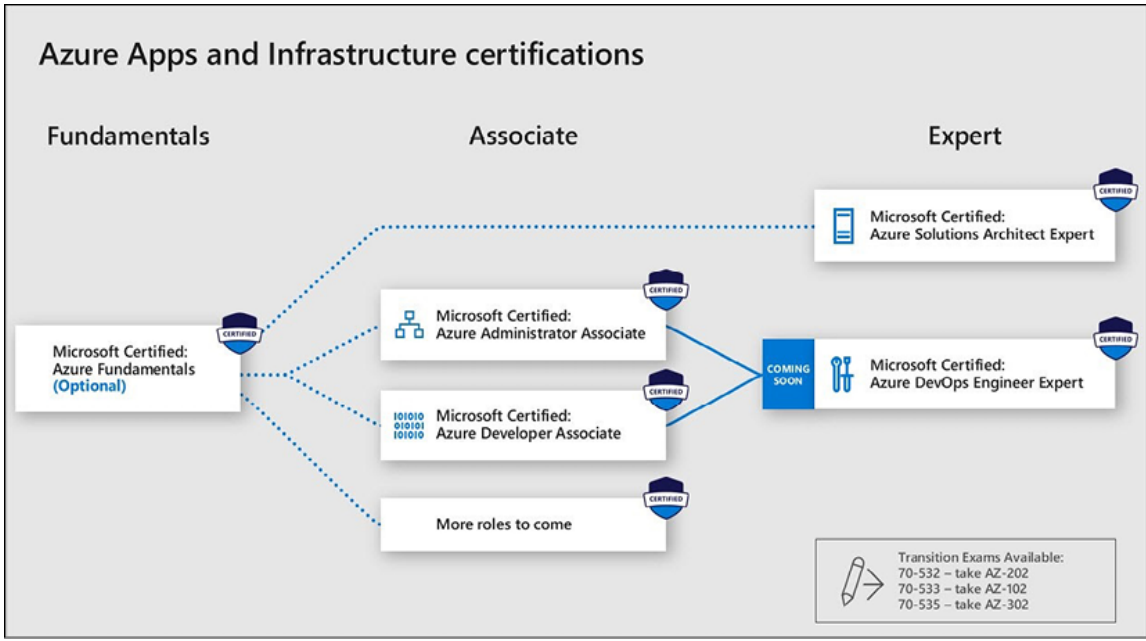
Figure 9.2: Role-based certifications for Azure apps and infrastructure

The move toward role-based certifications was prompted by IT roles becoming increasingly specialized and niche-oriented. For example, gone are the days of general IT roles such as system

administrator or system engineer. Nowadays, job titles include specific subheadings, such as Azure administrator or Azure Security Engineer, and some even further subcategorize into highly specialized roles. As a result, Microsoft saw the need to target these particular career roles with its new certifications rollout to provide more focused and job-specific training that goes beyond a general overview of a career sector.

In essence, the new role-based certifications from Microsoft are designed to help individuals gain the skills and knowledge needed to excel in their specific job roles and to keep up with the changing demands of the industry. As a result, individuals can demonstrate their expertise and stay competitive in a rapidly evolving industry by focusing on the skills required for specific job roles.

Note: The link **https://learn.microsoft.com/en-us/certifications/posts/new-role-based-certification-and-training-is-here** leads to a blog post on Microsoft's website announcing the launch of their new role-based certifications and training programs. The post provides information on the changes made to their certification program, the benefits of the new role-based approach, and the availability of the new courses. It also includes a list of the new role-based certifications offered by Microsoft and a link to the certification roadmap.

Who should take the Microsoft certification exam?

The Microsoft certification program provides evidence that an individual has the required technical skills and knowledge, making them a desirable candidate for organizations and businesses. This section is helpful for both those who are already certified and those who are not, as it explains the new format of Microsoft certification and provides information on how to obtain it.

Certification holders are informed about the new format of Microsoft certification, whereas non-certified individuals can learn about the certification process and how it can benefit their careers. Microsoft certification offers many advantages, as shown in *Figure 9.3*, including increased employment opportunities, the ability to prove expertise in the field, the capacity to apply theoretical knowledge to practical work, adaptability to work

environments, and increased opportunities for professional growth. Please refer to the following figure:

Figure 9.3: Pearson VUE survey on the value of IT certification

Microsoft certification provides a professional edge by providing globally recognized industry-endorsed evidence of skills proficiency, demonstrating the ability and willingness to embrace new technologies. The desire to learn is crucial for success in obtaining technology skills, and Microsoft offers a range of training and certification options to accommodate different learning preferences, as explained as follows:

- Candidates interested in learning technology and obtaining certification can use accessible learning paths on Microsoft Learn, which allows them to learn core concepts at their own pace and access training materials and test-drive products at no cost.

- Microsoft learning partners offer instructor-led training.

- MeasureUp provides official practice tests to help candidates prepare for certification exams.

Once a candidate passes a certification exam, they will receive an e-mail from Microsoft stating that they are now certified and will receive an e-mail shortly after to claim their certification badge. Even if candidates previously achieved certification, they could claim their badge through the Credly portal

(**https://info.credly.com/**), which contains all the badges earned from Microsoft based on past certification history.

Skills measured in the Microsoft certification exam

Certification exams are designed to test candidates' technical skills and knowledge in a particular field. To provide guidelines for exam candidates, exam clients such as Microsoft provide a list of skills likely to be included in the exam. These skills measured are periodically updated to reflect changes in the exam's content and ensure that the exam remains relevant. For instance, the AZ-800 exam measures the skills required to administer core Windows Server workloads using on-premises, hybrid, and cloud technologies.

Candidates preparing for the AZ-800 exam are expected to have expertise in implementing and managing on-premises and hybrid solutions, including identity, management, computing, networking, and storage. In addition, they should be proficient in using administrative tools and technologies such as Windows Admin Center, PowerShell, Azure Arc, and IaaS virtual machine administration.

It is worth noting that certification exams are regularly updated or retired to align with changing industry trends and technology. For example, the MTA 98-365, Microsoft's Windows Server Administration Fundamentals certification, was retired on June 30, 2022. After that date, MTA exams delivered through Certiport and Pearson VUE were no longer available.

By staying up-to-date with changes in certification exam content and requirements, candidates can ensure they have the knowledge and skills to succeed in their chosen field.

Note: The link

To prepare for the AZ-800 certification exam, being familiar with the skills that will be measured on the test is crucial. By reviewing the skills measured, as shown in *Figure 9.4*, you can better understand the topics that will be covered and prepare accordingly. For example, the AZ-800 exam measures skills related to designing and implementing solutions that span multiple Azure services, integrating them with existing on-premises technologies, identifying tradeoffs, and making decisions for creating public and hybrid cloud solutions.

Other skills measured include analyzing requirements and constraints, recommending appropriate Azure services, and designing for identity, security, and compliance. In addition to these technical skills, the exam also measures project management and governance skills. That includes understanding project delivery methodologies, developing project budgets and timelines, and identifying risks and dependencies. By being familiar with the skills measured on the exam, you can focus your study efforts on the most critical areas and ensure that you are well-prepared for the certification test. As cloud technology continues to evolve and become more integral to business operations, the demand for individuals with expertise in designing and implementing cloud solutions will likely increase.

Refer to *Figure 9.4:*
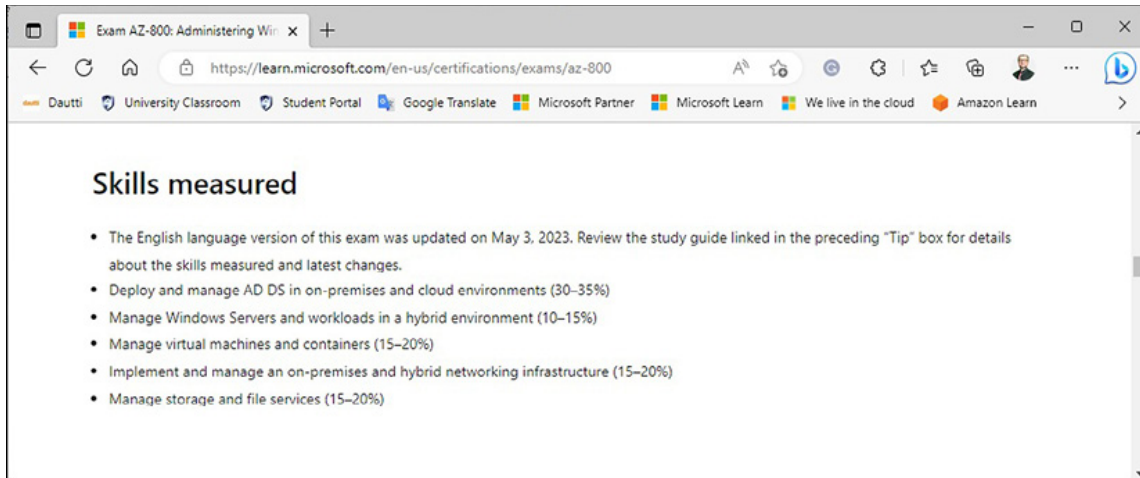
Figure 9.4: *Skills measured for AZ-800 exam*

Deploy and manage AD DS in on-premises and cloud environments (30%–35%)

To complete this exam objective, it is essential to have a solid understanding of several key components. First, you must have the knowledge and skills to deploy and manage domain controllers and configure and manage multi-site, domain, and forest environments. In addition, being familiar with AD DS security principles and effectively implementing and managing hybrid identities is crucial. Finally, it would help if you had a good grasp on how to address the Windows server using group policies. You will be well-prepared to accomplish the exam objective by mastering these critical concepts. It is worth noting that being proficient in these areas can also prove beneficial in real-world scenarios and fundamental to effective server management.

To deploy and manage AD DS domain controllers:

- Deploy and manage domain controllers on-premises
- Deploy and manage domain controllers in Azure
- Deploy RODCs
- Troubleshoot FSMO roles

To configure and manage multi-site, multi-domain, and multi-forest environments:

- Configure and manage forest and domain trusts

- Configure and manage AD DS sites
- Configure and manage AD DS replication

To create and manage AD DS security principals:

- Create and manage AD DS users and groups
- Manage users and groups in multi-domain and multi-forest scenarios
- Implement **Group Managed Service Accounts** (**gMSA**)
- Join Windows Servers to AD DS, Azure AD DS, and Microsoft **Azure Active Directory** (**Azure AD**), part of Microsoft Entra

To implement and manage hybrid identities:

- Integrate Microsoft Azure AD, part of Microsoft Entra, AD DS, and Azure AD Domain Services
- Implement Azure AD Connect
- Manage Azure AD Connect synchronization
- Implement Azure AD Connect cloud sync
- Manage Azure AD domain services
- Manage Azure AD connect health
- Manage authentication in on-premises and hybrid environments
- Configure and manage AD DS passwords

To manage Windows Server by using domain-based Group Policies:

- Implement Group Policy in AD DS
- Implement Group Policy preferences in AD DS
- Implement Group Policy in Azure AD DS

Manage Windows Servers and workloads in a hybrid environment (10%–15%)

To successfully achieve this exam objective, you must be proficient in managing Windows Servers on-premises and in the cloud. That includes a comprehensive understanding of operating workloads in the Azure environment, an increasingly important area of focus in modern IT. Being well-versed in server deployment, configuration, and maintenance tasks is essential when managing Windows Servers. In addition, you will need to be able to monitor and troubleshoot server performance and effectively manage server storage and networking resources. In terms of operating workloads in the Azure environment, there are several key concepts that you will need to master. These include effectively deploying and managing virtual machines in Azure and understanding how to leverage Azure services such as Azure Active Directory and Azure Storage. In addition, you should be familiar with monitoring and optimizing Azure workloads for performance and efficiency. By demonstrating proficiency in managing Windows Servers and workloads in the Azure environment, you will be well-prepared to accomplish this exam objective and succeed in real-world scenarios. It is worth noting that as more and more organizations move toward cloud-based solutions, having a solid understanding of cloud-based management will become increasingly important in the world of IT.

To manage Windows Servers in a hybrid environment:

- Deploy a WAC Gateway server
- Configure a target machine for WAC
- Configure PowerShell remoting
- Configure CredSSP or Kerberos delegation for second hop remoting
- Configure JEA for PowerShell remoting

To manage Windows Servers and workloads by using Azure services:

- Manage Windows Servers by using Azure Arc
- Assign Azure Policy guest configuration

- Deploy Azure services using Azure VM extensions on non-Azure machines
- Manage updates for Windows machines
- Integrate Windows Servers with log analytics
- Integrate Windows Servers with Microsoft Defender for Cloud
- Manage IaaS VMs in Azure that run Windows Server
- Implement Azure Automation for hybrid workloads
- Create runbooks to automate tasks on target VMs
- Implement Azure Automation State Configuration to prevent configuration drift in IaaS
- Machines

Manage virtual machines and containers (15%–20%)

To successfully achieve this exam objective, you must thoroughly understand managing virtual machines using Hyper-V Manager. That includes performing tasks such as creating, configuring, and maintaining virtual machines and managing virtual machine resources such as storage and networking. In addition, it would help if you were well-versed in setting up and managing containers, an increasingly important aspect of modern IT infrastructure. That includes understanding container architecture, configuring container environments, and managing container images and repositories. Finally, it would help if you had experience working with Windows Server virtual machines in Azure. That requires knowledge of deploying and configuring virtual machines in Azure, as well as being able to manage virtual machine resources such as storage and networking. In addition, you should be familiar with Azure tools such as Azure PowerShell, which can be used to manage Azure resources, including virtual machines. By mastering these essential concepts, you will be well-prepared to accomplish this exam objective and succeed in real-world scenarios. As virtualization and cloud-based solutions become increasingly prevalent, a strong understanding of virtual

machine and container management will be critical for success in IT.

To manage Hyper-V and guest virtual machines:

- Enable VM-enhanced session mode
- Manage VM using PowerShell remoting, PowerShell Direct, and SSH Direct for Linux VMs
- Configure nested virtualization
- Configure VM memory
- Configure integration services
- Configure Discrete Device Assignment
- Configure VM resource groups
- Configure VM CPU groups
- Configure hypervisor scheduling types
- Manage VM checkpoints
- Implementing high availability for virtual machines
- Manage VHD and VHDX files
- Configure Hyper-V network adapter
- Configure NIC teaming
- Configure Hyper-V switch

To create and manage containers:

- Create Windows Server container images
- Manage Windows Server container images
- Configure container networking
- Manage container instances

To manage Azure Virtual Machines that run Windows Server:

- Manage data disks
- Resize Azure VM
- Configure continuous delivery for an Azure VM

- Configure connections to VMs
- Manage Azure VM network configuration

Implement and manage an on-premises and hybrid networking infrastructure (15%–20%)

To succeed in this exam objective, it is crucial to have a strong understanding of deploying name resolutions and managing IP addressing and network connectivity both on-premises and in the cloud. Deploying name resolutions refers to assigning names to network resources such as computers, printers, and servers. That can be accomplished through **Domain Name System** (**DNS**) and **Windows Internet Naming Service** (**WINS**). By understanding how to deploy name resolutions effectively, you can ensure that network resources are easily identifiable and accessible. Managing IP addressing and network connectivity involves configuring and troubleshooting IP addresses, subnets, and network gateways. That includes understanding the various types of IP addresses, subnet masks, and default gateways and how to configure them on network devices such as routers, switches, and firewalls. Finally, in addition to manage network connectivity on-premises, it is also crucial to manage network connectivity in the cloud. That includes understanding how to configure virtual networks, network security groups, and load balancers in cloud environments such as Azure and AWS. By mastering these key concepts, you will be well-prepared to accomplish this exam objective and succeed in real-world scenarios. It is worth noting that as organizations increasingly rely on network connectivity for their day-to-day operations, having a solid understanding of network management is becoming increasingly important in IT.

To implement on-premises and hybrid name resolution:

- Integrate DNS with AD DS
- Create and manage DNS zones and records
- Configure DNS forwarding/conditional forwarding
- Integrate Windows Server DNS with Azure DNS private zones

- Implement DNSSEC

To manage IP addressing in on-premises and hybrid scenarios:

- Implement and manage IPAM
- Implement and configure the DHCP server role (on-premises only)
- Resolve IP address issues in hybrid environments
- Create and manage scopes
- Create and manage IP reservations
- Implement DHCP high availability

To implement on-premises and hybrid network connectivity:

- Implement and manage the remote access role
- Implement and manage Azure Network Adapter
- Implement and manage Azure extended network
- Implement and manage the Network Policy Server role
- Implement Web Application Proxy
- Implement Azure Relay
- Implement site-to-site VPN
- Implement Azure Virtual WAN
- Implement Azure AD Application Proxy

Manage storage and file services (15%–20%)

To achieve success in this exam objective, it is essential to have a strong understanding of configuring and managing file synchronization in Azure and file shares and storage in Windows Server. Configuring and managing file sync in Azure involves understanding how to enable Azure File Sync. This cloud-based service allows organizations to centralize file services in Azure while maintaining local access to files. That includes understanding how to configure synchronization policies, manage conflicts, and monitor sync activity. Managing file shares and storage in Windows Server involves creating and managing file

shares, assigning permissions to users and groups, and configuring storage options such as quotas and replication. That includes understanding how to manage storage resources such as disks and volumes and using tools such as storage spaces to optimize storage utilization. Finally, in addition to managing file shares and storage on-premises, it is also crucial to understand how to manage these resources in the cloud. That includes understanding how to use Azure File Storage to create and manage file shares in the cloud and using Azure Blob Storage to manage unstructured data such as images and video. By mastering these key concepts, you will be well-prepared to accomplish this exam objective and succeed in real-world scenarios. As organizations continue to rely heavily on data and file storage, having a solid understanding of file synchronization and storage management is becoming increasingly important in IT.

To configure and manage Azure File Sync:

- Create Azure File Sync service
- Create sync groups
- Create cloud endpoints
- Register servers
- Create server endpoints
- Configure cloud tiering
- Monitor File Sync
- Migrate DFS to Azure File Sync

To configure and manage Windows Server file shares:

- Configure Windows Server file share access
- Configuring file screens
- Configure FSRM quotas
- Configure BranchCache
- Implement and configure **Distributed File System** (**DFS**)

To configure Windows Server storage:

- Configure disks and volumes

- Configure and manage Storage Spaces

- Configure and manage Storage Replica

- Configure Data deduplication

- Configure SMB Direct

- Configure Storage QoS

- Configure file systems

What to expect and how to succeed in the Microsoft certification exam

You can expect to encounter between 40 and 60 questions when taking a Microsoft certification exam. The exam's duration depends on the type of certification exam you are taking, and it includes additional minutes for an introduction and survey. To pass the exam, you must score 700 or higher. You can flag questions for review during the exam and return to them later if you have time. However, this option is only available if you manage your time effectively. You can navigate within the exam using the Previous and Next buttons, which allows you to review and change your answers before submitting your exam for grading. It is essential to take advantage of all the features available during the exam, such as flagging questions for review, to ensure that you answer all questions to the best of your ability and achieve a passing score.

Refer to *Figure 9.5:*
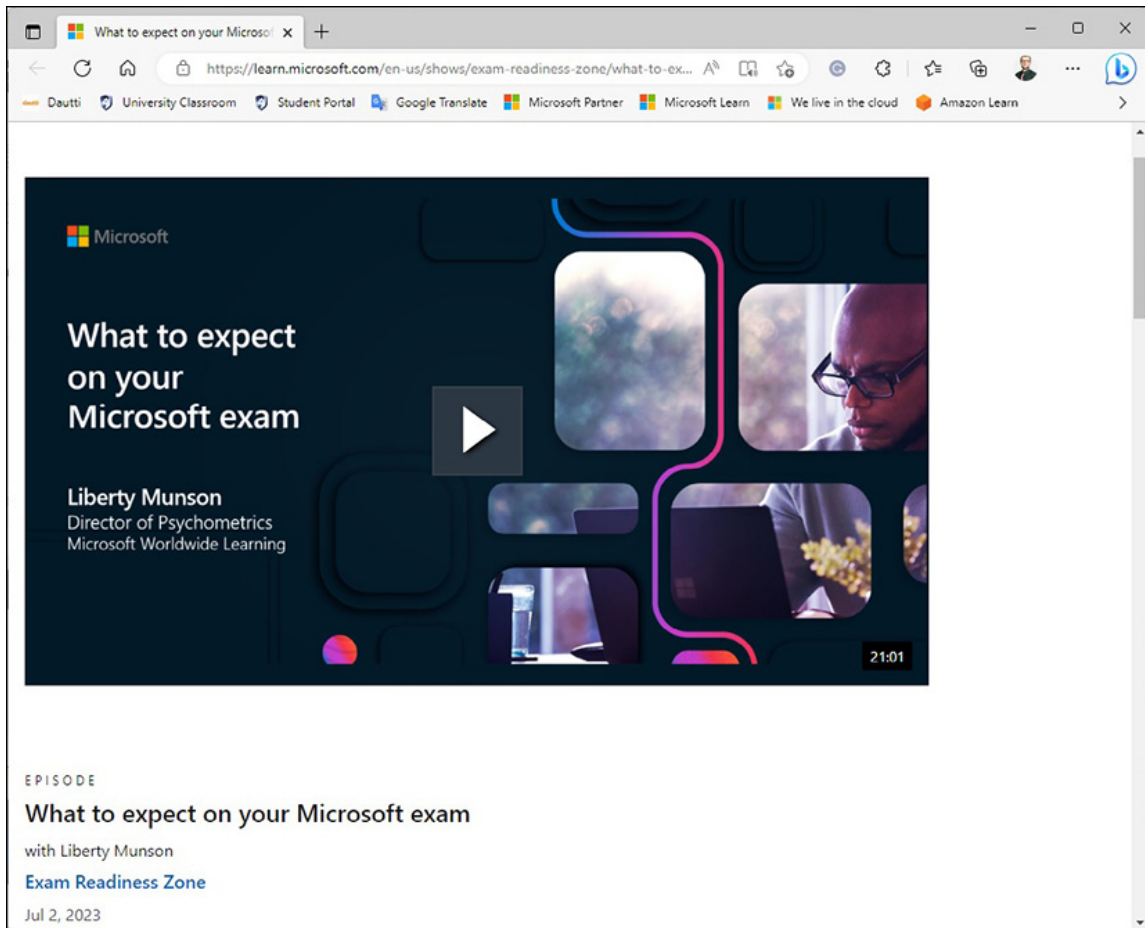
Figure 9.5: *"What to Expect on your Microsoft Exam" by Liberty Munson*

Note: The link **https://docs.microsoft.com/en-us/learn/certifications/exam-duration-question-types** provides information on Microsoft certification exam durations, passing scores, and question types. It also explains the review and flag options available during the exam and the ability to move back and forth within questions.

Preparing for the Microsoft certification exam

There is no standard to prepare for Microsoft certification exams, but certain best practices can be followed. These best practices include the following:

- Actively working in the ICT industry for 6–12 months
- Attending Microsoft training at a Microsoft Learning Partner

- Reading books on Microsoft technologies and using the Microsoft Learn portal

- Practicing with Microsoft technologies

- Getting certified by other vendors like CompTIA

- Attempting practice tests to become familiar with the exam questions, reviewing the exam's skills measured to identify areas of improvement

- Interacting with online and offline friends who have passed the Microsoft certification exams to learn from their experiences

By following these best practices, as shown in *Figure 9.6*, candidates can prepare themselves better for the certification exams and increase their chances of success. However, it is essential to note that each exam measures specific skills; hence, the exam's preparation strategy will vary based on the exam. Please refer to the following figure:
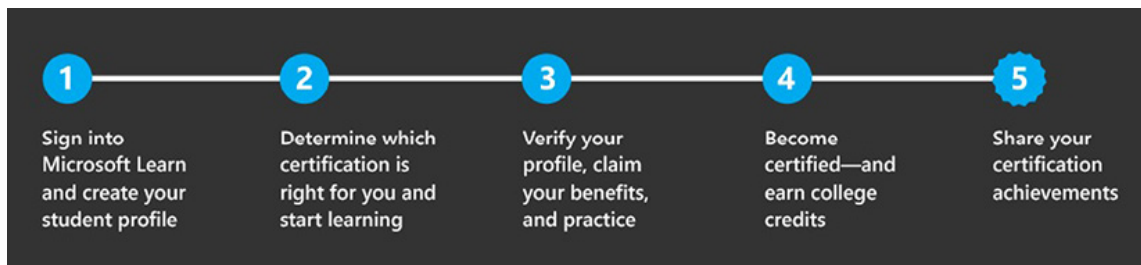
Figure 9.6: *Microsoft's strategy for getting certified*

Note: The link **https://aka.ms/examdemo** directs to a demo of a Microsoft certification exam. Users can experience the exam format and interface and answer sample questions to understand what to expect in an actual exam. The demo is available for various Microsoft certification exams, and it aims to help candidates familiarize themselves with the exam environment and assess their readiness for the actual exam.

How to register for the Microsoft certification exam

When it comes to writing for the Microsoft certification exam, there are two ways to do so, given as follows:

- The first way is to register online through the Pearson VUE website, which requires a Web account

- The second way to register is to contact a nearby Pearson VUE-authorized testing center

Certiport and Pearson VUE, as shown in *Figure 9.7*, offer Microsoft certification exams, with two exam delivery methods in both cases:

- The first method is proctored exams delivered at a test center. Test centers are authorized facilities that provide certification exams for test-takers.

- The second method is self-administered online exams that can be taken at home or in the office. Please refer to the following figure:
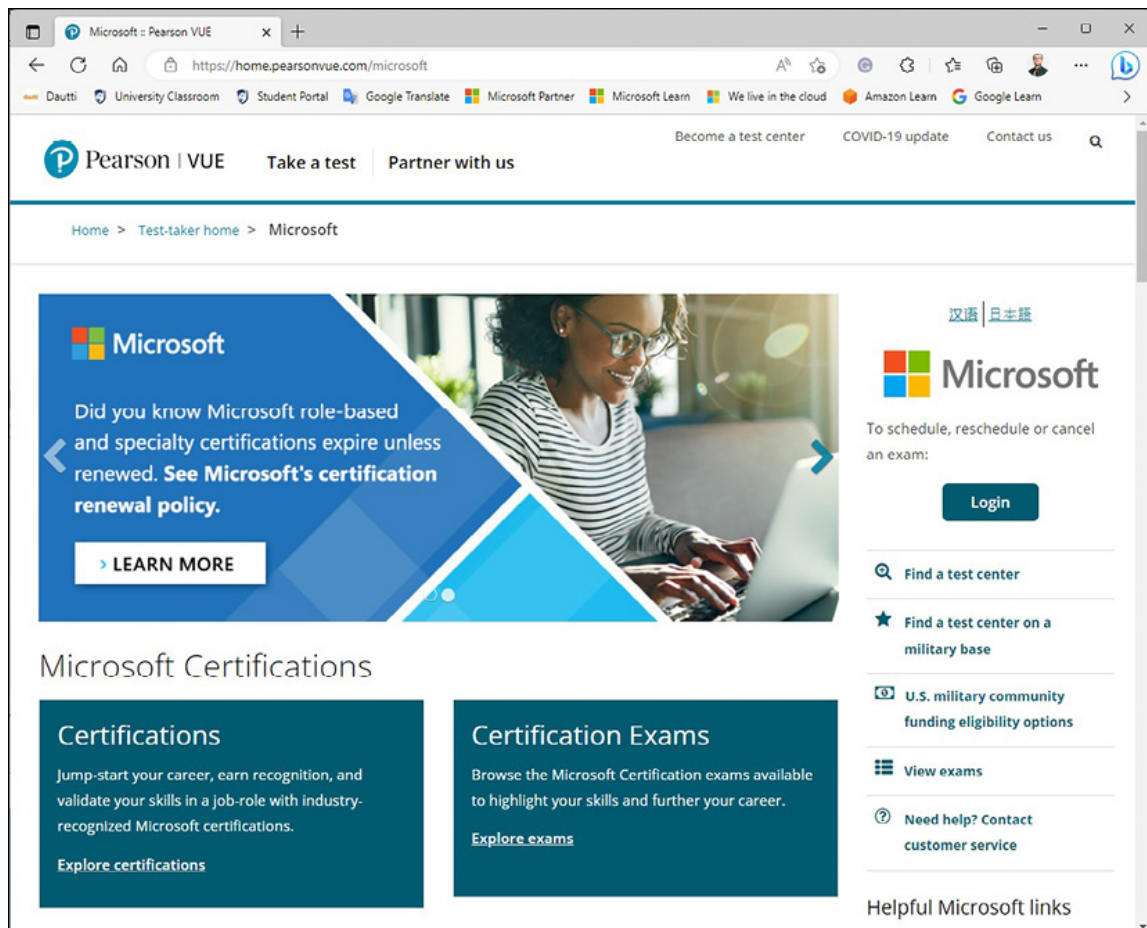
Figure 9.7: Pearson VUE website for registering for Microsoft exams

The online examination format became more popular during the COVID-19 pandemic, and many vendors have offered online exams. However, before the pandemic, Microsoft had already provided online exams through Pearson VUE.

Note: The link **https://home.pearsonvue.com/microsoft** directs to the Pearson VUE website's Microsoft certification page. The page provides information about Microsoft's certification exams, including available certification paths, exam formats, and how to register for and schedule an exam. It also allows users to search for nearby test centers and provides resources for exam preparation.

On the day of your Microsoft certification exam

Preparing for a certification exam involves more than just learning and practicing. It would help if you are mentally ready for the exam day. One important aspect is to ensure that you have had a good night's sleep before the exam day and not to stress too much. Arrive at the test center or start the online admission process 30 minutes before the scheduled exam time and carry the required ID. It would be best if you are also polite to the test center administrator and carefully read the Pearson VUE Candidate Rules Agreement.

When sitting in front of the delivery workstation, it is essential to relax, take a deep breath, and read the exam instructions carefully before starting the exam. You should read each question attentively and avoid rushing to answer the questions without giving them proper thought. If you have doubts about any question, mark it for review or return to questions you have already answered using the Previous button. Time management is also crucial, so be rational with the exam time and answer all exam questions on time.

Refer to *Figure 9.8:*
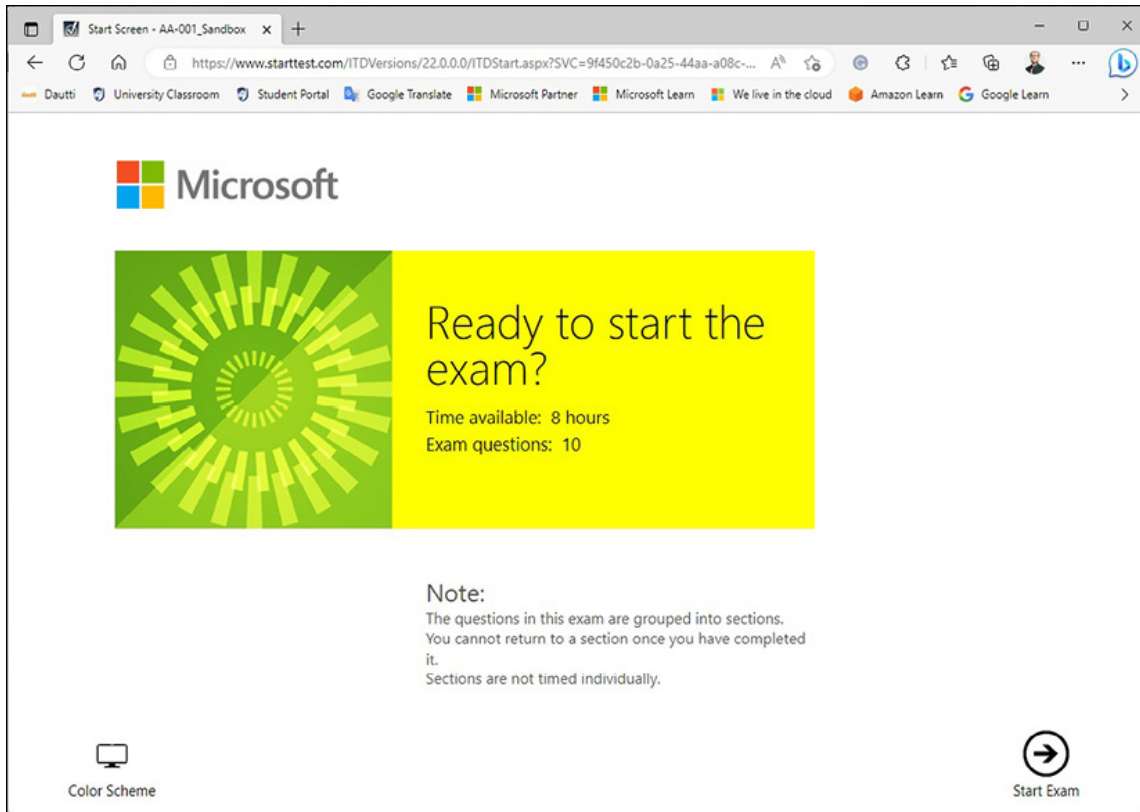
Figure 9.8: *Microsoft demo exam*

After answering all the questions, you will be shown the exam result, which can be either joyous or disappointing. If you pass, congratulations! If not, do not despair. Instead, accept the result and start preparing again by identifying the exam objectives you need to improve. Remember that exam experience will help you prepare better and pass the exam successfully.

Note: The link **https://home.pearsonvue.com/candidate-rules-agreement** provides information on the Pearson VUE Candidate Rules Agreement. This agreement outlines the rules and regulations that candidates must follow while taking the exam, both at the test center and during online testing. Therefore, reading and understanding this agreement before taking the exam is essential to avoid potential issues or disqualification.

New Microsoft Certification validity and renewal requirements

The pace of technology development is fast, and it is essential to keep up with the latest skills to stay caught up. Microsoft

recognizes this and constantly provides new and improved certification formats to help candidates keep their certifications active. For example, in the spring of 2021, Microsoft introduced a new certification validity period and renewal format, as shown in *Figure 9.9*. Microsoft exams, excluding the fundamentals track, are valid for one year. The renewal process is free of cost and can be done through the Microsoft Learn portal. Microsoft will also e-mail the candidate the certification renewal process six months before the certification expires. This system ensures that Microsoft certifications remain relevant and up-to-date, helping professionals stay competitive in today's fast-paced technology industry. Please refer to the following figure:

Figure 9.9: New Microsoft certification validity and renewal requirements

Note: The link **https://docs.microsoft.com/en-us/learn/certifications/renew-your-microsoft-certification** is a valuable resource for those seeking to renew their Microsoft certifications. Microsoft has implemented a new certification validity period and renewal format, requiring candidates to keep their skills current to avoid constantly playing catch-up. The renewal process is free of cost and can be done through the Microsoft Learn portal, with notifications sent out via e-mail six months before the certification expires. It is essential to stay up-to-date on these changes to maintain active Microsoft certifications.

Conclusion

In this chapter, you have learned about Microsoft certification and the process of obtaining those certifications. You were introduced to the different types of Microsoft certifications and the steps involved in acquiring them. That will help you determine if the Microsoft certification exam suits you. The module also used the example of the AZ-800 exam to provide you with information on the skills tested in Microsoft certification exams and how the exam questions are organized. In addition, this chapter has guided how to prepare for the exam and what to expect on exam day. Finally, you have also learned about the new certification validity period and renewal format, which will help keep your certification active and up-to-date.

Join our book's Discord space

Join the book's Discord Workspace for Latest updates, Offers, Tech happenings around the world, New Release and Sessions with the Authors:

https://discord.bpbonline.com

CHAPTER 10
Answers to Chapter Questions

Introduction

This chapter is dedicated to addressing the questions that have been raised throughout the chapters of this book as part of a dedicated questions section in each chapter. That will be a valuable resource for those struggling with a specific concept or topic, as the answers provided can offer valuable insights and clarity. By referring to this chapter, readers can deepen their understanding of the material and ensure they fully grasp the main ideas and concepts presented throughout the book. It is worth noting that this chapter serves as a comprehensive review of the book's content. That makes it a valuable resource for students, educators, and anyone looking to reinforce their knowledge of the subject matter. This chapter can be beneficial for exam preparation or for individuals who wish to test their understanding of the material. Overall, the answers provided in this chapter are a valuable reference for anyone seeking to enhance their knowledge of the book's subject matter. Whether you seek a better understanding of a particular concept or simply looking for a comprehensive review of the material, this chapter can help you achieve your goals.

Structure

In this chapter, we will cover the following topics:

- Answers to Chapter 1 questions
- Answers to Chapter 2 questions
- Answers to Chapter 3 questions
- Answers to Chapter 4 questions
- Answers to Chapter 5 questions
- Answers to Chapter 6 questions
- Answers to Chapter 7 questions
- Answers to Chapter 8 questions

Objectives

This chapter aims to answer the questions raised throughout the book in each chapter's Dedicated Questions section. The aim is to offer valuable insights and clarity to readers struggling with specific concepts or topics. Furthermore, by reviewing the answers provided in this chapter, readers can deepen their understanding of the book's content and ensure they have a firm grasp of the main ideas and concepts.

Answers to Chapter 1 questions

Chapter 1, *Understanding Network Components*, covers computer networking and provides a fundamental understanding of its components. It includes questions and their answers in the following sections, making it easy for you to locate and review the answers. This chapter sets the foundation for the book and prepares you for more complex concepts covered in subsequent chapters.

Q1: In your own words, define a computer network.

In simple terms, a *computer network,* as in *Figure 10.1*, involves two or more connected computers that share resources. That means that at least two computers are required to create a network. Other factors, such as the coverage area, how services

are accessed, and the purpose of network servers, also play a role in determining the type of computer network.
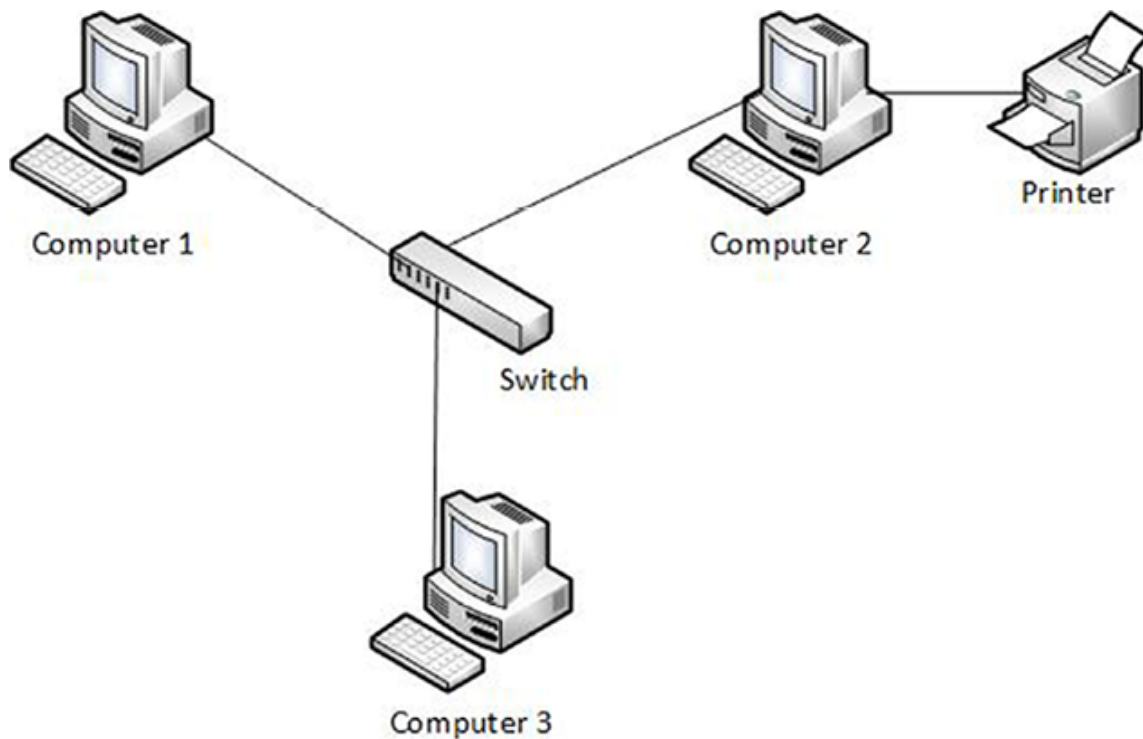
Figure 10.1: *Computer network*

Q2: How many types of computer networks can you name?

Various types of computer networks exist, including the following:

- **Personal Area Network** (**PAN**) is a network that connects devices in an individual workspace.

- **Local Area Networks** (**LAN**) connect devices in a specific area, like a floor or building.

- **Campus Area Networks** (**CAN**) is a network that connects LANs in a limited geographical area such as campus.

- **Metropolitan Area Networks** (**MAN**) is a network that connects LANs within a town, city, or metropolitan area.

- **A Wide Area Network** (**WAN**) is a network that spans a large geographical area and facilitates data transfer

between MANs. The internet is an example of a WAN.

Different types of networks use other technologies for interconnection, such as Bluetooth for a WPAN, radio waves for a WLAN, and the internet for a WAN.

Q3: How many types of network components can you name?

Various types of network components exist, including the following:

- A **node** refers to any device connected to a network, even if it does not have a network interface with an assigned IP address.

- A **host** is a device with an IP address assigned to its network interface, which it uses to communicate and access network services.

- **Clients**, as shown in *Figure 10.2*, are devices that request access to resources, whereas servers are devices that supply services:
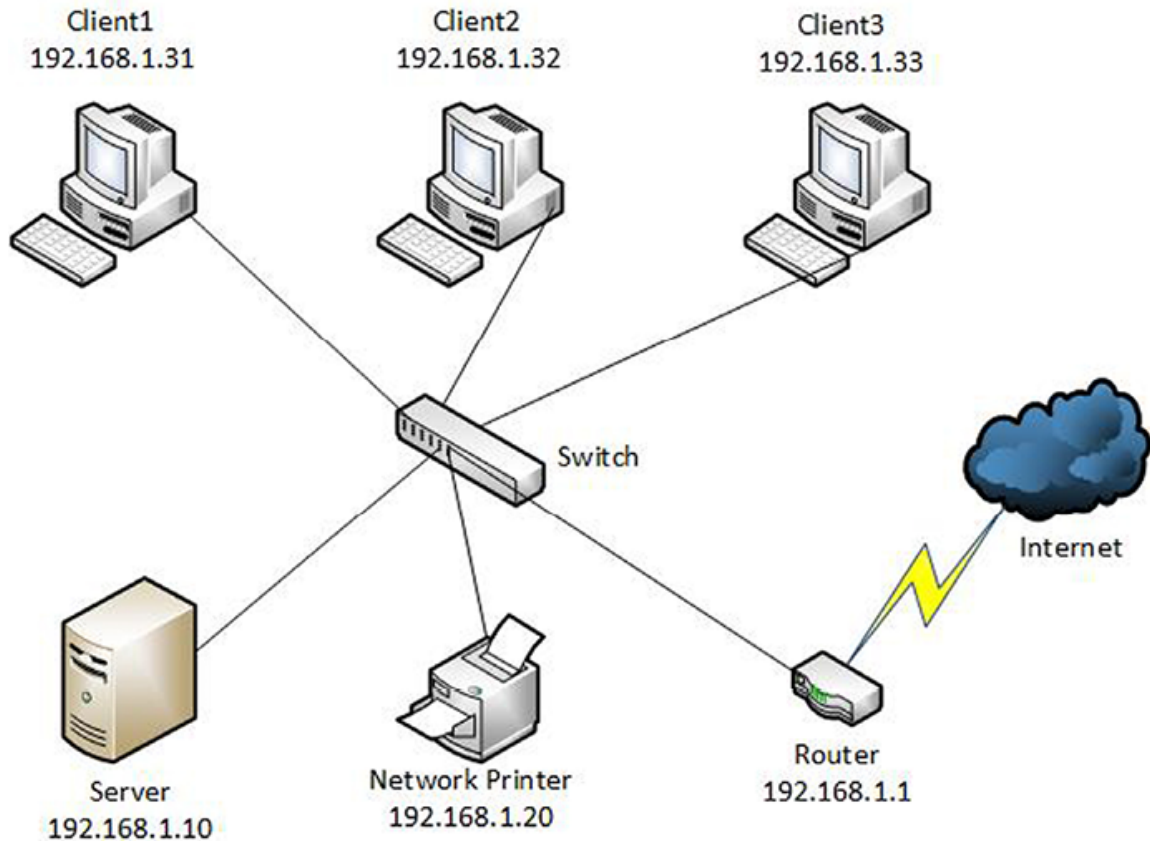
Figure 10.2: *Clients in a LAN*

- **Servers** respond to requests for service access by supplying the service itself.

- **Computer network architectures** are designs that facilitate communication between the components of a computer network.

- **Topology** defines the shape of a computer network from the perspective of the arrangements, interconnections, and communications among network components.

- A **Network Operating System** (**NOS**) is software specifically designed to manage, maintain, and provide resources in a network.

Q4: List three differences between IPv4 and IPv6 addressing technologies.

IPv4 and IPv6 differ in the following three ways:

1. IPv4 uses 32-bit addressing, whereas IPv6 uses 128-bit addressing.

2. IPv4 uses decimal dot notation for its addresses, whereas IPv6 uses hexadecimal.

3. IPv4 addresses comprise four octets, whereas IPv6 addresses comprise eight sextets.

Q5: In your own words, define a Network Operating System.

Network Operating System (**NOS**), as shown in *Figure 10.3*, is software created for managing, maintaining, and providing resources in a network. In addition, it can perform several other network resource-related tasks, such as sharing files and applications, providing Web services, controlling access to resources, managing users and computers, offering configuration tools, and maintaining resources. Please refer to the following figure:
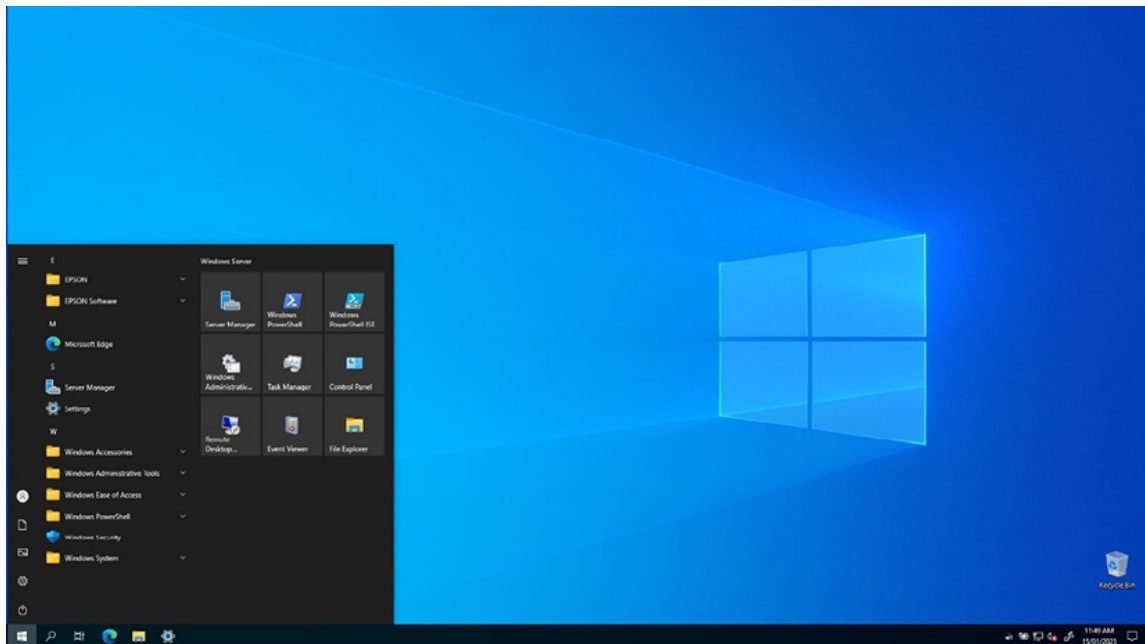
Figure 10.3: *A Network operating system*

Answers to Chapter 2 questions

Chapter 2, *Introduction to Windows Server 2022* overviews this server operating system and its hardware features. It also includes a comparison between Windows Server 2022 and Windows Server 2019. This chapter contains questions related to the topic, and their answers are provided in subsequent sections for easy reference.

Q1: What are the server's four hardware key components, and what is their function?

To ensure optimal server performance for both regular and intensive workloads, it is essential to monitor four crucial hardware components of the system:

- The **processor**, as shown in *Figure 10.4,* is a chip on the server's motherboard, similar to a personal computer's:

Figure 10.4: *Server's processor*

- **Random Access Memory** (**RAM**) is the server's working memory.

- The **disk** is the hardware component where data is permanently stored.

- The **network interface** enables the server to connect to the **Local Area Network** (**LAN**) and the internet.

These components significantly impact the server's overall performance, so it is recommended to assess their performance regularly.

Q2: Can you name each era of the Windows Server and list the corresponding versions?

The history of servers can be divided into the following different eras based on their evolution and the needs they were meant to address:

- The first era was the **Server for the masses** from 1996 to 2000. During this era, servers became more affordable and widely available, making them accessible to small and medium-sized businesses.

- The second era was the **Enterprise era,** which lasted from 2000 to 2008. During this period, servers became more robust and were designed to support larger organizations' needs, such as scalability and high availability.

- The third era was the **Datacenter era,** which lasted from 2009 to 2013. During this period, servers were built to support data centers and cloud computing, focusing on virtualization and automation.

- The fourth era, **Cloud for the masses**, started in 2016 and continues today. During this period, servers became more accessible through cloud providers, making them available to individuals and businesses of all sizes.

Table 10.1 shows the transition of the Windows Server technology over time:

Server for the Masses era 1996–2000	Enterprise era 2000–2008	Datacenter era 2009–2013	Cloud for the Masses era 2016-present
Windows NT Server 3.5 Windows NT Server 4.0	Windows 2000 Server Windows Server 2003	Windows Server 2008 Windows Server 2012	Windows Server 2016 Windows Server 2022 Windows Server 2022

Table 10.1: *Transition of the Windows Server technology*

The following are the several server operating systems that were released during these eras:

- Windows NT Server 3.5 and 4.0 were introduced during the **Server for the Masses** era.

- Windows 2000 Server and Windows Server 2003 were released during the **Enterprise era**.

- Windows Server 2008 and Windows Server 2012 were part of the **Datacenter era**.

- Windows Server 2016 and Windows Server 2022 were introduced during the **Cloud for the Masses** era, focusing on cloud computing and hybrid environments.

Q3: What do you mean by minimum system requirements?

Minimum system requirements refer to the hardware for installing software or operating systems. However, there is no assurance that it will operate at the best performance level. The minimum system requirements for installing Windows Server 2022 are as follows:

- **Processor:** 1.4 GHz 64-bit processor

- **RAM:** 512 MB (2 GB for Server with Desktop Experience installation option)

- **Disk Space:** 32 GB

- **Network:** Ethernet adapter with at least 1 Gbps throughput

- **Graphics device and monitor:** Capable of displaying Super VGA (1,024 × 768) or higher resolution

- **Other hardware:** DVD drive (if installed from DVD media), keyboard, mouse (or compatible pointing device), TPM, and internet access.

Q4: List three new features in Windows Server 2022.

Windows Server 2022 introduces three new features, which include the following:

- **Microsoft Edge**, as shown in *Figure 10.5*, is built on Google's Chromium engine, supported by Microsoft security and innovation:
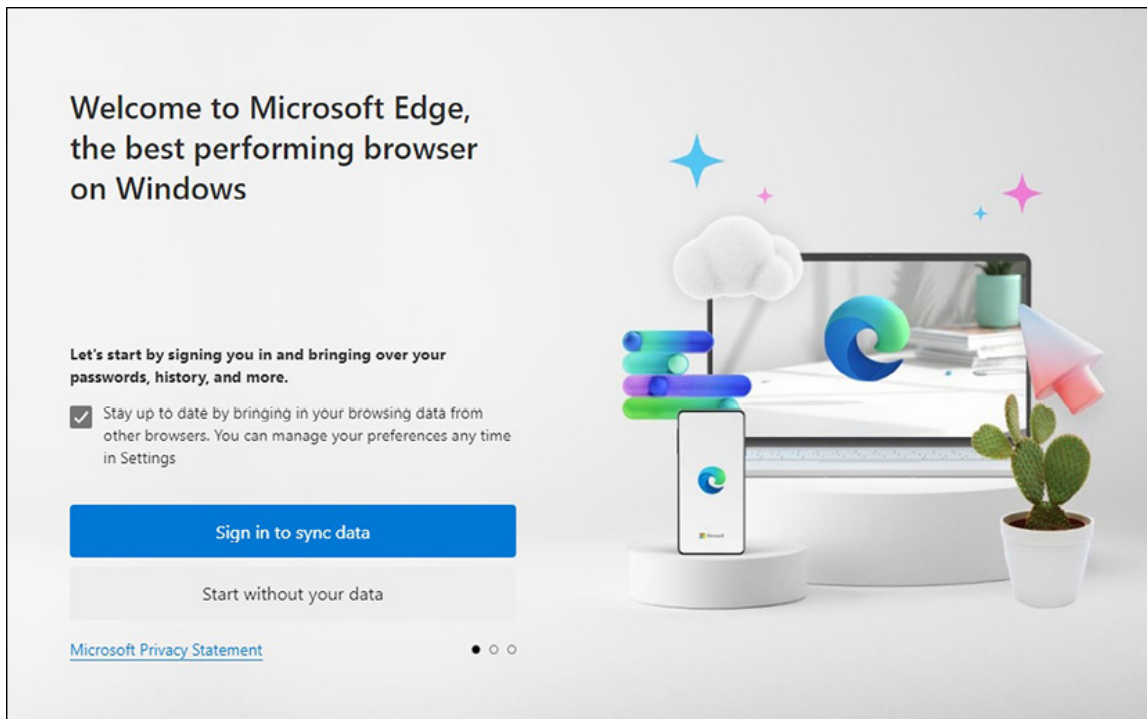
Figure 10.5: New Microsoft Edge

- The **Azure hybrid center** provides a centralized hub to access all of Azure's integrated services.
- The **Secured-core server** is a new feature providing multi-layered security across hardware, firmware, and operating systems to offer powerful protection against threats.

Q5: What do you like most about Windows Server 2022?

Microsoft has been attempting to improve Windows Server for cloud computing since Windows Server 2016. However, with the Windows Server 2022 Datacenter Azure edition, Microsoft has

achieved a fully cloud-focused operating system exclusively designed and developed for the Cloud.

Answers to Chapter 3 questions

Chapter 3, *Windows Server 2022 Installation* is structured to simplify the installation process for users. It provides detailed instructions and clear graphics to guide users throughout the process. This chapter also includes questions related to the topic, with their respective answers in subsequent sections, making it easy to refer to and understand.

Q1: What are the two primary partition schemes typically used in computers and servers?

The following are the two main partition schemes used in computers and servers:

1. **Master Boot Record** (**MBR**) is a legacy boot option. It operates on a disk sector of 512 bytes, allowing for a maximum of four primary partitions or three primary and one extended partition. The extended partition can have up to 26 logical partitions.
2. **GUID Partition Table** (**GPT**) is a newer partition scheme that surpasses the limitations of MBR. GPT uses a **Global Unique Identifier** (**GUID**), a 128-bit number used by Microsoft to identify resources.

Q2: What is the boot option?

The **boot option** determines how an operating system is started on a computer, indicating the device or method used to initiate the boot process. In addition, it specifies which device should be used to initiate the boot process, such as a hard drive, DVD, USB, or network connection.

Q3: Can you provide the names of installation methods?

Several methods are available for installing an operating system on a computer or server, including:

- A **clean installation** involves replacing the current operating system with a new one.

- An **upgrade** replaces the operating system while retaining files and settings.

- **Migration** involves transferring roles, features, applications, settings, and network services from an old server to a new one.

- Organizations deploying multiple servers can use **Windows Deployment Services** (**WDS**) or **Microsoft Deployment Toolkit** (**MDT**) for network installation.

Q4: What installation options should be considered before installing Windows Server 2022?

Before making a decision, it is essential to take into account the following options:

- **Desktop Experience:** With this installation option, all the features of Windows Server 2022 will be installed. However, your hardware must meet the minimum system requirements to effextively use the **Graphical User Interface** (**GUI**).

- **Server Core:** Microsoft recommends this installation option as it uses fewer hardware resources and provides better security. Roles and features can be installed on the local server using Windows PowerShell or remotely via Server Manager.

- **Nano Server:** This installation option is an alternative to Server Core that is more efficient regarding updates and reboots. It has a smaller server image size, which provides more disk space for other purposes.

Q5: What is the purpose of a virtual switch in Hyper-V?

Similar to a physical network, where a switch is needed to interconnect computers, a virtual switch, as shown in the following *Figure 10.6*, is necessary for a virtual network to connect **Virtual Machines** (**VMs**).
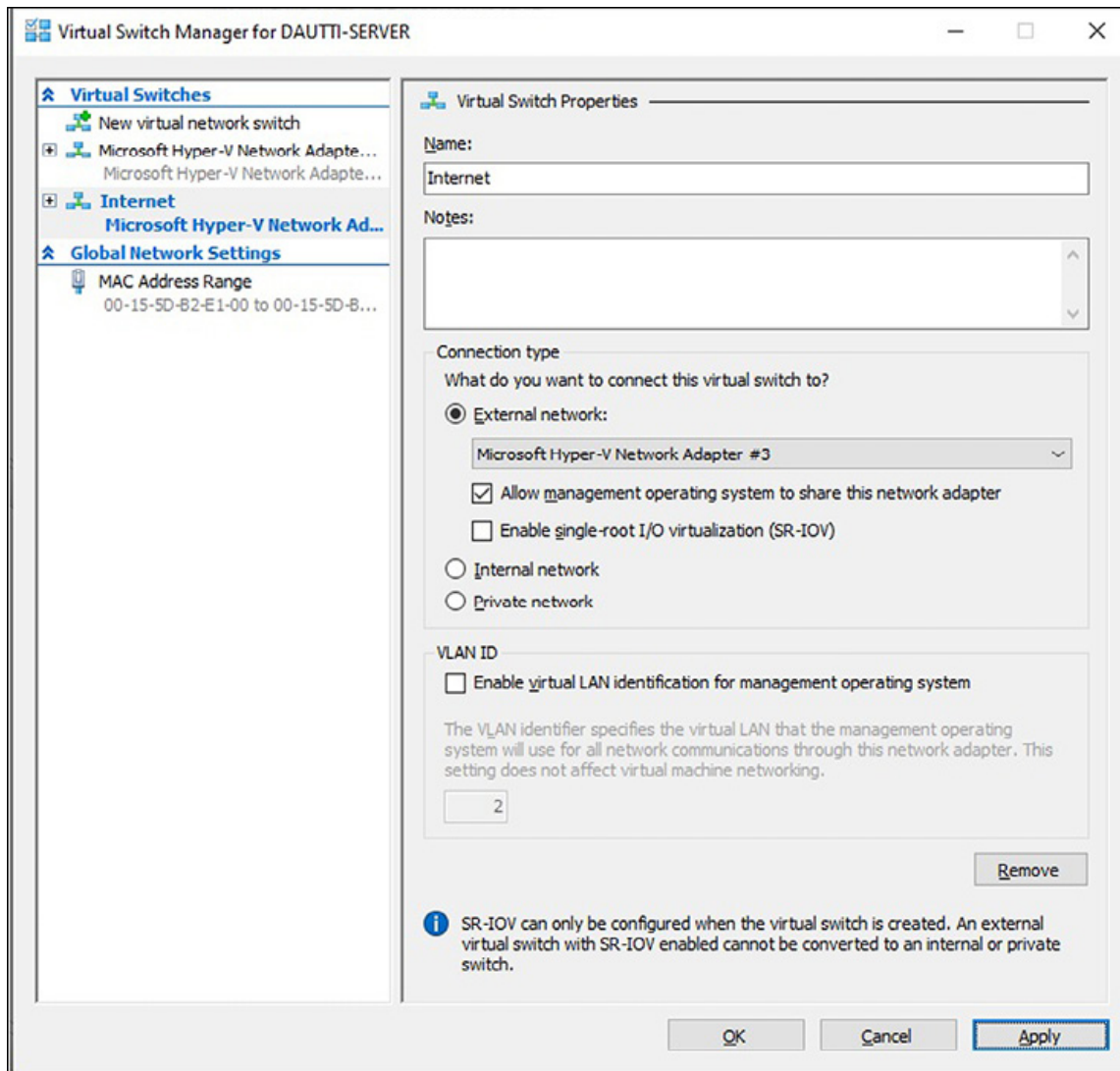
Figure 10.6: A virtual network switch

Answers to Chapter 4 questions

Chapter 4, *Initial Configuration of Windows Server 2022* explains how to perform initial tasks, manage devices and drivers, check the registry and service status, and configure the server. This

chapter also includes questions related to the topic and their answers for easy reference and understanding.

Q1: What are device drivers?

The device driver, shown in *Figure 10.7*, controls and runs the hardware. It can be acquired from a CD/DVD or downloaded from the manufacturer's website.
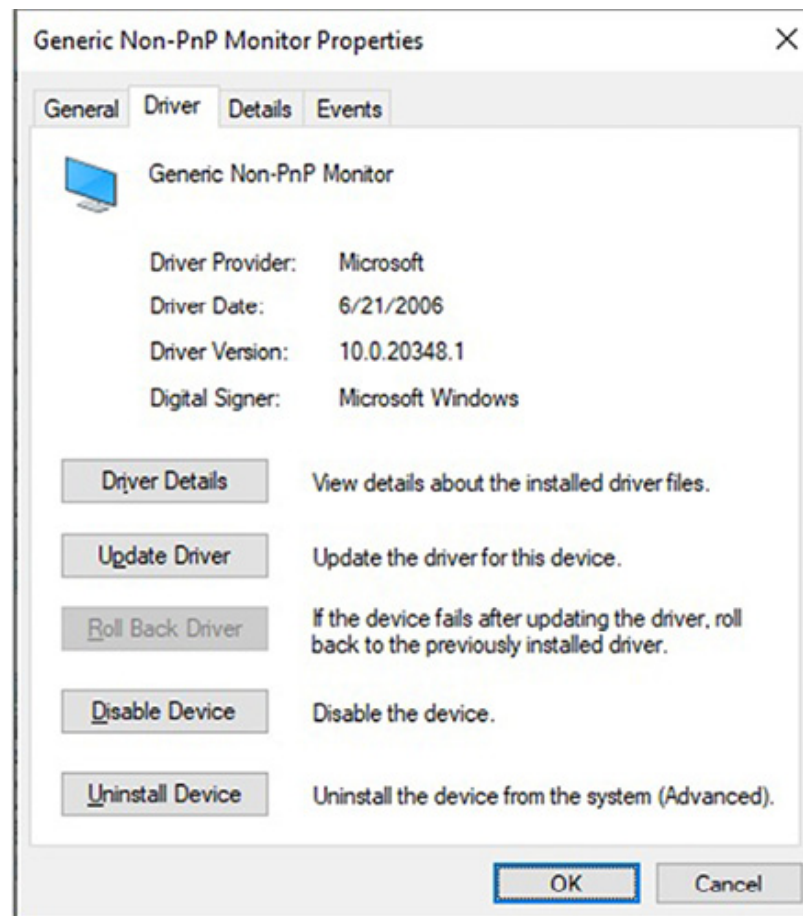
Figure 10.7: A device driver

Q2: What is Windows Registry?

The **Windows Registry**, as shown in *Figure 10.8*, is a database arranged in a hierarchical structure where the operating system stores configuration settings and system information. It is an essential Windows OS part containing details about user preferences, installed hardware, and software.
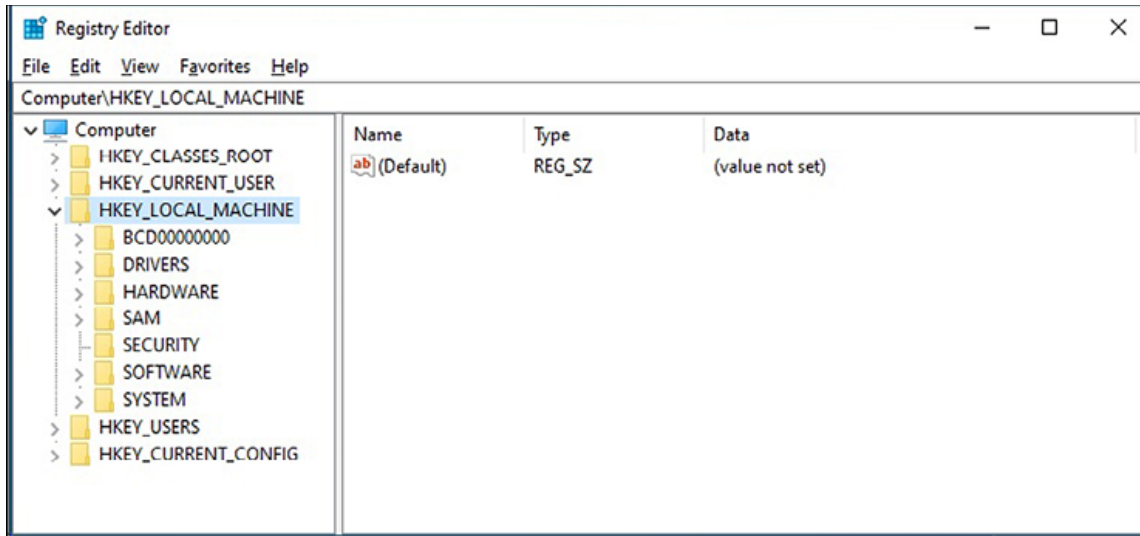
Figure 10.8: Windows Registry

Q3: What are Windows services?

Background programs or services, as shown in *Figure 10.9*, are programs that run in the background of a computer system to provide support for applications and network services. Please refer to the following figure:
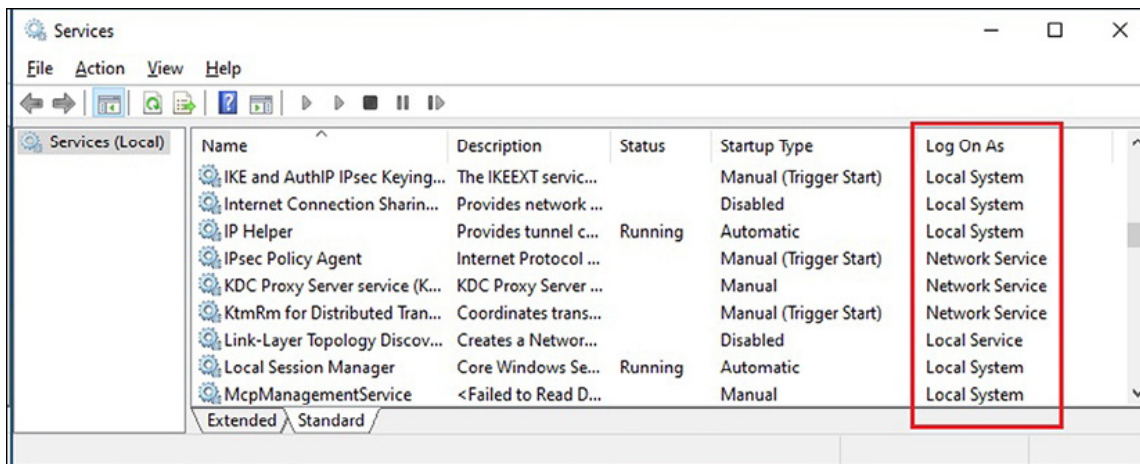
Figure 10.9: Windows services

Q4: Why is initial configuration essential for Windows Server?

Completing the *initial configuration* of a server is an important task that determines its functionality and capability to perform its designated roles. Furthermore, this ensures the server is appropriately configured and prepared for its intended purpose within the IT infrastructure.

Q5: Which tools can you use to run the initial configuration in Windows Server 2022?

The two following tools are available to perform the initial configuration of Windows Server 2022:

- The first tool is **Server Manager**, as shown in *Figure 10.10*, which provides a single interface to manage servers and their roles and features. It enables administrators to perform tasks such as adding or removing roles, configuring settings, and monitoring server performance. Please refer to the following figure:
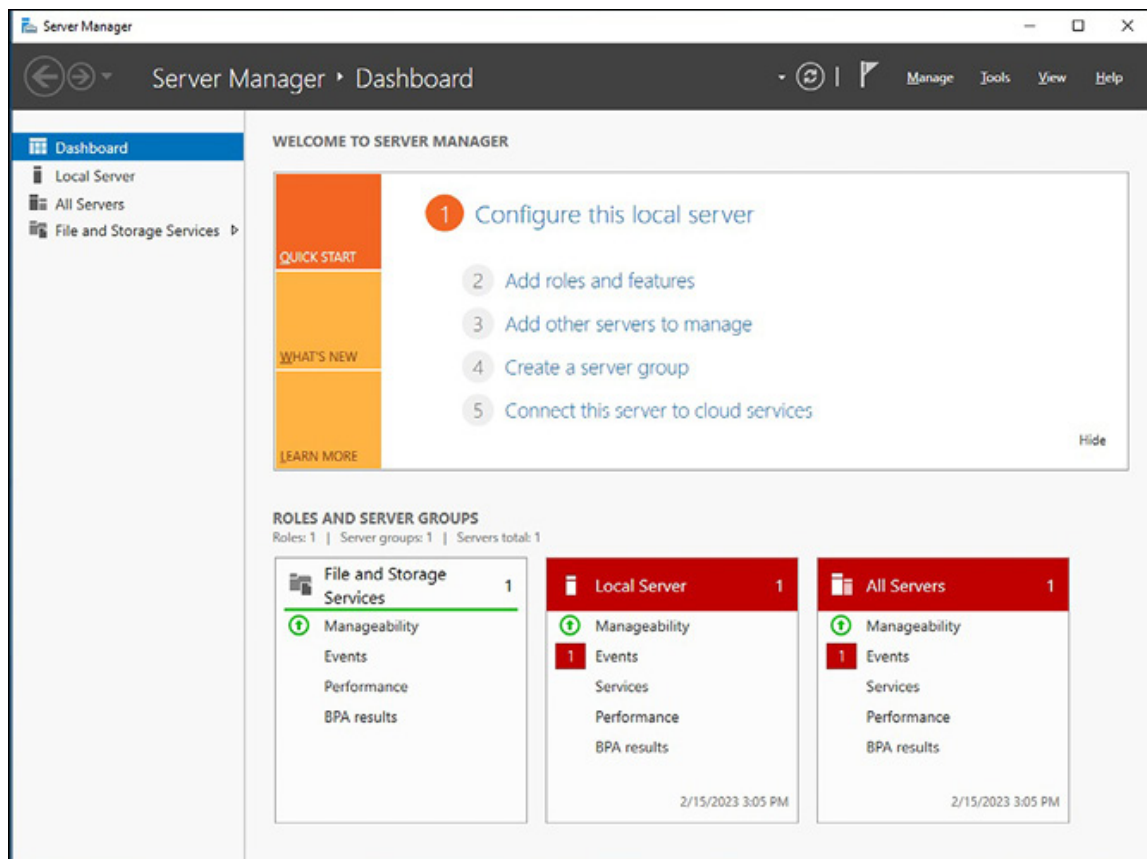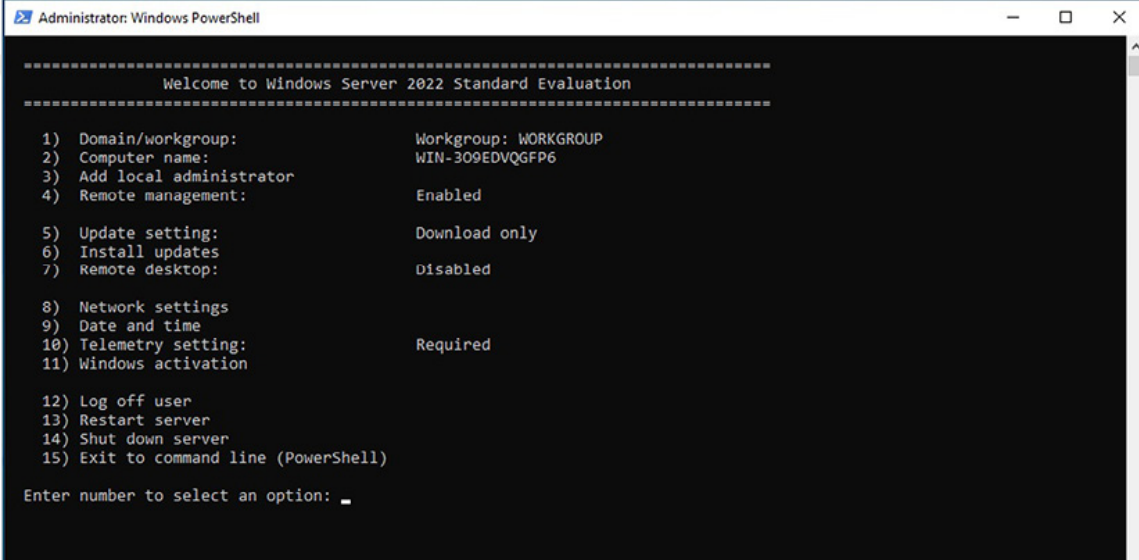
- The second tool is **Server configuration**, a command-line tool that performs basic configuration tasks on a Server Core installation. The server configuration has a menu-driven interface that allows administrators to configure settings like network settings, domain membership, and Windows Update settings. Refer to *Figure 10.11*:

Figure 10.11: Server configuration

Answers to Chapter 5 questions

Chapter 5, *Installing Roles in Windows Server 2022 Using Server Manager and PowerShell* covers the installation of roles in Windows Server 2022 using two methods, the **Add Roles** and **Features Wizard**, available in the Server Manager of Windows Server 2022 and PowerShell. This chapter also includes questions related to the topic and their respective answers to facilitate easy reference and comprehension.

Q1: What is AD DS role?

Active Directory Domain Services (**AD DS**) is an essential element of the Microsoft Windows Server operating system introduced in 2000. A distributed database stores objects such as

users, computers, peripheral devices, and network services in a secure and structured hierarchical format. Refer to *Figure 10.12:*
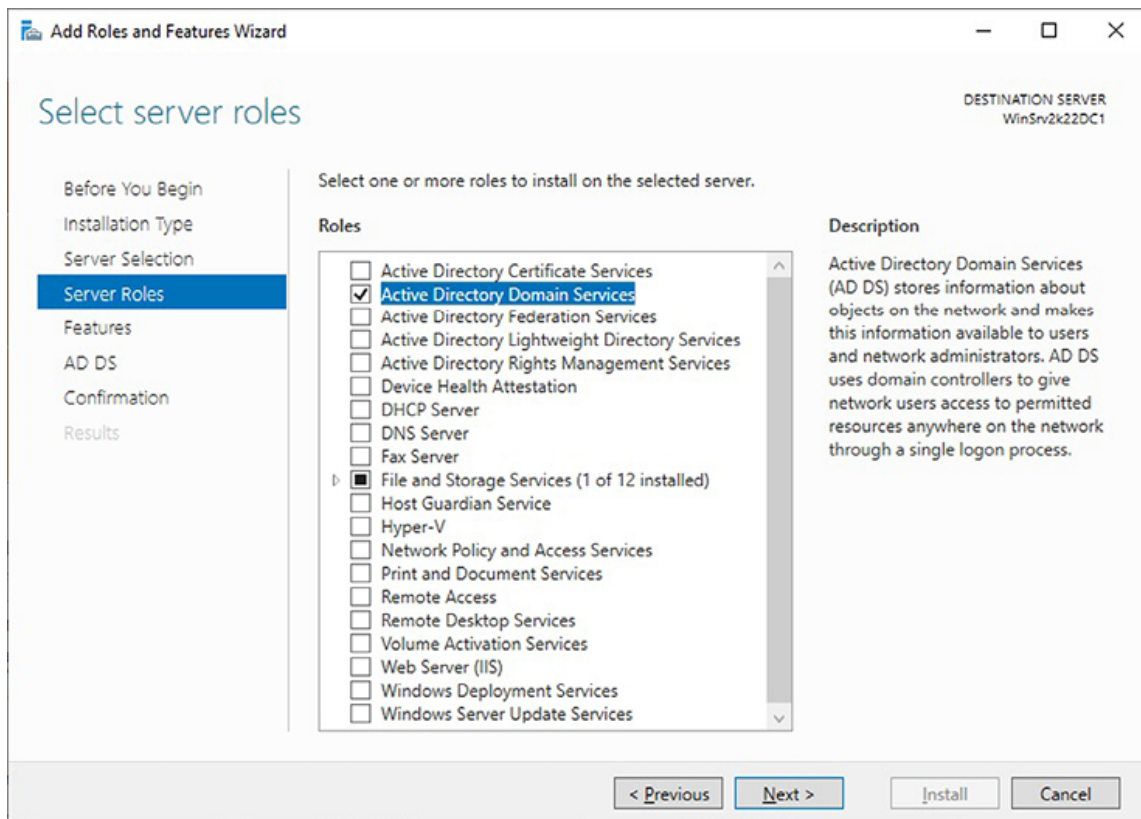
Figure 10.12: *AD DS role*

Q2: What is DNS role?

As shown in *Figure 10.13*, DNS translates user-friendly domain names into IP addresses. It is organized in a hierarchical tree structure, where each branch signifies the root zone, and each leaf can contain multiple resource records. Each area represents a root domain or multiple domains and sub-domains. A domain name comprises one or more labels separated by dots. DNS is managed through a database that employs a distributed client-server architecture, and network nodes represent the names of the servers in such a network. Please refer to the following figure:
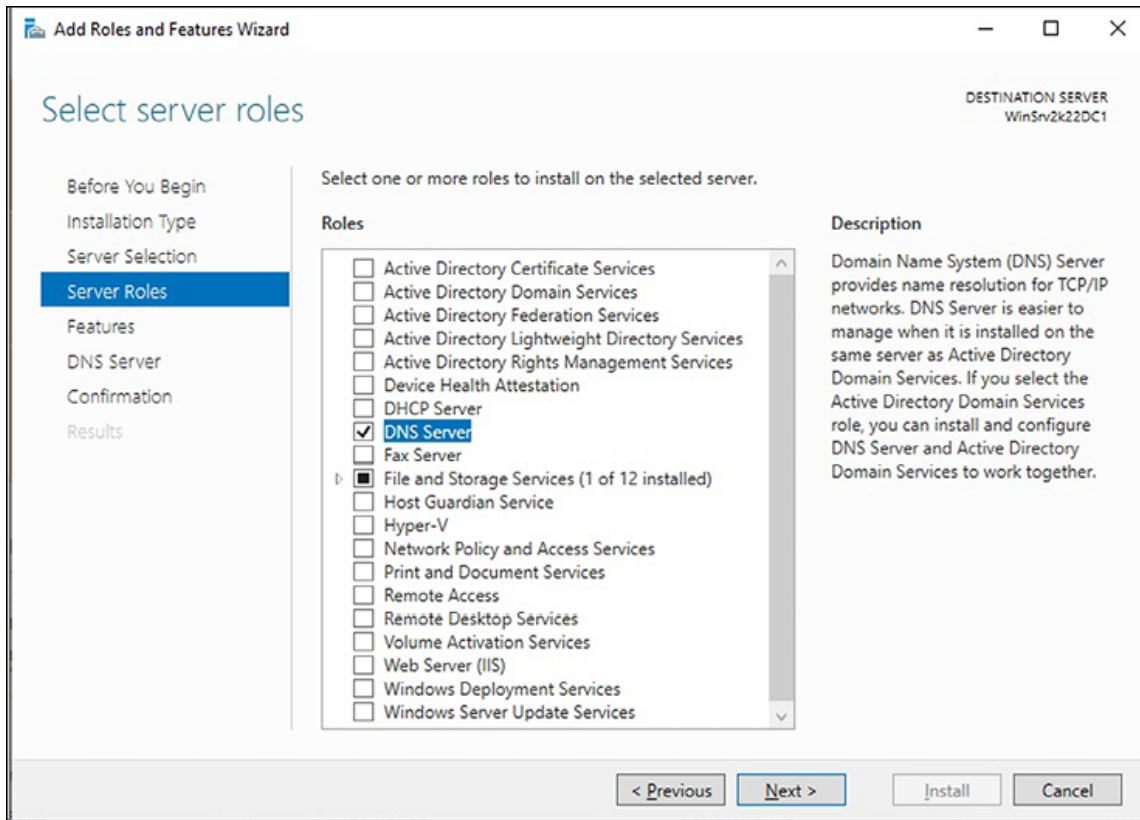
Figure 10.13: *DNS in Windows Server 2022*

Q3: What is the DHCP role?

In essence, **Dynamic Host Configuration Protocol** (**DHCP**) is used in computer networks to assign IP addresses to computers automatically. DHCP works by following a four-step process known as **DORA**, which stands for **Discovery, Offer, Request, and Acknowledgement**. When a computer is turned on and its operating system boots up, the DHCP Client service requests an IP address in the network.

Q4: What is the Web Server role?

Internet Information Services (**IIS**) is a Web server that offers dependable, easy-to-manage, and expandable Web applications. It supports various communication protocols, including HTTP, HTTPS, FTP, FTPS, SMTP, and NNTP, to enable communication between the Web server and the browser. Moreover, it provides dynamic content development on the server side, including

technologies such as **Active Server Pages** (**ASP**). Due to these and other advancements, IIS has become a strong competitor in the Web server market, ranked second to the Apache Web server.

Q5: What is WSUS role?

Windows Server Update Services (**WSUS**), included in Windows Server 2022 is a role that allows system administrators to oversee the delivery of Microsoft's product updates to the computers on their network. Using WSUS, administrators can download updates, patches, and fixes onto their central server and subsequently use it to update the other computers on the web.

Answers to Chapter 6 questions

Chapter 6, Setting Up Windows Server 2022 using Wizards and PowerShell provides detailed instructions on how to set up and configure different network services in Windows Server 2022 using both GUI Wizards and PowerShell. In addition, this chapter contains questions related to the topic and their corresponding answers, which can be used as a quick reference and aid in understanding the material.

Q1: What is the WDS role?

With **Windows Deployment Services** (**WDS**), you can install Windows operating systems on your corporate network. To do this, you must set up a WDS server, which allows you to set up new computers using a network-based installation.

Q2: What is PDS role?

Print and Document Services (**PDS**) is a network service that provides a centralized print server and allows printing jobs to be managed on the network. However, PDS is not just limited to printing services but also offers document scanning services on the web. With PDS's scanning service, network users can receive scanned documents from the network scanner and send them to shared resources on the network.

Q3: What is remote access?

The Remote Access role in Windows Server 2022, as shown in *Figure 10.14*, enables remote access to services, which differs from **Remote Desktop Services** (**RDS**). It encompasses several network access technologies, including the following:

- **DirectAccess** was introduced in Windows Server 2008 R2 and encrypted communication between the client and server, encapsulating IPv6 traffic over IPv4 to reach the intranet via the internet.

- **Routing and Remote Access Service** (**RRAS**), a successor to **Remote Access Service** (**RAS**) in Windows NT, was introduced in Windows 2000 and establishes links between remote locations via **Virtual Private Network** (**VPN**) and Dial-up and traffic paths between sub-networks.

- **Web Application Proxy** replaced Microsoft Forefront **Unified Access Gateway** (**UAG**) in Windows Server 2022 and served as a recursive proxy.

Refer to *Figure 10.14:*
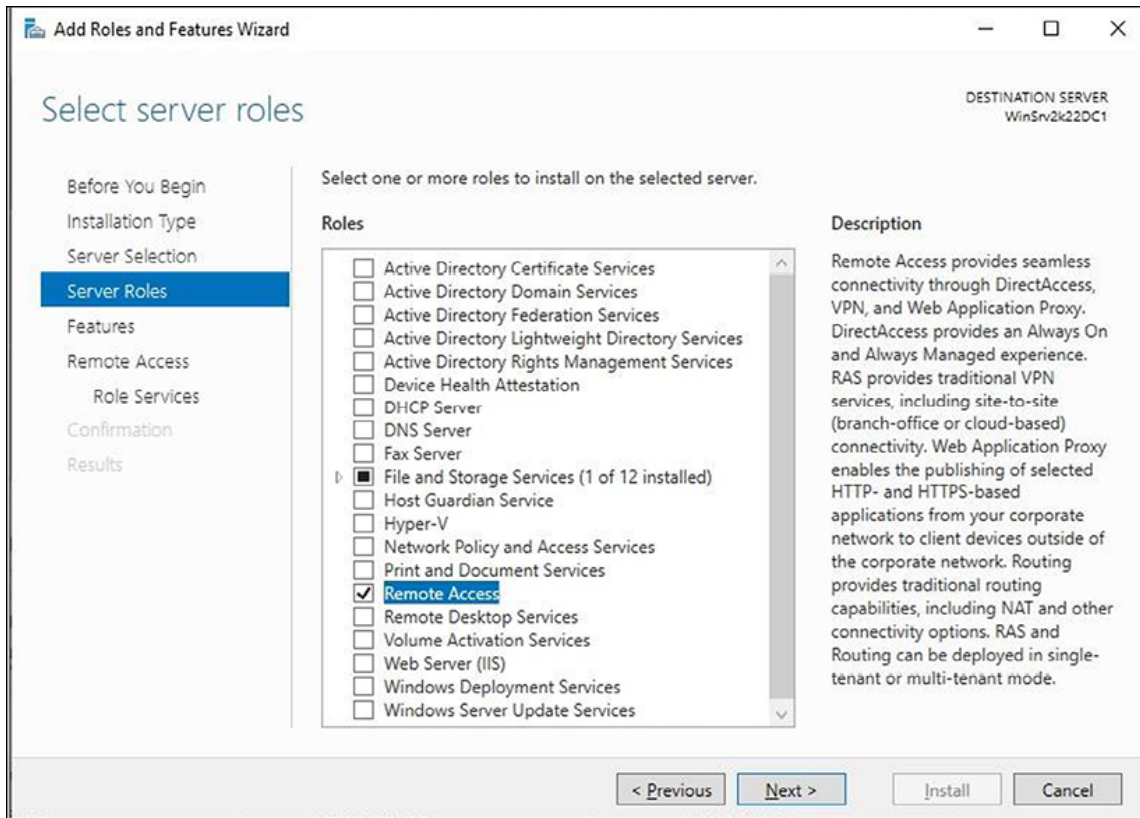
Figure 10.14: Remote access role

Q4: What is RDS role?

Remote Desktop Services (**RDS**), previously known as **Terminal Services** (**TS**) until Windows Server 2008, allows remote access to computers on a corporate network or over the internet. Regarding functionality, the central component of RDS is a Terminal Server that uses TCP port 3389.

Q5: What is NPAS role?

The **Network Policy and Access Services** (**NPAS**) role is designed to provide network access services for local and wide area networks while allowing the establishment and enforcement of policies for network access authorization, authentication, and client health. In Windows Server 2022, this role encompasses the following role services:

- **Network Policy Server** (**NPS**)
- **Health Registration Authority** (**HRA**)

- **Host Credential Authorization Protocol** (**HCAP**)

Answers to Chapter 7 questions

Chapter 7, *Tuning Windows Server 2022 for Peak Performance* explains the roles of hardware components in a computer network. Then, this chapter moves on to performance monitoring, which is crucial for maintaining the server's optimal performance and troubleshooting issues when they occur. In addition, this chapter provides a detailed explanation of the Windows Admin Center and its tools and features, which is a vital tool for sysadmins to monitor server performance effectively. This chapter also includes questions related to the topic and their answers to facilitate easy reference and comprehension.

Q1: Mention some of the server's miscellaneous hardware

Various miscellaneous hardware may be installed on a server, such as:

- **Processor architecture**, which may be 32-bit or 64-bit.
- **Removable drives** provide a way to store data externally and move it between devices.
- **Graphics cards** may or may not be needed depending on the server's intended use.
- **Cooling systems**, including processor coolers and case fans, help dissipate heat generated by the server.
- **Power supplies**, convert AC power to DC, and supply it to the motherboard and peripheral devices.

Q2: What is a Performance Monitor?

The Performance Monitor, shown in *Figure 10.15*, is a crucial tool for server admins that offers comprehensive information on the server's performance. It allows administrators to detect and fix any issues or obstacles impacting the server's availability or performance. In addition, the tool displays performance data

visually, making it easy to track real-time server performance or access data from log files. Please refer to the following figure:
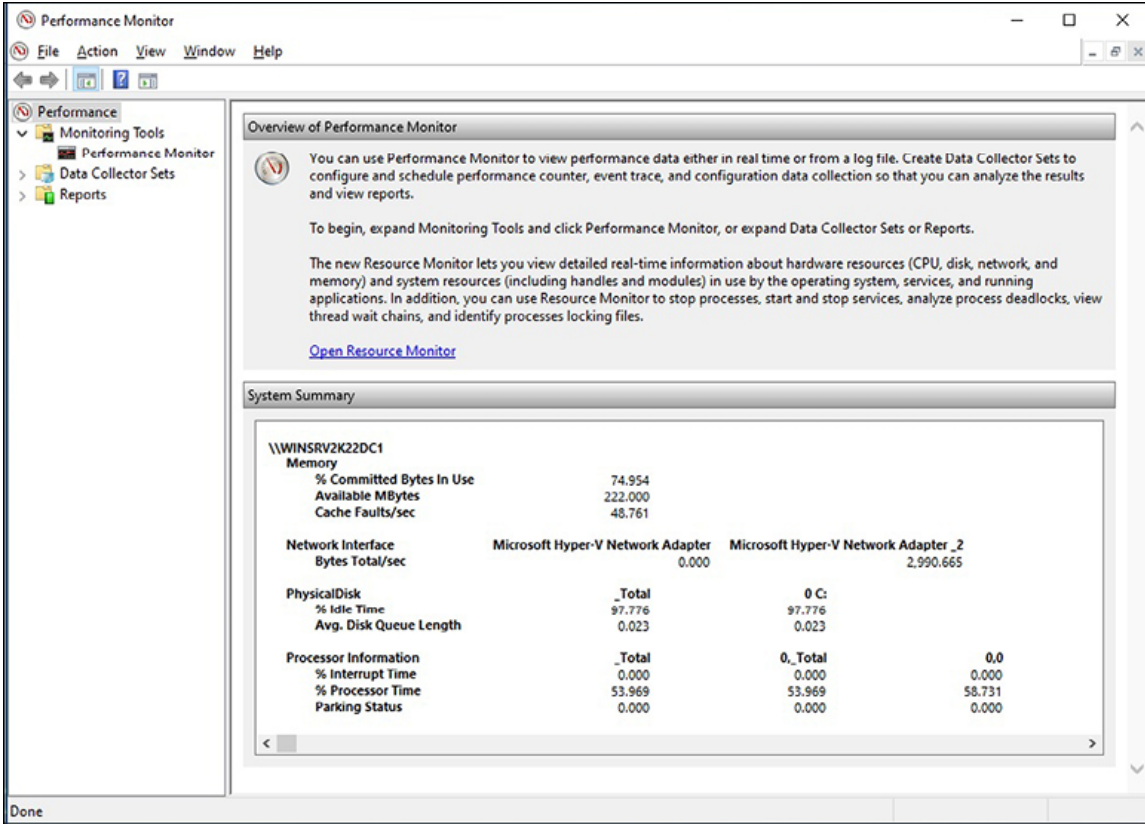
Figure 10.15: *Performance Monitor*

Q3: What is a Resource Monitor?

Windows Server 2022 includes a Resource Monitor tool that can help diagnose the reasons for slow performance on a computer or server. This tool monitors hardware and software resources in real-time, making it possible to identify the components responsible for slow performance. Refer to *Figure 10.16:*
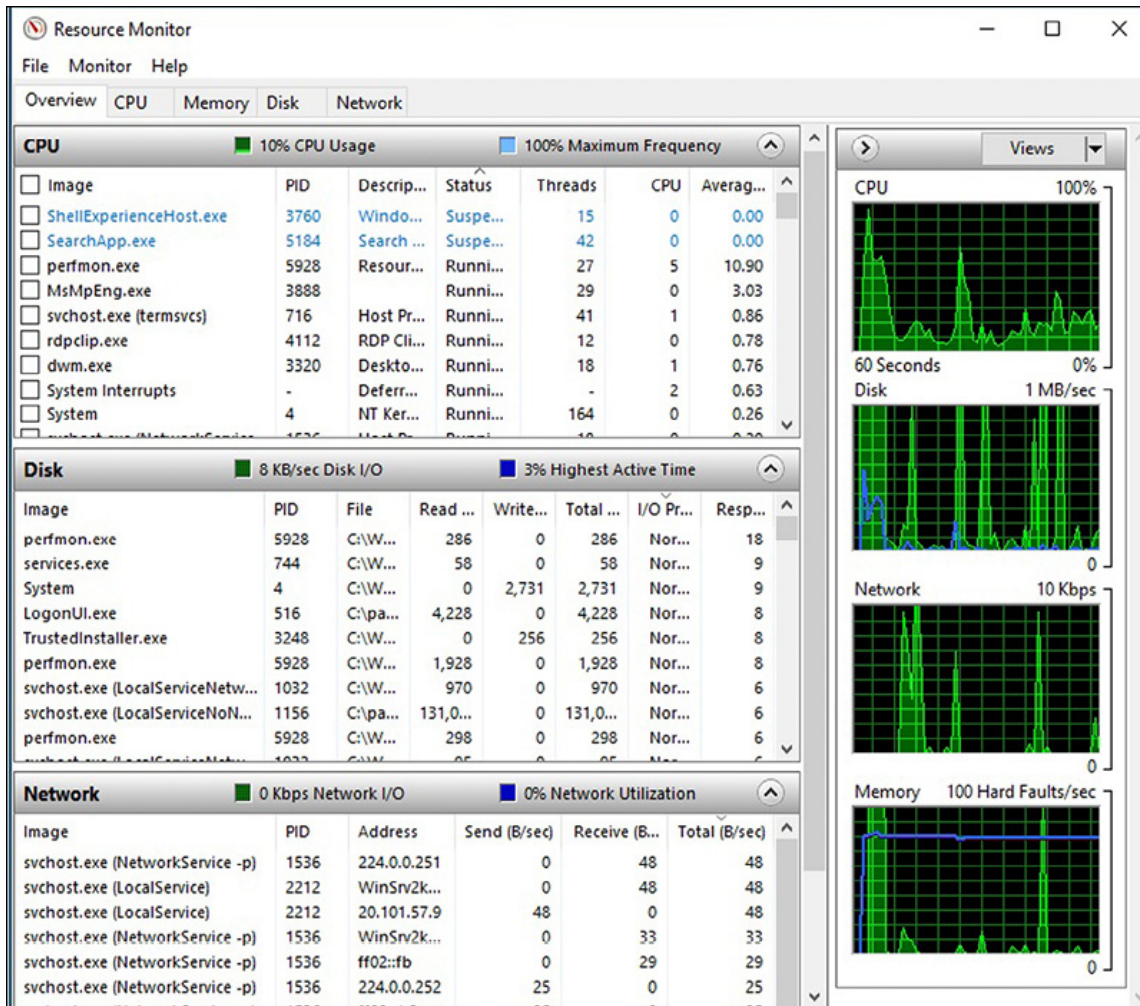
Figure 10.16: *Resource Monitor*

Q4: What is a Task Manager?

Task Manager, shown in *Figure 10.17*, is a pre-installed Windows tool that enables users to oversee and control running processes, services, and performance on a server. It presents a visual display of the server's status, including a summary and graph view, making it simple for users to comprehend the server's current condition. Furthermore, Task Manager allows users to initiate or terminate background processes and applications.
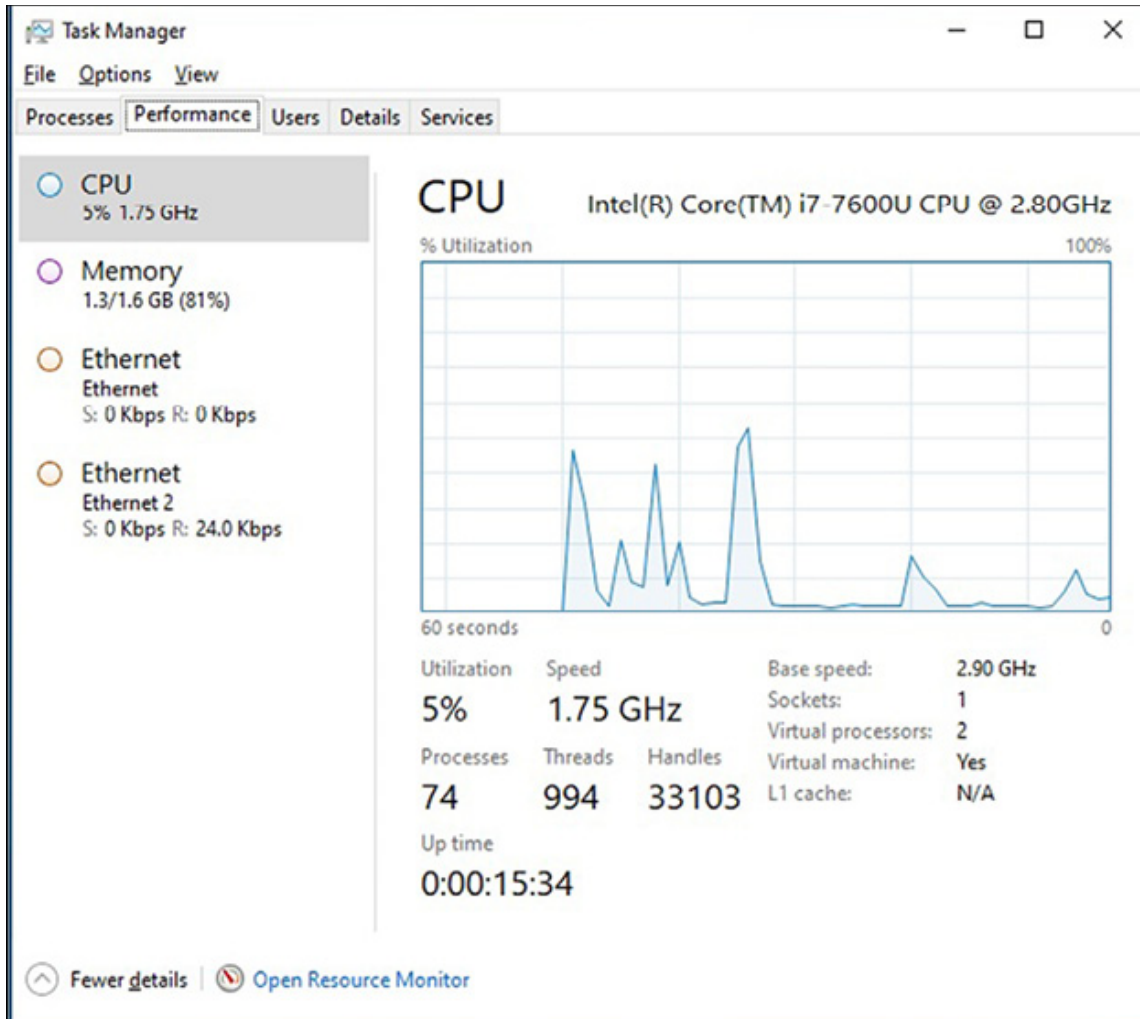
Figure 10.17: Task Manager

Q5: What is Windows Admin Center?

Windows Admin Center (**WAC**) is an advanced tool created for server management purposes. It can be accessed remotely, and administrators can manage their Windows servers using a Web-based interface. In addition, WAC provides a wide range of tools and features that enable administrators to manage and monitor various aspects of their server infrastructure more efficiently, thus enhancing system efficiency and maintenance.

Answers to Chapter 8 questions

Chapter 8, *Maintaining and Resolving Issues in Windows Server 2022* delves into the significance of troubleshooting, updating, monitoring, and maintaining servers to improve the business continuity standards that are vital to the success of any organization. It covers various topics, including the server startup process and advanced boot options, Safe Mode, backup and restore disaster recovery plan, and updating the Windows Server 2022, server hardware, and third-party software. Furthermore, the chapter includes questions about the subject and their corresponding answers to aid easy reference and understanding.

Q1: What is the startup process?

Starting a server is essential to minimize downtime, ensure smooth operation, and troubleshoot hardware-related issues. The first step of the startup process is the **Basic Input/Output System** (**BIOS**), which initializes the hardware components and checks for any errors before loading the operating system. The process ends with the initializing operating system, thus being ready for the user's session.

Q2: How is business continuity maintained?

In today's technology-dependent world, minimizing downtime is a crucial responsibility for system administrators. Downtime can lead to financial losses for the company, and it is vital to assess components at risk of failure and take proactive measures to prevent them. Identifying potential points of failure and taking necessary actions can help minimize downtime and ensure smooth system operation. By doing so, system administrators can help companies increase *business productivity* and reduce losses caused by system failures.

Q3: What is a Windows Update?

Every second Tuesday of the month, Microsoft releases updates, also known as Patch Tuesday, which contain the latest features, security updates, and fixes for Microsoft operating systems and programs, including Windows Server 2022. These updates are available through Microsoft's **Windows Update** server, accessed

via the Windows Update feature or the official website. In addition, users will receive notifications about available updates in the system tray and Notification Center.

Refer to *Figure 10.18:*
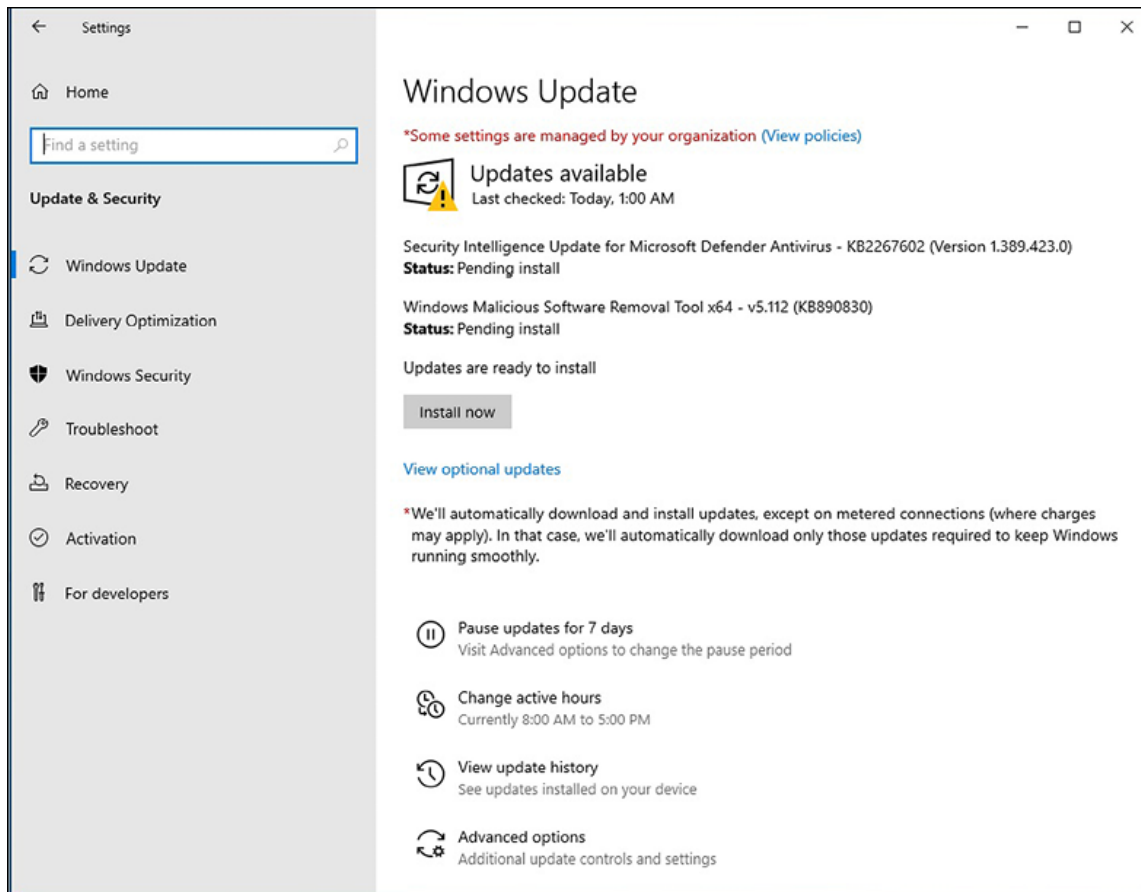
Figure 10.18: *Windows Update*

Q4: What is troubleshooting?

Practicing and gaining experience is essential to master *troubleshooting*, a vital skill for IT professionals. Solving IT problems builds the problem solver's confidence and knowledge base, and it is crucial to continue learning and practicing troubleshooting to enhance proficiency. With increased ability, IT professionals can more effectively solve problems.

Q5: What is Event Viewer?

The Event Viewer, shown in *Figure 10.19*, is a tool within the Windows OS that helps system administrators track server events and diagnose software, hardware, and network-related problems that may affect the server. Nevertheless, it is worth noting that a system operating correctly can still display various warnings and errors in the Event Viewer.
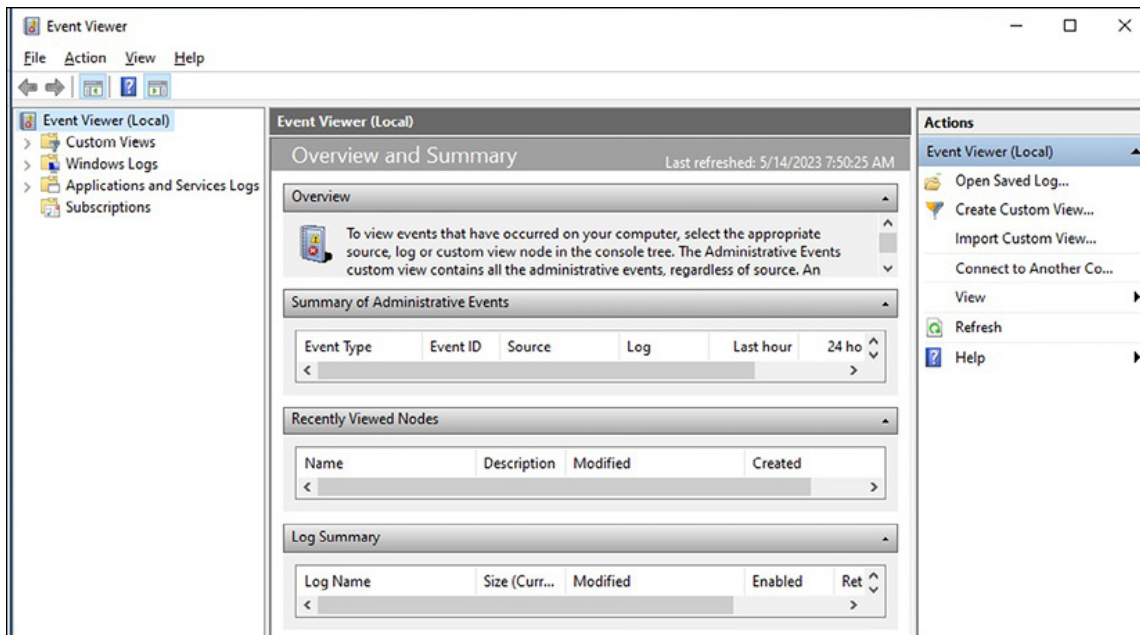
Figure 10.19: *Event Viewer*

Conclusion

In this chapter, you have learned valuable insights and clarity on questions raised throughout the book. The answers provided serve as a comprehensive review of the book's content, helping you deepen your understanding of the material and fully grasp the main ideas and concepts presented throughout the book. This chapter is a valuable resource for students, educators, and anyone looking to reinforce their knowledge of the subject matter. This chapter can be beneficial for exam preparation or for individuals who wish to test their understanding of the material. Overall, the answers provided in this chapter are a valuable reference for anyone seeking to enhance their knowledge of the book's subject matter and achieve their learning goals.

Join our book's Discord space

Join the book's Discord Workspace for Latest updates, Offers, Tech happenings around the world, New Release and Sessions with the Authors:

https://discord.bpbonline.com

Index

L

O

P

T