9

Managing Storage

In this chapter, we cover the following recipes:

* Managing Physical Disks and Volumes
* Managing File Systems
* Exploring Providers and the File System provider
* Managing Storage Replica
* Deploying Storage Spaces

# Introduction

Windows Server 2019 provides a range of features that allows access to a wide variety of storage and storage devices. Windows supports spinning disks, USB memory sticks, and SSD devices (including MVMe SSD devices).

Before a disk can be used, you need to create partitions or volumes on the device, then format the volume. When you first initialize a disk, you need to define which partitioning method to use. You have two choices: Master Boot Record (MBR) or GUID Partition Table (GPT). For a good discussion of the differences between these two mechanisms, see: https://www.howtogeek.com/193669/whats-the-difference-between-gptand-mbr-when-partitioning-a-drive/.

With a volume created, you can then format the disk volume. Windows supports five key filesystems you can use: ReFS, NTFS, exFAT, UDF, and FAT32. For details of the latter four, see: https://docs.microsoft.com/en-us/windows/desktop/fileio/filesystemfunctionality-comparison. The ReFS filesystem is newer and is based on NFTS, but lacks some features a file server might need (it has no encrypted files). For a comparison between the ReFS and NTFS filesystems, see: https://www.iperiusbackup.net/en/refs-vs-ntfs-differences-and-performance-comparison-when-to-use/. You examine partitioning and formatting volumes in the Managing physical disks and disk volumes recipe.

NTFS (and ReFS) volumes allow you to create access control lists (ACLs) that control access to files and folders stored in Windows volumes. Managing ACLs is somewhat difficult and lacks rich PowerShell support. To manage ACLs on NTFS volumes, as you will see in the Managing NTFS Permissions recipe, you can download and use a third-party module, NTFSSecurity.

The Windows File Server Resource Manager (FSRM) feature in Windows Server 2022 which helps  
you to manage filestore resources. With FSRM, you can set Filestore quotas. With soft quotas, users can exceed their Filestore quota and administrators are notified when this occurs. With hard quotas, users are prohibited from storing more than their allocated quotas. You work with quotas in the Managing Filestore Quotas recipe.

FSRM also supports detailed file server reporting, which you examine in the Using filesystem reporting recipe. These reports, and the supporting XML files, can provide assistance in managing and controlling file servers.

This chapter, specifically the Managing Filestore quotas recipe, makes use of a free email  
account from Sendgrid.com. This enables you to set up the Windows SMTP server to  
forward mail to SendGrid for onward transmission. This could be a great way to test reporting  
or to avoid issues with internal SMTP servers.

# Managing Physical Disks and Volumes

## Getting Ready

This recipe uses SRV2, a recently added workgroup host. By default, this host is a DHCP client.

## How to do it...

## How it works...

## There's more...

# Managing File Systems

## Getting Ready

This recipe uses SRV2, a workgroup host. You gave this host a static IP address in “Configuring IP Addressing”.

## How to do it...

## How it works...

# Exploring Providers and the File System Provider

## Getting Ready

This recipe uses DC1, a domain controller in the Reskit.Org domain. You should have installed AD on this host and configured it as per earlier recipes in Chapter 5 and Chapter 6.

## How to do it...

## How it works...

In step 1,

# Managing Storage Replica

## Getting Ready

You run this recipe on DC1, a domain controller in the Reskit.Org domain after installing the DHCP server service. You must have installed PowerShell 7 and VS Code on this host.

## How to do it...

## How it works...

# Deploying Storage Spaces

After installing the DHCP service and configuring scope(s) and option values, your DHCP services can issue IP configuration data to any client. Since the DHCP protocol acts at the IP level, the protocol performs no authentication when any DHCP client uses the protocol to request IP configuration details. That means that any client you attach to the physical subnet can ask for and receive IP confirmation details.

In “Configure IP Addressing”, you set a static IP address for SRV2. In this recipe, you reconfigure this server to obtain a DHCP based IP address (and options you set in “Configure DHCP Scopes and Options”.

## Getting Ready

You run this recipe on SRV2 which you reconfigure to get its address via DHCP. You also need DC1, a domain controller for the reskit.org domain and a DHCP server which you set up and configured in earlier recipes in this chapter.

## How to do it...

## How it works...

Obtaining a lease can take a few seconds, so be patient.