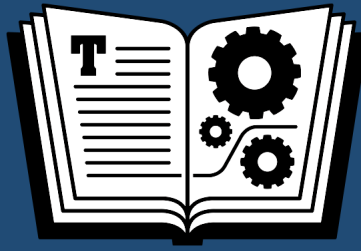


EBOOK EXTRAS: v3.1
Downloads, Updates, Feedback



TAKE CONTROL OF
**BACKING UP
YOUR MAC**

by **JOE KISSELL**
\$14.99

3rd
EDITION

Table of Contents

Read Me First.....	5
Updates and More	5
Basics	6
What's New in Version 3.1	6
What Was New in the Third Edition	7
Introduction	10
Quick Start	12
Plan a Backup Strategy	14
Understand Joe's Basic Backup Strategy	14
Why Create Versioned Backups?	16
Why Create Bootable Duplicates?	19
Why Use an External Hard Drive?	21
Why Use Multiple Partitions?	23
Why Automate Backups?	23
Why Keep Multiple Backups?	25
Why Store Backups Offsite?	26
Can Cloud Sync Simplify Backups?	27
Can You Reduce Your Backup Footprint?	29
Reassess Your Backup Strategy	31
What's New in Mac Backups	31
Factors to Reevaluate	37
Choose Local or Network Backups	42
Local Backups	42
Network Backups	43
Local vs. Network Backups: Joe's Recommendations	47
Choose Backup Software	50
Decide If Time Machine Is Best for You	50
Explore Versioned Backup Features	54

Choose Another Versioned Backup App	67
Choose a Bootable Duplicate App	72
Choose Backup Hardware	73
Decide on Capacity	73
Decide on a Storage Configuration	77
Hardware You Should Probably Avoid	92
Prepare Your Hard Drive	95
Choose a Partition Map Scheme	95
Decide How Many Partitions to Make	98
Configure Your Drive	99
Configure and Use Time Machine	105
Time Machine Basics	105
Choose a Destination	106
Exclude Files from Time Machine	108
Restore Data with Time Machine	116
Delete Files from a Time Machine Backup	127
Encrypt Your Time Machine Backup	129
Use a Mac as a Time Machine Server	131
Use a Single Backup Disk with Multiple Macs	135
Use Power Nap	137
Manage Your Time Machine Schedule	138
Migrate to a Larger Time Machine Disk	141
Avoid or Solve Time Machine Problems	145
Use Other Versioned Backup Software	148
Arq Tips	148
ChronoSync Tips	150
DollyDrive Tips	152
QRecall Tips	152
Retrospect Tips	153
Test Your Versioned Backup	156
Create and Use a Bootable Duplicate	158
Give the Destination Volume a Unique Name	160
Create a Duplicate with Carbon Copy Cloner	160

Create a Duplicate with SuperDuper!	162
Test Your Duplicate	164
Store an Extra Backup Offsite	167
Use an Extra Hard Drive	167
Use a Cloud Backup Service	169
What to Do When Disaster Strikes	178
Restore Individual Files.....	178
Use Your Bootable Duplicate	179
Restore a Disk from a Bootable Duplicate	181
Manage Your Media	184
What to Do When Your Disks Fill Up	184
Consider Long-Term Archive Storage	186
Consider Special Backup Needs	189
Back Up Digital Photos	189
Deal with Huge Volumes of Data	193
Back Up a NAS	197
Back Up Data from the Cloud	199
Back Up While on the Road	202
Back Up an iOS Device	205
Back Up Windows Files and Volumes	207
About This Book.....	215
Ebook Extras.....	215
About the Author and Publisher	216
Credits	216
Also by Joe Kissell	217
Copyright and Fine Print	218

Read Me First

Welcome to *Take Control of Backing Up Your Mac, Third Edition*, version 3.1, published in January 2019 by alt concepts inc. This book was written by Joe Kissell and edited by Caroline Rose.

The data on every Mac should be backed up to protect against theft, hardware failure, user error, and other catastrophes. This book helps you design a sensible backup strategy, choose and configure the best backup hardware and software for your needs, and understand how to make your backups as painless as possible.

If you want to share this ebook with a friend, we ask that you do so as you would with a physical book: “lend” it for a quick look, but ask your friend to buy a copy for careful reading or reference. Discounted [classroom and Mac user group copies](#) are available.

Copyright © 2019, alt concepts inc. All rights reserved.

Updates and More

You can access extras related to this ebook on the web (use the link in [Ebook Extras](#), near the end; it’s available only to purchasers). On the ebook’s Take Control Extras page, you can:

- Download any available new version of the ebook for free, or buy any subsequent edition at a discount.
- Download various formats, including PDF, EPUB, and Mobipocket. (Learn about reading on mobile devices on our [Device Advice](#) page.)
- Read the ebook’s blog. You may find new tips or information, as well as a link to an author interview.

If you bought this ebook from the Take Control website, it has been added to your account, where you can download it in other formats

and access any future updates. However, if you bought this ebook elsewhere, you can add it to your account manually; see [Ebook Extras](#).

Basics

To review background information that might help you understand this book better, such as finding System Preferences and working with files in the Finder, I recommend reading Tonya Engst’s ebook [Take Control of Mac Basics](#).

In this book, when I use the term *disk* by itself, I generally mean your Mac’s primary internal storage device—whether that’s a mechanical hard drive, an SSD, or other solid-state storage. (Apple, after all, still uses the term “Macintosh HD” as the default name for your Mac’s startup volume, even when it’s not stored on a hard disk.) A *drive* is a physical device for storing data; a single drive can comprise one or more *volumes*, or logical storage devices. The volume that contains the copy of macOS currently used to boot your Mac is your *startup volume*. I’ll specify *hard drive* when I need to talk specifically about the little boxes with spinning platters.

What’s New in Version 3.1

Version 3.1 is a minor revision that brings this book up to date with macOS 10.14 Mojave and various changes in hardware and software. Along with numerous small edits, this version contains the following significant changes:

- Added a lot of new information in [What’s New in Mac Backups](#), including mentions of the end of Prosoft Data Backup and of Apple’s Time Capsules, the beginning of Retrospect Solo, continuing changes related to APFS, and things owners of new Macs equipped with T2 chips will need to know about backups

- Included more information about snapshots in APFS; see the note in [Snapshots and File Lists](#) and changes to the sidebar [Local Snapshots](#)
- Removed various mentions of Data Backup and other products that are no longer available
- Added information in [Retrospect](#) and [Retrospect Tips](#) about the new Retrospect Solo app
- Made several mentions of Jeff Carlson’s new (and highly relevant) book [*Take Control of Your Digital Storage*](#)
- Updated [Creating a RAID with SoftRAID](#) to discuss issues relating to APFS volumes
- Stripped most of the discussion of Time Capsules from [Network Storage Devices](#)
- Updated [Configure a Drive in El Capitan or Later](#) to cover cases in which APFS is a suitable format
- Added a sidebar about putting [APFS Bootable Duplicates on HFS Plus Volumes](#)
- Included notes in [Test Your Duplicate](#) and [Use Your Bootable Duplicate](#) about booting Macs with T2 chips from external drives
- Gave a different example of a cloud backup service in [HIPAA and Cloud Backups](#)
- Added a potential downside to Backblaze in [Self-Contained Cloud Backup Services](#)

What Was New in the Third Edition

The book you’re now reading has a long and complex history, having gone through various title changes, splits, and merges stretching all the way back to 2004—and the third edition of this book (version 3.0) represented not only a change in its version number but also in its title.

This book's most recent ancestor in the Take Control series was *Take Control of Backing Up Your Mac, Second Edition*, which was published in November 2014. I subsequently acquired publication rights to the book, updated it significantly, and rereleased it with a new title (*Backing Up Your Mac: A Joe On Tech Guide*) in May 2015. The second edition of that title appeared in June 2016, followed by a version 2.1 update in September 2016.

After I purchased Take Control Books from TidBITS Publishing Inc. in May 2017, I decided to bring this book back under the Take Control umbrella. That meant reverting to its previous title and incrementing the edition number by one (even though there were, in effect, two editions of the book between the second and third).

It would take many pages to detail the differences in each iteration of the book (and the third edition alone contains hundreds of changes), but here are the most significant changes since *Backing Up Your Mac: A Joe On Tech Guide*, version 2.1:

- Updated the entire book for compatibility with macOS 10.13 High Sierra; see [APFS Evolves in Mojave](#) for an overview
- Removed coverage of CrashPlan, except for the explanation of why I no longer recommend it; see [CrashPlan for Home Is Finally Gone](#)
- Removed coverage of FireWire (which hasn't been seen on new Macs in many years) and eSATA (which was never a built-in option), while saying more about Thunderbolt 3 and USB-C
- Updated information on various cloud storage and backup services; see [Use a Cloud Backup Service](#)
- Expanded [Factors to Reevaluate](#) to cover Optimized Storage (in 10.12 Sierra and later) and network backups
- Added a new chapter, [Choose Local or Network Backups](#), to explore the relative merits of using a hard drive connected directly to your Mac versus a NAS, Time Capsule, or Mac server
- Removed coverage of Synk, which has been discontinued

- Totally reorganized, updated, and expanded the [Choose Backup Hardware](#) chapter; new topics include [Decide on a Storage Configuration](#) and [Evaluate Network Storage Options](#)
- Added a sidebar on why to [Keep Time Machine Backups Separate from Other Data](#)
- Updated the [Configure and Use Time Machine](#) chapter to cover High Sierra changes (such as the new topic [Use a Mac as a Time Machine Server](#)), add advice, and remove obsolete information
- Updated the tips for using Arq, ChronoSync, and Data Backup in [Use Other Versioned Backup Software](#)
- Updated the instructions for using Carbon Copy Cloner and SuperDuper! in [Create and Use a Bootable Duplicate](#)
- Updated [Self-Contained Cloud Backup Services](#) with new information on Acronis True Image and IDrive, and updated information about Backblaze and DollyDrive
- Updated [BYOS \(Bring Your Own Software\) Internet Backups](#) with current pricing, plus information on Wasabi
- Updated [Back Up Data from the Cloud](#) with current details about several providers

Introduction

The first time I thought seriously about backups was right after I lost a valuable, irreplaceable piece of data—an email message sent to me by a celebrity—as the result of a disk crash. That was more than 20 years ago, and ever since, I’ve practiced and preached diligent Mac backups. After all, Macs may be fantastic computers, but they’re still subject to electronic and mechanical failure, theft, human error, and many other problems that could cause anyone to lose data.

My first book about Mac backups was published in 2004. Back then, I found that many readers still needed convincing that hard drives were better for backups than CDs, that backups ought to run without manual intervention, and even that backups were worth the bother in the first place. When Apple introduced Time Machine as a built-in backup feature in Mac OS X 10.5 Leopard in 2007, backups became easier to perform and harder to ignore. Although Time Machine isn’t the only way (or even, necessarily, the best way) to back up your Mac, it has done more to popularize the concept of Mac backups than anything that came before it, and it set a new standard for usability.

If you don’t back up your Mac at all—or if you do so only haphazardly—this book will help you over the initial hump of getting started with a solid backup plan. Having great backups no longer requires lots of money, time, or technical expertise. You can be up and running in a couple of hours, after which things will run mostly on their own, and the only time you’ll have to think about your backups is when it comes time to restore lost data—something you won’t have to fear anymore.

On the other hand, if you already have a backup system, it might be time for you to update it. Technology changes rapidly, and you could find that a different approach (or newer hardware, software, or cloud services) will serve your current needs better.

This book explains how to develop a solid backup strategy, what your hardware and software choices are, how to set everything up, what pitfalls you may encounter, and how to restore your data if disaster

strikes. Rather than explore every alternative, I guide you gently but firmly into a fairly narrow set of options that should yield excellent results for the vast majority of Mac users.

Before we get started, I need to mention a few qualifications:

- This book is primarily for people who need to back up either a single Mac or a small network—not for system administrators who need to back up dozens or hundreds of machines. As a result, I say little about the high-end equipment and enterprise-grade software used for backing up large networks.
- I don't cover command-line software such as `cp` or `rsync`. My goal is to make the process as simple as possible—ideally, without requiring you to know anything about Unix or using the Terminal utility to configure and interact with your backups.
- Although I provide basic guidance for performing backups with several popular apps, I can't give you foolproof, step-by-step instructions for setting up every backup app you might use. But by the end of this book, you should have enough information to determine, with the help of your software's documentation, the preferences and settings that will produce your desired outcome.
- To make this book easier to read, I've included specific instructions only for OS X 10.9 Mavericks and later, including macOS 10.14 Mojave. Although much of this material applies generally to Macs running older versions of OS X, I don't spell out any differences. Also, although I don't cover Windows extensively, do see [Back Up Windows Files and Volumes](#), which discusses backing up Windows when it's running on your Mac.
- I've put certain information—like feature comparisons of Mac backup hardware and software—in [online appendixes](#).

Quick Start

First things first: most people do *not* need to read this entire book! There's a lot of detail here for those who want it, but if your backup needs are unexceptional, you can skim much of this material. Even so, don't skip [Plan a Backup Strategy](#), which outlines the basics and helps you understand the hardware, software, and setup advice I give later.

For all readers, the following points should help you understand what I cover where, and which parts you're most interested in.

Decide on a backup strategy:

- If you don't already have a backup system in place, start at the beginning, with the [Plan a Backup Strategy](#) chapter. You'll soon [Understand Joe's Basic Backup Strategy](#), which revolves around three key components: *versioned backups* (containing multiple copies of files as they existed at various points in time), a *bootable duplicate* (a complete, bootable copy of your startup volume), and *offsite storage* (in case something wipes out your Mac *and* the backup media sitting right next to it).
- If you're already backing up your Mac (even if your strategy is based on recommendations from an earlier version of this book), read [Reassess Your Backup Strategy](#) to find out what's new and which [Factors to Reevaluate](#) to determine whether any changes are in order.

Assemble the components:

- Consider whether the best approach for your situation is to store your backups on hard drives (or other devices) directly connected to your Mac(s), or on network servers or appliances. See [Choose Local or Network Backups](#).
- Decide whether Time Machine is a good match for your needs, and if not, select a different app to perform versioned backups. Read [Choose Backup Software](#) for a feature overview, then pick an option

noted in [Explore Versioned Backup Features](#) or consult the [online appendixes](#) for details and sources.

- [Choose Backup Hardware](#)—such as a hard drive or two, and/or a network storage device—to store your backups on.
- [Prepare Your Hard Drive](#) with the right number and type of partitions and volume formats for the types of backups you want to do.

Set up your backups:

- If you've chosen to use Time Machine for versioned backups, read [Configure and Use Time Machine](#). Otherwise, see [Use Other Versioned Backup Software](#) to learn how to configure a versioned backup and verify that you can retrieve stored files.
- Make a bootable copy of your startup volume, schedule it for regular updates, and test it to make sure it works with the advice in [Create and Use a Bootable Duplicate](#).
- One way or another, [Store an Extra Backup Offsite](#)—either by physically moving backup media or by signing up for an online backup service.

Address problems and unusual situations:

- If your disk dies, your Mac is stolen, or an important file goes missing, don't panic; read [What to Do When Disaster Strikes](#).
- After months or years of backing up your Mac, you may run out of space on your backup disks, or you may become concerned about the long-term viability of your backup media. Discover what to do about this in [Manage Your Media](#).
- Find out how to deal with backup needs that don't fit neatly into the duplicate or versioned categories in [Consider Special Backup Needs](#). As appropriate, read [Back Up Digital Photos](#), [Deal with Huge Volumes of Data](#), [Back Up While on the Road](#), and [Back Up Windows Files and Volumes](#).

Plan a Backup Strategy

This book focuses on the strategies, hardware, and software I can most heartily recommend based on extensive personal and professional experience. I'm going to give you my expert advice, and although that will include areas in which you can choose among several options, in this book I'm framing the decision simply. I'll be telling you, "Today's choices are lasagna, fried rice, and ratatouille (and by the way, my lasagna is pretty darn good)" instead of saying, "Choose anything from the *Joy of Cooking*."

If you follow my suggestions, you can rest easy knowing that your data is safe—and you won't break the bank or waste days of work setting things up. And even if you opt out of any of the three main components I recommend in my basic backup strategy, you'll do so with both eyes open.

Understand Joe's Basic Backup Strategy

The strategy I want you to follow consists of three key parts:

- **Versioned backups:** Use Time Machine or another backup app to store *versioned backups*—multiple copies of each file, so you have both the latest version and numerous previous versions. Update your versioned backups incrementally (copying only new or changed data each time) at least daily, and preferably more often.
- **Bootable duplicate:** Create a bootable duplicate of your startup volume on an external hard drive, and update that duplicate regularly.
- **Offsite copies:** Keep at least one backup copy of your important data somewhere safely away from your Mac—in another building, at least, and perhaps even in another part of the world (in the latter case, by using a cloud backup service).

Tip: Later in this chapter I also talk about how cloud-based file *syncing* services (which are different from backup services) can supplement your backup strategy. See [Can Cloud Sync Simplify Backups?](#).

In most cases, you can use a single external hard drive for both versioned backups and a bootable duplicate—for example, by dividing it into two partitions (see [Prepare Your Hard Drive](#)) or by using backup software that creates a versioned bootable duplicate (see [Bootable Duplicates with Versioning](#)). You might choose to add a second drive for extra peace of mind. But I’ll also discuss using online storage for versioned backups, which counts as an offsite copy and could reduce the amount of hardware you must buy.

Furthermore, my goal is to automate nearly all of this so that backups happen in the background without your having to remember anything, press buttons, run apps, or intervene in any other way. And I’ll try to make even the setup process as painless as possible.

Because I want you to understand why I make the recommendations I do and how the whole process works, I spend just a few pages describing my suggested backup strategy in more detail and outlining what choices you’ll make along the way. (If you’re already on board with my basic strategy, you can skip these details and go straight to [Choose Backup Software](#).) As you read, I suggest that you jot down a few notes about hardware that you may want to purchase, software features that seem important to you, or special questions relating to your circumstances to keep in mind as you continue reading the book.

Later on, I provide instructions for every part of the process, so don’t worry if the details still feel fuzzy as you read this introductory topic. I also talk about situations in which this basic strategy requires modifications—for example, when you’re backing up multiple computers on a network, or backing up a laptop Mac while traveling.

No? Really?

Every so often I receive email from readers who assure me that even after reading about my three-pronged backup strategy, they're certain they have no need whatsoever for either bootable duplicates or versioned backups—and then they go on to detail some other convoluted backup strategy and ask for help making it work.

In response, I can only say: *Really?*

The strategy in this book comes from years of experience—not only my own but also that of numerous other industry experts. In my professional judgment, bootable duplicates and versioned backups are, for Mac users, the only procedures worthy of the name “backup.” So feel free to do other sorts of copying or syncing, but if you do that instead of following my guidance, I won't be able to help you!

Why Create Versioned Backups?

Time Machine and most other backup apps protect data by using versioned backups—that is, backing up your files *without* overwriting or deleting earlier versions already stored on your backup media. The first time your backup software runs, it copies all your files in their entirety; then on subsequent runs it performs an *incremental* update—that is, it copies only new or changed data. In some cases, incrementally updating a backup means copying each file that has changed in its entirety; in others, backup apps copy only the changed *portions* of files. The latter approach, which I refer to as [Delta Encoding](#), is faster and uses less storage space.

Note: You may hear this approach referred to by many other names, including *block-level incremental backups*, *byte-level incremental updates*, or *sub-file updates*.

You might be tempted to believe that all those extra versions of your files are a waste of space, but because both humans and computers make mistakes, this type of backup can come in extremely handy.

Let's say your only backup is a duplicate of your entire disk that you update every Wednesday. On Tuesday, you accidentally delete a file, but you don't realize that until Thursday. Too bad: it's not in your backup, because in the process of duplicating your disk, you also deleted any files on the duplicate that weren't on the original. Ironically, the more frequently you update your duplicate, the greater the chances of encountering this problem!

Or consider another situation: A buggy app writes some data to the wrong place, damaging numerous files. Again, you don't realize right away that there's a problem, and you update your duplicate. Sure, you have a backup, but it's a backup of a corrupted disk!

You may not notice a missing or damaged file for weeks or months. So it pays to maintain versioned backups that go back as far as possible (for practical reasons, I'd say that a year's worth is probably enough).

Although a duplicate includes a single copy of your data, a versioned backup includes many different versions of your data—including, crucially, copies of files that have since been deleted. This makes it much more likely that you'll be able to retrieve the files you need in the event of a problem. Don't get hung up on the word "version," because even if you never need to see a *previous* version of a file, you may want to see a file that was accidentally deleted, damaged, or overwritten. And, because versioned backups can be updated much more quickly and easily than bootable duplicates (sometimes as often as every time you save, or as seldom as once a day), your prospects of recovering from data loss are much better than with duplicates alone.

You might use Time Machine to create your versioned backups. It's easy to use, and the cost is right—it's included with macOS. Time Machine isn't perfect for everyone, though, and I say more about why you might consider something different (and what to choose if so) in [Decide If Time Machine Is Best for You](#).

Most people need versioned backups (including those who rely on Autosave and Versions in macOS; see [Version Control](#)), but in some cases I can truthfully say they're unnecessary. If you create very little new content on your Mac, using it mainly to surf the web, play games,

or consume streaming content, versioned backups won't benefit you much. Or, if you do create lots of content but store it mostly in the cloud—especially using services that already store multiple versions of your files, such as Dropbox and Google Docs—then again, having (local) versioned backups may be overkill. But the more you use your Mac to create and store unique information, the more valuable versioned backups become.

Backing Up iTunes Store Purchases

Apple lets you re-download purchases from the iTunes Store later (see the Apple support page [Redownload apps, music, movies, TV shows, and books from the iTunes Store, iBooks Store, and App Store](#) for details), and if you subscribe to iTunes Match you can get an online copy of *all* your music—even tracks not purchased from Apple (see [iTunes Match, Apple Music, and Music Backups](#)). So, to save space on your backup media or time uploading to cloud services, you might reasonably choose to omit such files from your backups—or include them only in your bootable duplicate.

However, note that purchased media such as TV shows and movies could become unavailable later, if Apple stops selling them in the iTunes Store. And downloading lots of large audio and video files again can be quite time-consuming.

If you decide to back up your iTunes purchases separately from your main backups:

- ✦ Be sure to include not only the files in your iTunes folder (usually located in `/Users/your_name/Music`) but also the `/Users/Shared` folder in your versioned backups; this folder contains hidden information required to enable authorization. (For information on this folder's importance to iTunes, see [Remove the SC Info folder](#).)
- ✦ If your Mac suffers a severe crash and you decide to erase your disk (to restore all your data from a backup), deauthorize your computer first. (This prevents you from losing one of your five authorizations if your computer turns out to require a major repair.) To do this, open iTunes and choose Account > Authorizations > Deauthorize This Computer. In the dialog that appears, authenticate, and click Deauthorize. After restoring your backup, reauthorize your Mac in iTunes by choosing Account > Authorizations > Authorize This Computer.

Why Create Bootable Duplicates?

Of the many things that could go wrong with your Mac, quite a few of them involve problems with either a drive itself (that is, physical or electronic damage) or the way data is stored on it (directory corruption or media errors of other sorts). No matter how scrupulous you are with saving files and performing versioned backups, you could find yourself one day facing symptoms such as these:

- Your Mac refuses to start up when you turn it on—perhaps with a blinking question mark icon, or with a blue or gray screen that never goes away.
- Your Mac crashes repeatedly, for no apparent reason.
- You begin noticing misbehavior in multiple apps, such as failure to launch, incorrect preferences, or missing documents.

In situations like these, you're looking at some down time. Maybe your computer is out of commission for a half hour while you quickly run a disk repair utility; maybe it's out for days while you wait for a replacement hard drive to be delivered. In any case, there's going to be a period of time during which you can't get any work done. For many of us, myself included, that's a serious problem. Even though most modern Macs can boot from a hidden Recovery HD volume or, in a pinch, over the internet (see Apple's [About macOS Recovery](#) page for details), booting this way doesn't give you immediate access to your apps and data.

That's why, in addition to versioned backups, I recommend creating a bootable duplicate. You'll store a complete copy of your startup volume on another drive, such that if the startup volume or the drive it resides on ever goes south, you can start up your Mac—or even a different Mac—from your backup drive and get back to work in minutes (instead of hours or days). Bootable duplicates also give you insurance against software updates gone bad. If you install a new version of macOS and encounter compatibility problems, you can quickly revert your disk to the way it was before.

Note: If a volume isn't bootable, then by definition you can't make a bootable duplicate of it. There may still, however, be an argument for making an exact copy of that volume instead of or in addition to versioned backups of it. I say more about this in the sidebar [Duplicates of Non-Boot Volumes](#), later in this book.

The only real decisions you have to make concerning duplicates are which software to use and how often to update your duplicates. I discuss these topics in [Create and Use a Bootable Duplicate](#).

Tip: Another good reason for bootable duplicates is that they make drive upgrades relatively painless. After installing the new drive (say, a larger hard drive or an SSD), boot from the duplicate. Then follow your existing procedure to make bootable duplicates, choosing your duplicate as the source and your new drive as the destination.

I told you that a handful of people may not need versioned backups; is the same true of bootable duplicates? If you already have another way to boot your Mac in an emergency, if you have versioned backups of all important files, and if you wouldn't particularly mind extended down time in the event of a disk catastrophe, you might skip regular duplicates without harm. Even then, though, I'd argue that you should make a duplicate before installing any major macOS upgrade.

If you have more than one Mac, should you make a separate duplicate of each one? That's up to you, of course, but in general the answer is yes. More specifically, any Mac that you rely on to get your work done and that you can't afford to be without for a day or so ought to have its own duplicate. (If you have enough space on your backup disk, you can store more than one duplicate on it—each on its own partition. See [Prepare Your Hard Drive](#) for details.)

Note: It's possible to create a bootable duplicate that also includes multiple versions of your files, but that might not be the panacea it sounds like. See [Bootable Duplicates with Versioning](#).

Synchronization Utilities

Lots of utilities—including several that call themselves backup apps—perform *synchronization* over your local network or with a directly attached hard drive. As the name implies, synchronization means maintaining identical copies of a file, folder, or even an entire disk in two or more locations. Some synchronization utilities can run on a schedule, automatically copying files from a location you specify to another volume—or even continuously, keeping two locations perpetually in sync. And some can even create a bootable duplicate by synchronizing an entire disk to another disk. But in most cases, they don't create versioned backups as described in this book; they simply make the folders in two places identical.

There's nothing wrong with this type of synchronization—in fact, it can be incredibly useful in certain circumstances, such as keeping a MacBook updated with documents you use often on a desktop Mac. A convenient way to make an extra copy of certain files, it can serve as a type of primitive backup. But syncing utilities can in some cases lead to data loss, in that they generally synchronize *deletions* too; by inadvertently deleting a file in one place, you could delete it from both. In any case, remember that a single copy of a single version of your data does not a backup make. By all means, synchronize if you like, but not as a substitute for proper versioned backups and bootable duplicates.

If you happen to choose a sync utility that can preserve older versions and deleted files (ChronoSync, for example), you may be able to kill two birds with one stone. Alternatively, you can sync via a cloud-based service rather than directly between computers, and in so doing gain some extra benefits. I turn to that topic later in this chapter; see [Can Cloud Sync Simplify Backups?](#).

Why Use an External Hard Drive?

Hard drives offer the highest capacity of any storage medium plus fast performance and low cost. You can also make a backup onto a hard drive in such a way that you can start up your Mac directly from the backup—a trick you can't do with most other media. For reasons of capacity, speed, cost, and convenience, external hard drives are ideal.

I want to emphasize the word *external*. Some Mac models can accommodate more than one internal hard drive or SSD (or one of each). And on any Mac, you can divide a single disk into two or more *partitions*—volumes that look and act like separate disks. Of course, you could put a backup on a second internal drive or on an extra partition of your main drive. But you shouldn't do that, because if you do, anything bad that happens to your computer could knock out your backup, too. And if you have to send your Mac out for repairs, your backups would go with it. External drives give you some degree of protection against common hazards, the flexibility to use them with multiple Macs, and the option to rotate them offsite (see [Store an Extra Backup Offsite](#)).

So, you'll be using an external hard drive for backups, but you still have (up to) four decisions to make:

- **Which drive should I buy?** I discuss a variety of options (capacity, interface, case design, and so on) in [Choose Backup Hardware](#).
- **How many drives should I buy?** Having two or more sets of backup media is much safer than having just one. Read [Decide How Many Drives to Buy](#) to decide which number is best for you.
- **Should I use the drive(s) locally or over a network?** If you have multiple Macs, they can all back up to the same drive over a wired or wireless network. Network backups solve some problems but also introduce certain challenges; see [Choose Local or Network Backups](#) for details.
- **For network backups, should I use a Mac or a network storage device?** You can use a hard drive connected to another Mac on your network to store backups for all your computers. Or you can use a *NAS* (*network-attached storage*) device, including Apple's now-discontinued AirPort Time Capsule appliance. For my advice, see [Local vs. Network Backups: Joe's Recommendations](#) and [Network Storage Devices](#).

Why Use Multiple Partitions?

You can, if you like, use one external drive for versioned backups and another for duplicates. But I suggest getting a single, higher-capacity drive and dividing it into two or more partitions (as I describe ahead in [Prepare Your Hard Drive](#)) to reduce cost and clutter. (This applies, by the way, whether you're attaching the drive directly to your Mac or accessing it over a network.)

Note: If you create a bootable duplicate that also includes versions (see [Bootable Duplicates with Versioning](#)), you could in theory get use a single partition for that combined backup type, but I recommend that type of backup only as a supplement to conventional versioned backups.

Why Automate Backups?

I can say from personal experience that backups are far more likely to happen regularly if your backup software runs without any manual intervention. And I want to assure you that *regular* backups are the only kind that matter. I think it's fair to state this as a corollary to Murphy's Law: "The likelihood of suffering data loss increases in direct proportion to the elapsed time since your last backup." In other words, if you're performing all your backups manually, the one day you forget (or run out of time) will be the day something goes wrong.

In some situations, you don't have to do anything special to get backups to run automatically; in others, you have to be careful to set up your backup software to run at a set time.

Schedule-Free Backups

Not so long ago, most backup software required you to set a specific time for it to run—say, every day at 3:00 A.M., or once a week on Sunday afternoon. An underlying assumption of this sort of scheduling was that the backup would probably take a long time, possibly slowing

down your computer (and maybe also your network), meaning you may not want backups happening while you're trying to get something done with your Mac.

Increasingly, though, backup apps have become more sophisticated, such that they don't necessarily require an explicit schedule. Time Machine, for example, runs incremental backups every hour. Retrospect has a mode (called Proactive Backup) in which it runs as often as needed, giving you more flexibility than with conventional schedules. Numerous other apps can detect when files change and then back them up immediately (or after a brief delay, such as 15 minutes).

All things being equal, I prefer schedule-free backups (of whatever sort), because they require less setup and maintenance work and they increase the probability that your backups will happen when they should. But if your backup software doesn't offer that option, you'll have to manually set up a recurring schedule, as I describe next.

Scheduled Backups

In cases where you must schedule a backup explicitly, when should you schedule it to run?

Some backup apps can slow down your Mac significantly while backups are running. This could be an argument for scheduling backups for when you're not using the machine. However, if you don't leave your computer on all the time, you'll need to take special care to ensure that it's on and ready when the backups are scheduled to run (see the sidebar [Power Management and Backups](#) for more details).

Note: If you have FileVault enabled, it will prevent scheduled backups from running when your Mac is asleep, which is another argument for using schedule-free backups.

How often should you back up your Mac? And if you're making both duplicates and versioned backups, how often should you update each?

No single answer is right for everyone, but my rule of thumb is that duplicates should be updated *at least* once a week and versioned

backups should be updated *at least* once every day that you make minor changes (receiving email, modifying text files, and so on).

More frequent updates are even better. For anyone with a reasonably fast Mac, an external hard drive, and modern backup software, there's no good reason not to do backups as frequently as possible. (I have two different kinds of versioned backups running continuously, and I update my bootable duplicates twice a day. But that's me.)

Tip: Regardless of your schedule, always update your duplicate manually just before installing system software updates. That way, if the new version has serious problems, you can easily roll back your Mac to its previous state.

If you're actively working on an important, time-sensitive document, then even hourly backups, such as those offered by Time Machine, may not be enough. You may want to supplement ordinary versioned backups with software that stores every single version you save. Many Mac apps can do that automatically, and other options exist if that approach won't work for you (see [Version Control](#) for details).

Why Keep Multiple Backups?

A sound backup strategy always includes more than one backup. Picture this: You've diligently backed up your Mac's internal disk to an external drive. One day, a lightning strike damages *both* drives. So much for your backup! Even under ordinary conditions, backup media can fail for all the same reasons your hard drive can fail. Having just one backup, in my opinion, is never enough. Most people should alternate between two or more sets of local backup media for greater safety. If you've set up your backups to run on a schedule, this might mean using Drive A every day for a week, then switching to Drive B for each day of the following week, then switching back—and so on.

Another good reason for multiple backups is to protect against *ransomware*—an insidious type of malware that encrypts all the files on your disk and demands a hefty payment for the decryption key. Refuse

to pay and you'll never see your files again. Restoring from a backup made before the ransomware kicked in can solve the problem, but some types of ransomware deliberately wait a few days after being downloaded before they become active, partly to foil daily backups. If you have two backups, one of which is several days or a week old, you're much more likely to recover from ransomware unscathed.

So are *two* sets enough? It depends. To protect against media failure, most experts recommend using at least three sets, of which one is always stored offsite. But using online backups (see [Use a Cloud Backup Service](#)) counts as one set, and perhaps as more than one if the provider keeps its own internal backups. If you're not backing up online, using three hard drives does make rotating media more convenient, as I describe in [Use an Extra Hard Drive](#).

In my opinion, except for mission-critical business use, two sets each of duplicates and versioned backups should be plenty. This can mean a total of two hard drives, each of which is partitioned to store both a duplicate and a versioned backup (see [Configure Your Drive](#)). It's better to have fewer sets that you maintain diligently than multiple sets that you don't maintain because your backup plan is too complicated or time-consuming. In any case, if you have more than one set of media, you certainly should keep one in another location all the time. That brings us to the next crucial part of a good backup strategy: offsite backups.

Why Store Backups Offsite?

If someone breaks into your home or office and steals your Mac, chances are they'll also grab whatever's attached to it, such as your backup drive! Fires, floods, earthquakes, and other disasters could likewise wipe out your backups as well as your computer. As much as we want to believe these things will never happen to us, the prudent course is to plan as though they will. So I urge you to keep at least one extra copy of your data far away from your computer. You have quite a few choices, including physically moving hard drives from place to

place and using an online backup service; I outline the options in [Store an Extra Backup Offsite](#).

Online backups also provide extra protection against ransomware. Even if a malicious app encrypted everything on your Mac and on mounted external disks, it couldn't affect backups already stored in the cloud.

Can Cloud Sync Simplify Backups?

Speaking of storing data online, you may be thinking, “Hey! I use Dropbox (or iCloud Drive or Google Drive or any of a zillion other cloud storage services) already. Doesn't that count as an offsite backup?” Well...no, sorry, not really; I explain why in the sidebar [Dropbox, the Almost-Backup Service](#).

However, cloud sync absolutely *can* simplify your backups! More specifically, it can simplify *restoring* your data, especially when you're moving to a new computer or a replacement hard drive.

I was discussing backup and restoration strategies with a reader, and he asked me exactly what I'd do if my hard drive died and had to be replaced. In particular, he was wondering how I'd deal with the differences between my last bootable duplicate and what had been backed up more recently by Time Machine or an online backup service (see [Finding Recently Backed-Up Files](#)).

I told him I'd restore my disk from the duplicate, which would get me pretty close to my disk's last state because I update my duplicate twice a day. But then, realistically, I probably wouldn't have to touch my versioned backups, even if they were hours or days out of date. That's because nowadays I store most of my important day-to-day data in the cloud.

Personal data such as email, contacts, calendars, reminders, notes, browser bookmarks, and photos sync automatically thanks to iCloud and other services. And most of the files I work on regularly are stored either in iCloud Drive or in my [Dropbox](#) folder. So merely starting up a

Mac on which the relevant apps are installed and logged in to their respective accounts will make most of my personal data automatically update itself to the latest versions. If I noticed anything missing, I could always fetch it from a versioned backup later, at my leisure.

I'm not saying that cloud-based data storage and syncing is a substitute for backups, but rather that when the cloud contains the “master” copy of your important data, you can often skip a number of tedious steps when it comes to restoring backups, because the most crucial data syncs all by itself.

So—both to simplify data restoration and to make your life easier when working with multiple devices—my recommendation is to use IMAP for email if you don't already (see my article [FlippedBITS: IMAP Misconceptions](#)); use iCloud or a comparable service for syncing data such as contacts and calendars; and use iCloud Drive, Dropbox, or any of numerous similar services for syncing your files to the cloud and across computers. And, crucially, adjust your habits so that your most frequently used files are stored in a location that syncs automatically to the cloud.

The Backup Computer

I practice what I preach when it comes to backups. In fact, I probably go overboard. I have lots and lots of backups of many sorts, undoubtedly far more than I need, and I have complete confidence that I could recover from any sort of data loss. However, even I realized my backup strategy had a crucial missing component when my Mac broke down and had to spend a couple of weeks in the shop. I had all my data, sure, but not a computer suitable for using it! (Read more in [The Hole in My Backup Plan](#).)

In fact, my household has several Macs, and I figured I'd just attach a duplicate drive to one of the other computers and off I'd go. But the problem was that all the other Macs had a deficiency of some sort. Whether it was a matter of processor power, RAM, display size, or some other attribute, I quickly realized that because the specs of every other available device were far below that of my main MacBook Pro, even my excellent backups didn't enable me to get my work done easily.

I looked into renting a Mac, but the prices were astronomical. Nor could I find any nearby internet cafés or other public spots that would let me use Macs by the hour. And buying a new Mac with adequate horsepower was beyond my means at the time.

I tell you this to urge you to think ahead. Backups notwithstanding, you could find yourself without a computer at some point. If you depend on your Mac to get important work done, do you have a plan to get access to another suitable Mac temporarily? If you don't already have a second Mac that you can use for all your normal activities, spend some time researching places in your area where you can rent an adequate Mac—or friends who might let you borrow one in a pinch. (Your repair shop may even have a loaner they can offer you.) It's best to work out a strategy before you run into a crisis!

Can You Reduce Your Backup Footprint?


When you're making a bootable duplicate, you'll almost invariably want to copy every single file from your startup volume. With versioned backups, however (whether stored locally or in the cloud), you

may want to reduce the volume of data you're backing up in some situations. For example:

- You're stuck with an external hard drive that's smaller than what you should ideally have (see [Decide on Capacity](#)).
- You're using a cloud service that charges by the gigabyte and you want to economize as much as possible.
- Your external drive or broadband connection is slow, meaning backups take longer than you prefer.

One approach to this problem is to be selective about what you back up; for example, you may exclude certain extra-large files for which having multiple copies isn't crucial (see [Exclude Files from Time Machine](#)). Another approach is to reduce the total amount of data on your Mac in the first place.

Getting rid of unneeded files can address numerous problems besides backups. It can reduce software incompatibilities, simplify software upgrades, and keep your Mac from running out of disk space (which can also slow it down). I cover decluttering in detail in [Take Control of Maintaining Your Mac](#), but here are a few quick tips:

- If your Mac is running 10.12 Sierra or later, choose Apple  > About This Mac > Storage, and then click Manage, to configure Optimized Storage options (which can reduce the amount of disk space used). In particular, consider clicking Optimize and selecting both checkboxes to permit macOS to remove movies and TV shows you've already watched, and email attachments, from your Mac. (You can always download them again later if needed.)
- Try an uninstaller utility, such as [CleanMyMac](#), which can also find large and old files you might want to delete.
- Eliminate duplicate files using a utility such as [Gemini 2](#).
- Be sure to empty the Trash (in the Finder, choose Finder > Empty Trash) to recover disk space after deleting files.

Reassess Your Backup Strategy

If you're reading this book for the first time, you may not already have a backup strategy, in which case feel free to skip this chapter for now and move on to [Choose Backup Software](#). But I suggest returning to this chapter in a year or so, by which time you may benefit from its recommendations. If you already have a backup strategy, though, read on to learn the best way to proceed.

Just as I reevaluate my own stance every so often, you too should periodically reassess your backup strategy in light of new information. If you read an earlier incarnation of one of my books and set up your backup system based on what I said years ago, I'd like you to reassess your strategy right now. In any case, put a reminder on your calendar for one year from now to come back and (re)read this chapter, then reassess your strategy again!

I want to begin with a brief “state of the union” look at what has changed in the last year or so (as I write this in early 2019), and then say a few words about [Factors to Reevaluate](#) as you reconsider your backup strategy, both now and every year. Feel free to skim this chapter to see which topics are applicable to you; you might want to jot down a few notes about those topics to help you identify items to concentrate on as you reformulate your backup approach.

What's New in Mac Backups

Since version 3.0 of *Take Control of Backing Up Your Mac* in December 2017, a number of things have changed that affect Mac backups. I present the highlights here in a number of different categories.

Prosoft Ends Development of Data Backup

One of my long-recommended Mac backup apps, Prosoft's [Data Backup](#), has now marched off into the great beyond. More precisely, development has stopped, and although the company still sells the app, it comes with limited support and is fully functional only up through 10.12 Sierra. I'm sad to see it join the ranks of other previous favorite backup apps such as Synk and CrashPlan Home. Speaking of which...

CrashPlan for Home Is Finally Gone

In August 2017, Code42 Software discontinued its consumer online backup service, CrashPlan for Home, but let people who had recently signed up run out their subscription. The last of those grandfathered accounts expired in August 2018. I covered the saga in my TidBITS article [CrashPlan Discontinues Consumer Backups](#). But the long and the short of it is that CrashPlan, which I'd heartily recommended for many years—for both local versioned backups and online backups—is now off the table.

Well, for *some* people, it's not *entirely* off the table. CrashPlan does have a backup service for small businesses that's still available, even to consumers with just one computer to back up. But it costs twice as much as CrashPlan for Home did; it lacks popular features of the consumer version, such as peer-to-peer backups; it still uses a clunky, Java-based client; and it means entrusting your data to a company that has shown itself not to be trustworthy.

There are lots of other cloud backup services. I've switched to Backblaze (see [Self-Contained Cloud Backup Services](#)) for my family's online backup needs, and I discuss other options later in this book. But candidly, none of them have the breadth of features, the flexibility, or the overall value that CrashPlan for Home offered, so my enthusiasm about cloud backups as a whole has become, shall we say, more muted.

Retrospect Goes Solo

Now for some happier news. Another Mac backup app I've long recommended, Retrospect, now comes in a new edition for individual users: [Retrospect Solo](#). This new product has most of the powerful features for which Retrospect has long been known, but it's far less expensive at only \$49, and slightly less complex. On the downside, Retrospect Solo works with only one computer (so, no client-server mode), it can't use a NAS device as a source or destination, and it doesn't support tape or optical drives as destinations either (not that an individual user is likely to care). If you want those more-advanced features, you'll have to step up to [Retrospect Desktop](#), which starts at \$119 but can back up five Macs on your network. I say more about both apps in [Retrospect](#) and [Retrospect Tips](#).

APFS Evolves in Mojave

In 10.13 High Sierra, Apple introduced a file system: Apple File System, or APFS. It supersedes the decades-old Mac OS Extended file system (otherwise known as HFS Plus), with promises of better performance (at least for SSD users), improved data integrity, and greater security (among other virtues). Its reach has now been extended.

In September 2018, 10.14 Mojave was released. Whereas High Sierra used APFS only for SSD startup volumes, Mojave uses it for all startup volumes (including mechanical hard drives and Fusion drives). This change brings the benefits of APFS to more people, but it also comes at a cost, as the performance of APFS on mechanical hard drives is quite poor.

APFS has a built-in mechanism for making snapshots that's somewhat reminiscent of the method certain backup apps use (see [Snapshots and File Lists](#)). In theory, this should be a capability that backup apps can tap into to get quicker, easier, and more compact backups. However, at present, only Time Machine seems to have access to this capability—and even then, only in the limited sense of storing local, temporary backups while your backup disk is disconnected (as I mentioned just

above). Perhaps other backup apps will be able to take advantage of this feature in the future.

But there's a bigger problem with APFS: Time Machine can't use an APFS-formatted disk as a backup destination, because APFS has no concept of hard links, which Time Machine depends on (see [The Magic of Hard Links](#)). So even though Disk Utility in High Sierra or later will let you reformat your Time Machine disk to use APFS, you should *not* do this, because Time Machine won't work; you'll be forced to erase the disk and restart your backups from scratch. Ouch. I have heard nothing about whether, when, or how Apple plans to address this.

The introduction of APFS also made life difficult for developers of backup software, because it was poorly documented at first and a lot of things work in, shall we say, surprising ways. Dave Nanian, the developer of SuperDuper!, wrote about one such situation in his article [Fraternal Twins](#). Mike Bombich, the creator of Carbon Copy Cloner, wrote about another issue in [Think twice before encrypting your HFS+ volumes on High Sierra](#).

In short, although APFS holds great promise, it currently leaves Mac users and developers alike in a sort of uncomfortable limbo, making decisions that should otherwise be straightforward (like “How should I format my backup disk?”) unnecessarily complicated.

T2 Chips Change the Backup Rules

Recent Mac models, such as the iMac Pro and the Mac mini, MacBook Air, and MacBook Pro models introduced in 2018, use a new [Apple T2 Security Chip](#). The T2 chip adds a number of security features, and of course I'm all for extra security. However, it also complicates a couple of things when it comes to backups. To wit:

- You can still make a bootable duplicate, but in order to actually boot from that duplicate, you'll have to [follow these instructions](#) to reboot in macOS Recovery, choose Utilities > Startup Security Utility, and select “Allow booting from external media” under External Boot. Then restart your Mac. (Note that you should *not* change the Secure Boot setting, however.)

- It's no problem to create a bootable duplicate of an APFS startup volume onto a backup disk formatted as HFS Plus; such a disk is still bootable (keeping in mind the previous point). However, if that HFS Plus volume is *encrypted* (as I generally recommend; see [Encryption](#)), a Mac with a T2 chip can't boot from it. So you must either forgo encryption on your bootable duplicates or format the destination volume as APFS, create the duplicate, boot from the duplicate, and enable FileVault. This is even more of a pain considering how slow APFS is on mechanical hard drives.

Privacy Concerns Increase

High-profile hacking cases have continued to occur at troubling rates. Every week or two, another big site announces that it's suffered a data breach, often involving the exposure of millions of passwords (or other private information). These cases highlight the need to be cautious with what information is stored online and how it's protected.

Throughout this book, I discuss using encryption as one means of protecting your backed-up data. You should also use excellent passwords and enable two-factor authentication where available. For details on all these things, see my book [Take Control of Your Online Privacy](#).

Hard Drives Are Larger and Cheaper

Nothing surprising there; hard drive sizes are always on the rise. You can now easily find individual 3.5-inch drive mechanisms that hold up to 14 TB, and 2.5-inch mechanisms that hold up to 5 TB. (The largest Fusion drive currently available directly from Apple in a build-to-order new Mac is only 3 TB, while build-to-order SSDs go up to 4 TB.)

Meanwhile, the price of storage per gigabyte continues to fall: you can buy an external, bus-powered, 2.5-inch, 4 TB drive for under \$100, or a 5 TB model for under \$120. And I've seen 3.5-inch, 8 TB USB 3.0 external drives on sale for less than \$140.

Note: External SSDs are still pricey, but less so than previously. I’ve seen 1 TB drives for as little as \$170, and 2 TB drives for \$300. But higher-capacity SSDs are still outrageously expensive.

Interface Options Evolve

Apple has continued to release new Mac models (including updated MacBook Pro and MacBook Air models and the iMac Pro) featuring super-speedy Thunderbolt 3 ports. Thunderbolt 3 supports 40 Gbps connections—double the speed of Thunderbolt 2 and quadruple the speed of the original Thunderbolt. Thunderbolt 3 peripherals such as RAID arrays are less plentiful than those that use USB 3.0, but the number of options is increasing.

Thunderbolt 3 uses the USB-C connector, which is also used by USB 3.1 devices. This has caused considerable confusion, because all Thunderbolt 3 ports support USB 3.1 peripherals, but the reverse is not true—a Thunderbolt 3 peripheral won’t work on a computer that supports only USB 3.1 (such as the 2015 or 2016 MacBook), even though the connector is physically identical. I say more about these standards later, in the sidebar [USB 3.1, USB-C, and Thunderbolt 3](#).

Time Capsules Officially Bite the Dust

We saw this coming for a couple of years, but in 2018 it finally happened: Apple discontinued its entire line of AirPort products, including the AirPort Time Capsule. If you already have a Time Capsule (or buy one used), it will still work—at least for the time being—but now, if you want a Time Machine backup over a network, you’ll have to use either another Mac (see [Use a Mac as a Time Machine Server](#)) or a third-party NAS device as a destination.

Dropbox, the Almost-Backup Service

I'm a big fan of [Dropbox](#). The service syncs files in a single folder (and its subfolders) to storage space in the cloud, and from there to all your other devices. It even keeps older versions and deleted files, somewhat like a versioned backup app does. So, in a manner of speaking, it can serve as a primitive backup tool. (The same can be said of numerous competing services, such as Box, Google Drive, iCloud Drive, Microsoft OneDrive, SpiderOak, and SugarSync.)

However, fond as I am of Dropbox for syncing and sharing files, I don't think it's a good substitute for the types of backup I describe in this book, for three reasons:

- ✦ Only the files in your Dropbox folder are synced, which probably excludes a lot of important data. (Some competing services let you sync whatever folders you like.)
- ✦ Dropbox stores old versions and deleted files for only 30 days. You can change that to one year, but only if you have a paid Dropbox Pro account and pay an extra \$39/year for the Extended Version History option.
- ✦ Restoring older versions or deleted files can be done only from the Dropbox website, and it's a tedious, one-file-at-a-time operation. That's fine for restoring a few files on occasion, but beyond that, it's unpleasant.

So, by all means, use Dropbox or a comparable service to your heart's content. But choose something else for keeping versioned backups—and be sure to back up your Dropbox folder too!

Factors to Reevaluate

The mere fact that technology evolves does not, by itself, mean you need to change anything about your backup system. If everything you set up last year continues to work perfectly now, it's entirely reasonable to leave well enough alone. However, changes that affect your backups have a way of sneaking up on you slowly, so this is a good time to think about not only new things you can buy but also numerous other factors.

In particular, consider the following questions:

- **What are your current data and storage media figures?** You selected backup methods and storage media based partly on how much data you have to back up (consult [Decide on Capacity](#)), but data inevitably grows over time. If you haven't recently done so, check to see how much data you have to back up. Then make sure your media still has enough breathing room to accommodate your needs over the next year or so—and if not, look into moving up to something with higher capacity. You might also think about whether your data is likely to grow at a faster rate. For example, as our kids grow, the number of photos and videos we record increases dramatically.
- **Do you have any new equipment?** Related to the last point, maybe you've purchased a new Mac since last year (including more internal storage, no doubt)—or maybe you've upgraded your digital camera, bought an iOS device or two, or added external storage. Whatever the case, take all these into account when calculating how much space you'll need for backups.
- **Have you upgraded to a new version of macOS?** With more recent versions of macOS, you may find new backup options (products that work only with the new operating systems). You may also find that products you relied on previously are no longer supported.
- **Are you using Optimized Storage?** In 10.12 Sierra and later, a group of features collectively called Optimized Storage may have an effect on the way you back up your Mac. Among other capabilities, Optimized Storage lets you move your Desktop and Documents folders to iCloud Drive, and permits macOS to delete local copies of older files that are stored in the cloud (you can download these again later if need be). On the one hand, that could mean less data that you need to include in your versioned backups (see [Can You Reduce Your Backup Footprint?](#)). On the other hand, using Optimized Storage makes it all the more important to have backups of the “optimized” data apart from what Apple stores for you.

With Optimized Storage, your Mac won't tell you when it's about to delete the local copy of a file (or photo or whatever) such that the only copy is stored in the cloud. If the local copy wasn't backed up before this happens, you have just a single copy of that data in the cloud—and if anything happens to that copy, you're out of luck. So, a word to the wise: make sure your backups (at least your bootable duplicates) include all locations subject to Optimized Storage, and update them frequently.

- **How old is your media?** The physical media on which you store your backups—hard drives, optical discs, or whatever—is subject to degradation and data loss over time. If the media you're currently using is older than a few years or so, strongly consider copying your backups onto fresh new media (and you'll probably want to upgrade to higher-capacity storage in the process).
- **Are *network* backups more—or less—viable than before?** If you have more computers in your home or office, if their combined storage needs strain individual backup drives, or if you're tired of moving drives and messing with cables, you might consider switching from local drives to network backups (see [Choose Local or Network Backups](#)). The fact that any Mac running High Sierra or later can function as a Time Machine server with no extra hardware or software (see [Use a Mac as a Time Machine Server](#)) may also influence you to embrace network backups. On the other hand, if you've been using network backups and found them to be too slow or otherwise unsuitable—and if you have only one or two Macs to back up in the first place—it might be worth switching to individual hard drives.
- **Are *cloud* backups more—or less—viable than before?** Increases in bandwidth and decreases in price may lead you to reconsider cloud backups (see [Use a Cloud Backup Service](#)) if you decided against them in the past. Conversely, if you've been using online backups and your data has grown at a rate your broadband connection (or budget) can't keep up with, maybe it's time to switch services or explore other forms of offsite storage.

- **Are you relying more heavily on cloud storage and syncing?** If you use Dropbox or a similar service for your most important documents, you already have a safety net of sorts, at least for those files. Although it's not quite the same thing as a real versioned backup (see the sidebar [Dropbox, the Almost-Backup Service](#)), it might make restoration easier, leading you to rethink which backup tools you prefer.
- **Is it finally time to ditch optical media?** If you chose optical discs (recordable CDs, DVDs, Blu-ray discs, or whatever) as your storage media, do you feel less secure in that choice knowing that optical technology is rapidly on the decline, at least as far as Macs are concerned? Even if your discs remain viable for decades, your next Mac might not have a way to read them, which might make you think twice about continuing to rely on optical media.
- **Are you responsible for protecting more people's data?** If there are more people than before in your household or office and they rely on you to keep their data safe, be sure your current system can scale to accommodate their needs. If not, it may be time to look into client-server backup software (described in [Network Backup Approaches](#)) and expandable storage (see [Drobo Storage Devices](#)). Likewise, if your child once used an old laptop for games and web browsing but now uses it to write essays and book reports for school, it's time to start backing up that laptop.
- **Has your budget changed?** For many of us, income fluctuates from year to year. If you've been fortunate enough to earn more money in the last year, perhaps you should consider investing in larger or faster storage devices, or fancier backup software. Conversely, if you feel the need to economize, it might be necessary to scale back on significant recurring expenses, such as high-end online backup services.
- **Would any of the latest products be a better solution?** New and higher-capacity storage devices (see [Consider RAIDs and RAID-Like Tech](#)), better online backup options (see [Use a Cloud Backup Service](#)), and updated backup software (see [Choose Backup](#)

[Software](#)) may offer solutions to problems that couldn't be solved easily a year ago—or they may be more affordable than they once were. I'm not one to buy new gadgets just for the sake of keeping up with the latest fads, but if a new product genuinely makes my life simpler or saves me money, I'm all for it.

- **Is your overall strategy still sound?** I hope you took my advice to make use of the three main pillars of a solid backup strategy: versioned backups (see [Why Create Versioned Backups?](#)), bootable duplicates (read [Why Create Bootable Duplicates?](#)), and offsite storage (see [Why Store Backups Offsite?](#)). If you decided against any of these components, I'd like to kindly suggest that you take a moment to review my reasons for recommending them and your reasons for rejecting them. There's no shame in changing your mind; if something makes sense now that didn't a year ago, adjust your setup accordingly. Think about the details as well. For example, if you chose to keep versioned backups of only your home folder because your external hard drive was too small, but now you have a bigger one, consider expanding your backups to include every file on your disk.

If the time has come to move to new media or even to an entirely different storage method, give some thought to whether you should migrate your existing backups—for example, moving your Time Machine backups from a hard drive onto a server or NAS (see [Migrate to a Network Volume](#)) or from a smaller Time Capsule to a larger one (see [Migrate to a Larger Time Machine Disk](#))—or start over from scratch. Migrating your old backups ensures continuity, so you can be certain of having access to all your old files. Creating new backups will reduce your storage space requirements, but you'll spend a lot of time doing the initial backup, and your backups won't contain previously changed or deleted files (so if you do this, be sure to keep your existing backups safely on hand for a while).

Choose Local or Network Backups

Before you go too far in designing a backup plan, you should take a moment to ponder whether you'll back up to a local storage device (that is, one connected *directly* to a Mac with a cable) or to a device located somewhere else on your (wired or wireless) network—or both.

In years past, I assumed that in most cases, each Mac would have one or more backup drives of its own, and that network backups were mainly for locations with more than a few Macs or with exceptional backup needs of some sort. Now, however, the decision seems less obvious, and network-based backups of one sort or another seem like a good fit for a wider range of people.

In this brief chapter, I help you think through the pros and cons of both local and network backups. Whether you choose to use one approach or the other (or a combination), your decision will help inform which software and hardware you use; I discuss those choices in the next two chapters.

Note: This decision affects only the backups in your home and office, and is thus independent of whether to use a cloud backup service (see [Use a Cloud Backup Service](#), later).

Local Backups

With a local backup, you plug your hard drive or other storage device into a Mac and let your backup software run. (Time Machine starts automatically, as do some third-party backup apps; other software requires either an explicit schedule or that you manually run backups after attaching a drive.) When it's done, you can disconnect the drive and hook it up to another Mac if you have one.

The biggest advantage of a local backup is *speed*. Even if you have a fast network, chances are your backup and restore operations will complete much more quickly over a cable—especially if that cable uses Thunderbolt 3. Another advantage is that any backup software that can create a bootable duplicate can do so with a locally attached drive, whereas only a few apps can create bootable duplicates over a network (see [Network Backups](#), ahead)—and none of them can make bootable duplicates to a NAS device or Time Capsule (even if it has an external disk connected).

The downside to local storage is that backups and restorations can occur for a given computer only while the drive is connected, and if you forget to connect the drive, you won't have a backup at all. You may end up doing a lot of plugging and unplugging—and more so if you're moving a single drive between computers. And, if you have a laptop and you actually use it on your lap (as opposed to a desk), having an external drive attached can be a real hassle.

Keep in mind that local storage need not be a single external hard drive; it could also be a RAID or other multi-drive assembly. See [Decide on a Storage Configuration](#) for further details.

Network Backups

In a network backup, one computer (or other device) typically functions as the backup server—the machine to which your backup drive(s) are physically connected. Files from your other machines (which function as clients) are copied over the network onto each backup drive.

If you have multiple computers—especially if one or more of them is a laptop that gets moved around a lot—network backups can be far more convenient than local backups that require being physically tethered to an external drive. They require virtually no intervention; just leave all the necessary devices turned on and, assuming you have your backup software configured appropriately, the computers on your network will back themselves up automatically as needed.

For a long time, conventional wisdom held that network backups would always be slower than local backups—and, moreover, that network backups could cause sufficient congestion to slow down other things on your network to unusable speeds. Although a directly connected Thunderbolt 3 drive will indeed give you much faster performance than even an 802.11ac Wi-Fi connection or a 10Gb Ethernet wired connection, real-world network performance these days is usually fast enough that the average user won't perceive backups or network operations as being too slow. In my opinion, network backups are fast enough for most people, most of the time, that speed is essentially a nonissue.

Note: While the *initial* backup of each computer over the network will take some time, subsequent updates should go much more quickly because there will be less data to transfer.

Network Backup Approaches

Network backups can proceed by any of four different methods:

- **Push:** The *server*—a computer or a NAS device—shares its backup volume (for example, using the File Sharing feature in System Preferences > Sharing; see [Share a Volume](#)), which the client machines mount as a volume in the Finder. Then each client machine uses its own backup app to back up files to the network volume (rather than to a locally attached hard drive). This is sometimes called a *push* backup, as each client “pushes” its data onto the network volume.

Note: When Time Machine uses a Time Capsule, NAS device, or shared network volume as its destination, it employs a type of push backup—even though the network volume isn't necessarily mounted. However, when you're backing up to a Mac functioning as a Time Machine server, it's a client-server backup (see below).

- **Pull:** Each *client* Mac shares the volume(s) to be backed up. The server mounts these volumes in its Finder, and then the backup app, running only on the server, copies files from each network

volume onto its locally attached backup volume. This is sometimes called a *pull* backup, as the server “pulls” data from each of the clients onto its backup volumes.

- **Client-server:** The server runs backup software that supports client-server network backups, and the other machines run client software that communicates with the server directly—usually without any of the machines having to share or mount volumes. Retrospect Desktop is the best-known example of client-server backup software, but Carbon Copy Cloner and ChronoSync (among others) also support client-server backups of sorts.

If you have a Mac running High Sierra or later, it can function as a Time Machine server on your network, providing a storage place for backups from all your Macs without the need to mount network volumes as in a push or pull backup. You can even configure where Time Machine backups are stored, how much space they’re permitted to occupy, and more. For instructions, see [Use a Mac as a Time Machine Server](#). (Macs running earlier versions of macOS along with Apple’s [macOS Server](#) app can also be set up to do this.)

- **Peer-to-peer:** Each computer on the network runs backup software that can act as both a client (backing up that computer’s files to other computers) and a server (hosting the backed-up files from other computers)—again, with no need to share or mount volumes. When two or more computers use software that allows mutual backups of this sort, it’s called *peer-to-peer* backup. Given that CrashPlan has exited the consumer market and Synk is no longer being developed, I’m not aware of any great options for peer-to-peer Mac backups right now. (ChronoSync comes fairly close, but it falls short of a true peer-to-peer model.)

Although any of these approaches can work under the right conditions, a client-server configuration is likely to produce the best and most reliable results; it’s also the setup most likely to support Windows and Linux computers. Be aware, too, that when a backup depends on a remote volume being mounted in the Finder (as in most push and pull backups), quite a few things can prevent that from occurring as expect-

ed, with the result being failed backups. That's just one of many reasons to consistently [Test Your Versioned Backup](#).

Network Backup Considerations

As you consider whether to use a network destination for your backups, keep these facts in mind:

- It probably goes without saying, but I'll say it anyway: the storage device you use for network backups must have sufficient free space for *all* the computers you plan to back up. (See [Decide on Capacity](#).)
- Time Machine can see a network volume *only* if it's attached to a Mac, a Time Capsule, or a NAS device that's expressly designed to work with Time Machine. In other words, if you choose Time Machine as your backup software, you need to be pickier than you otherwise would about what type of network storage you use.
- To make an external drive (connected directly to your Mac) available to other computers on your network, you must share it. See the sidebar [Share a Volume](#) (just ahead) for instructions.
- You can create a bootable duplicate over a network—that is, store the duplicate on a hard drive connected to another Mac on your network. As far as I know, only Carbon Copy Cloner, ChronoSync, and Retrospect Desktop can perform this trick, which requires administrative access to the source Mac and, in some cases, client software running on it as well.



For this to work, you'll need to attach an external hard drive to the server; the bootable duplicate will be stored on that drive (or on one of its partitions). However, to *boot* your Mac from the duplicate (or restore your disk in its entirety), you'll have to disconnect the drive from the server and connect it to the client; you can't boot from a duplicate over your network. See the documentation for your backup app for detailed instructions.

- For a scheduled network backup to occur, both server and client machines must be turned on and awake. (Read the sidebar [Power](#)

[Management and Backups](#) for advice on how to wake a sleeping Mac for a backup.)

Share a Volume

To share a volume on your Mac for the purpose of backups:

1. Open System Preferences > Sharing.
2. In the list on the left, make sure File Sharing is both checked and highlighted.
3. Click the plus  button under the Shared Folders list. Select the volume you want to share and click Add.
4. Click Options. In the dialog that appears, check "Share files and folders using SMB." If any Macs running a version of OS X older than Mavericks must connect to the shared volume, also check "Share files and folders using AFP." Click Done.
5. Make sure each person who will connect to the drive is listed under Users. To add a user, click the plus  button at the bottom. Then select a name from your Contacts list and click Select. Enter and verify a password for that user, and click Create Account. (Be sure to tell that user the password you entered.) Finally, in the Users list, set the newly added user's access to Read & Write.

Other authorized users on your local network can then connect to your Mac by selecting it in the Finder sidebar, clicking Connect As, and entering their credentials.

Local vs. Network Backups: Joe's Recommendations

I can't make a one-size-fits-all recommendation when it comes to selecting a backup destination. The number of computers you have to back up, the amount of data they store, your network configuration, your budget, and your tolerance for complexity all factor in.

However, I would like to offer the following suggestions:

- If you have just one Mac, the path of least resistance is to store your backups on a directly attached hard drive. If your single Mac is a laptop and you can't bear to fiddle with the external drive and cables, a simple, inexpensive NAS device is your next-best option for versioned backups. But if you want a bootable duplicate—and you do!—you'll still need to attach a drive directly from time to time to update it, since you can't make a bootable duplicate over a network to a NAS device.
- If you have multiple Macs and saving money is your priority, once again, a large external drive is your best bet. Assuming it has enough space, you can partition it so that it can hold multiple bootable duplicates and versioned backups (see [Prepare Your Hard Drive](#)). You'll have to shuttle it around, plugging and unplugging as necessary—and you'll have to make sure you choose an interface that's compatible with all your Macs (see [Choose an Interface](#)).
- If you have multiple Macs, one of which is always kept in the same place (so an external hard drive can remain connected) and always turned on, that Mac can function as a backup server for the rest. You can then do any or all of the following with it:
 - ▶ Share a backup volume, which other Macs on your network mount and copy data to using backup apps they run (push backups).
 - ▶ Mount volumes shared by other Macs and copy data using a backup app on the server (pull backups).
 - ▶ Use it to host Time Machine backups; see [Use a Mac as a Time Machine Server](#).
 - ▶ Run the server component of another client-server backup app, such as Retrospect Desktop, while your other Macs run the client.

- ▶ Use it to create bootable duplicates over the network—onto separate hard drives or partitions—using Carbon Copy Cloner, ChronoSync, or Retrospect Desktop.

Of these, my personal choice would be to use it as both a Time Machine server and a destination for bootable duplicates, using Carbon Copy Cloner.

- If you have multiple Macs but none of them is available to function as a backup server, a NAS device—with enough storage for all your Macs and then some—is a great choice for versioned backups; see [Network Storage Devices](#). You'll still want one or more hard drives, which you'll have to connect to each Mac, to hold bootable duplicates.

Once you've decided whether you plan to store your backups locally or on a network volume, you'll want to select the appropriate software (which I cover in the next chapter, [Choose Backup Software](#)) and hardware (see [Choose Backup Hardware](#)).

Choose Backup Software

In this chapter, I help you decide which backup software to use for versioned backups and which to use for bootable duplicates. (You might choose the same app for both purposes, but as we'll see, the best app for one type of backup isn't necessarily best for the other.)

Decide If Time Machine Is Best for You

Time Machine is the backup software built into the Mac starting with OS X 10.5 Leopard. Apple's goal was to make backups as easy as possible, and compared to anything that came before it, Time Machine is certainly much simpler to set up and use. In some cases, you can set it up and turn it on with a grand total of one click! It's hard to beat that. Anything that makes backups easier and thereby encourages more people to use them gets a gold star in my book.

However, Time Machine is not ideal for everyone. Before getting into the details about setting up and using it (see [Configure and Use Time Machine](#)), I want to tell you what I like and dislike about it, and look at a few situations in which it may be the wrong solution. For those people who need different software, I point you in the right direction with a discussion of features to look for and examples of other versioned backup apps I can recommend.

Without a doubt, Apple got a lot of things right about Time Machine:

- The user interface is elegant, if unusual.
- I love how I can restore files right in the Finder, and how I can restore missing email messages from within Mail.
- I appreciate the fact that my MacBook Pro can back up files using Time Machine even when I'm away from my desk and a Time Machine volume (see [Local Snapshots](#), later in this book).

- Time Machine supports encryption for both local and network backups, and also lets me choose multiple destination disks (which it rotates among automatically).
- You can back up either to a locally attached hard drive or to any of several kinds of network destinations (including a NAS device, an AirPort Time Capsule, and another Mac)—whatever you find most convenient.

All that is fantastic, and in many respects better than the competition. And yet, having used Time Machine since day one, I find the shine wearing off, for several reasons:

- Time Machine’s approach doesn’t scale well to large amounts of data. For one thing, backing up lots of large files takes far longer than it should, because Time Machine always copies entire files rather than using delta encoding as many other backup apps do (see [Delta Encoding](#), ahead). And, even if your Time Machine drive has plenty of storage space, by the time you have several months’ worth of backups the sheer number of files seems to bog down Time Machine and make simple operations unreasonably sluggish.
- Although Time Machine is supposed to be almost invisible in ordinary use, it sometimes uses up far too many system resources. If I notice the fan on my wife’s MacBook Pro start to wail, it’s usually because Time Machine happens to be running.
- Time Machine is pretty good at restoring individual files and folders from a specific point in time, but it falls down in a number of common usage scenarios. For example, suppose your hard drive dies and you replace it with a bootable duplicate you created last week—and now you want Time Machine to restore only the files that changed *since last week*. There’s no easy way to do that (see [Finding Recently Backed-Up Files](#)).
- One of Time Machine’s flashiest features when it was introduced was the capability to restore individual items within apps like iPhoto, Mail, and Contacts (previously called Address Book). Indeed, Time Machine remains the best way I know of to restore

individual email messages. Although Apple later added Time Machine support to GarageBand, they inexplicably *removed* support from iPhoto—and never added it to Photos. Lots of other apps could benefit from in-app restoration (Calendar, in particular, as well as numerous third-party apps), but for whatever reason, Apple has backpedaled on that capability.

- Time Machine works best with a directly connected hard drive or a Mac functioning as a Time Machine server (see [Use a Mac as a Time Machine Server](#)) but tends to be flakier and slower when backing up to a Time Capsule or other NAS device. And woe betide the person whose Time Capsule malfunctions; repairing or replacing that disk is a pain and a half.
- Time Machine has a lot of troubleshooting issues—judging by not only personal experience and anecdotal reports but also, for example, Apple’s pages [Time Machine: Troubleshooting backup issues](#) and [If you can’t back up or restore your Mac using Time Machine](#). One particular issue I’ve encountered more than once, and have seen multiple other reports of, is a dialog that tells you Time Machine has encountered a verification error and has therefore stopped making new backups; your only choice is to abandon your existing backup archive and restart your backups from scratch.
- As I mentioned in [APFS Evolves in Mojave](#), Time Machine is currently unable to use backup drives formatted with the new APFS file system in High Sierra and later.

Despite these issues, I use Time Machine myself because it offers the fastest and most convenient way to restore individual files. But I also use other software for versioned backups to make up for some of Time Machine’s shortcomings and provide additional flexibility.

So, should *you* use Time Machine? The biggest question to ask is whether the underlying philosophy of Time Machine works for you. If Time Machine’s design is incompatible with your needs, then you need to choose a different solution for creating versioned backups.

Whether or not you ever encounter the issues I listed previously, Time Machine makes a poor match for these backup needs:

- **High-volume backups:** Because Time Machine lacks file compression, deduplication, and delta encoding features (read [Explore Versioned Backup Features](#), just ahead), backups may require much more storage space than with other software, and as a result may require expensive, high-capacity hard drives.
- **Backing up many Macs:** Time Machine is fine for backing up, say, two or three Macs to a single drive, but the more Macs you back up, the less sense Time Machine makes, because it wastes space with duplicate files and bogs down the host Mac (or other storage device).
- **Backups to an unsupported NAS:** Time Machine doesn't work with some network-attached storage (NAS) devices as a backup destination. (A NAS is essentially a hard drive with a network interface, which functions as a standalone file server.) Apple's now-discontinued Time Capsule is a notable exception (as is an AirPort Extreme base station with an external USB hard drive, or "AirPort Disk"), and there are numerous others—but not all NAS devices work with Time Machine.
- **Backups of Boot Camp and network volumes:** Time Machine can back up your startup volume and most other mounted local volumes (such as a second internal hard drive or a secondary partition of your main disk). But to back up Boot Camp partitions or mounted network servers, you'll need a different app. The same goes for backing up the data on a NAS; see [Back Up a NAS](#).
- **Fine-grained control:** Time Machine offers simplicity at the expense of flexibility. What if you want to exclude from your backup all files that match a certain pattern (disk images, videos, music)? You'd have to add each item individually, or the folders that contain them, to Time Machine's "Exclude these items from backups" list (see [Exclude Files from Time Machine](#)). What if you want to use a different scheme for deleting old backups? Or you want to store some kinds of files in one destination, and other files in another

place? These are just a few examples of the kinds of control you give up with Time Machine, but which you could gain, if you need it, with other backup software.

- **Bootable duplicates:** It's possible to restore an entire disk from a Time Machine backup and then boot from that disk. You can even reboot in macOS Recovery to do this, without having a separate boot volume. But you can't boot directly from a Time Machine backup in such a way that your apps and data are immediately usable—and it could take hours or even days to restore an entire disk, during which time you won't be able to do anything else with your Mac. So Time Machine should be considered a companion to a bootable duplicate, not a substitute for one.

If any of the foregoing makes you think Time Machine isn't right for your needs—or if, like me, you want to use Time Machine but supplement it with other backup software—don't worry; there are many other options to choose from. I turn next to the features to look for in versioned backup software, and then discuss a few particular apps I can recommend. However, if you're satisfied with Time Machine, you can skip directly to [Choose a Bootable Duplicate App](#).

Explore Versioned Backup Features

I've tried more than 100 backup apps, and I've read websites and instruction manuals until my brain went numb. Evaluating any given app on its own is hard enough, but comparing them is even more challenging. For one thing, because software developers use terms like *incremental*, *versioned*, *snapshot*, and even *backup* differently, you may think you're getting certain capabilities that later turn out to be missing. For another, even when two apps have essentially the same feature, they may implement it in entirely different ways.

In the next several pages, I describe features that may be significant to you in choosing an app to create versioned backups. Also, in the [online appendixes](#), I provide a table that lists the features found in current versions of many backup apps, using my preferred terminology (which

may or may not match what a given app's marketing materials say). You may find it helpful to jot down the features you find particularly important as you read this section and compare your list against the latest version of the tables in the online appendixes.

However, please keep in mind that you don't necessarily need *all* these features in your backup software, and that in some cases a combination of two or more apps might serve you best.

Change Detection

In general, backup software doesn't start copying files immediately when it runs. It must first figure out what to copy—that is, apart from the first full backup, it needs to know which files are new or different since it performed the last incremental update. A backup app typically starts each run by scanning all the folders and files you've asked it to back up to determine not only what has changed but also how much space your backup will require and whether your backup will fit on the destination volume.

Some apps take a *long* time to scan, whereas others use any of several tricks to reduce or eliminate scanning time. Quite a few apps use the FSEvents (file system events) notification system in macOS to determine which files have changed recently, while others run in the background and use their own methods to watch for file changes. Whatever the mechanism, the result is that new or modified files can be copied immediately, and full scans (to identify changes that may have slipped through the cracks somehow) can occur infrequently. Among the backup apps that detect file changes instantly so that they can perform incremental updates without lengthy scans every time are NTI Shadow, Synchronize Pro X, and Time Machine. Some other apps, like SuperDuper!, scan and copy in a single pass for greater efficiency.

Sources and Destinations

The volume *from* which you back up files is known as the *source*; the volume *to* which you back them up is known as the *destination* (or

target). Be sure to select software that can accommodate the sources and destinations you want to use.

All backup apps can copy data from your startup disk, and most can also copy data from other attached hard drives and mounted network volumes. In most cases, your destination options also include any Finder-mountable volume. If you like, you can even back up your files onto a *disk image* (a special file that functions as a removable disk), although many apps require you to manually create the disk image using Disk Utility and mount it in the Finder before you can use it as a backup destination.

Finally, some backup apps can copy data directly to online storage facilities, such as Amazon S3, a private server, or a proprietary destination (Backblaze, IDrive, and the like). If you want to store a copy of your data online, you may find it convenient to use a single app for both local versioned backups and online backups, assuming you can find one that works with all your preferred destinations.

Note: If you plan to back up over your network to a NAS or another computer, make sure the software you’re considering supports that configuration—ideally, using a client-server setup (see [Network Backup Approaches](#)).

Rolling Backups

Among those backup apps that store multiple copies of your files, there’s an important distinction to make: true versioned backups versus *rolling backups*. In a true versioned backup, every version of every file you designate is saved, but identical files in the same location are never duplicated. In a rolling backup, the app creates a complete, separate copy of all your files each time it runs—basically a non-incremental backup. Then, after a certain number of days or backup runs (specified by the user), the app erases the oldest backup and adds a new one. Rolling backups give you multiple versions of all your files, but because they copy every single file each time they run, they take longer to perform and require more storage space.

Versioned Backup Pruning

Whereas a rolling backup scheme saves a fixed number of complete backups, deleting older ones as newer ones are added, many backup apps offer a more sophisticated way of saving space: they *prune* (or erase) older files or snapshots from versioned backups when certain conditions are met. For example, an app might let you choose the maximum number of copies of any given file to save; once you reach that limit, it prunes the oldest one to make space for newer ones. Or it may go by age—extra versions older than, say, 30 days are deleted automatically to make space for newly backed-up files.

Time Machine does its own sort of pruning: it keeps hourly backups for 24 hours, daily backups for a week, and weekly backups until it runs out of space. That means almost every time it runs, it purges at least some older files. And when your backup disk is almost full, it deletes further files to ensure that, if possible, you always have at least a day's worth of hourly backups and a week's worth of daily backups—even if you're seriously low on disk space.

Without a pruning feature, you could get stuck when your backup media runs out of space: you'd have to migrate your backups to a larger drive or manually erase backed-up files to make room for new ones. So pruning can be a valuable feature, but use it with caution; you don't want to erase files you might need to recover later. All things being equal, I prefer to have a choice as to whether and when pruning should occur. So, especially when you're considering an online storage provider for your backups, pay attention to the flip side of pruning—*data retention*. That is, be sure you know how long the service retains old versions and deleted files, and whether you can adjust the retention period.

File Format and Compression

To oversimplify somewhat, most software employs one of two basic methods to copy files when performing a backup. One way is to copy each file in a standalone Finder-readable format, so that the backed-up files look and act exactly like the originals. Another way is to copy all

the files into a single, larger file (sometimes called an *archive file* or a *backup set*). Each approach has advantages and disadvantages.

Finder-format copies can be restored without backup software; just drag and drop or copy and paste. Some people feel more secure knowing they can get at their files easily even if their backup software isn't working or the developer goes out of business. Generally, each version of each backed-up file takes up exactly as much space as the original. (Time Machine, Personal Backup, and Mac Backup Guru store Finder-readable files but avoid using extra space for identical duplicates, thanks to a Unix trick; see the sidebar [The Magic of Hard Links](#).)

Archive files, on the other hand, can be compressed as they're stored, potentially saving a large amount of disk space. Of course, you'll need the backup software to restore files, and you could have a slightly higher risk of data loss due to file corruption (since all the data is stored in a single file)—but most backup software has verification mechanisms to compensate for this.

Some backup software stores backups in disk images. Like archive files, disk images can thus contain many files and folders—and can optionally be compressed. But their contents are also Finder-readable.

For making a bootable duplicate, Finder-readable copies are obviously mandatory. For versioned backups, I consider Finder-readable files optional; the benefits of compression, along with delta encoding and deduplication (discussed ahead), that you can often get with proprietary archive files may outweigh the slight inconvenience of having to use backup software to restore your data. (Indeed, as I point out in [Ease of Restoration](#), a backup app's Restore feature may turn out to be easier than using the Finder.)

Encryption

If there's any chance at all that your backup drive could be lost, stolen, or otherwise accessible to an unauthorized person, you'll be smart to encrypt its contents.

Some backup apps have built-in encryption features. You see this most often when an app stores backups in proprietary archive files; the archive itself is encrypted.

Encrypting Finder-format copies usually means encrypting the whole volume (using Disk Utility or a third-party tool). The same goes for disk images: they can be encrypted, which protects everything inside them. The contents of the encrypted volume (or disk image) will be protected only when it's unmounted.

If you need an encrypted bootable duplicate, you can use either full-disk encryption software such as FileVault (which is built into macOS) or a hardware-encrypted drive, both of which I cover in the sidebar just ahead.

However, note that if you have a newer Mac with a T2 chip ([see full list here](#)), it can't boot from an encrypted duplicate if that duplicate is formatted as HFS Plus (refer back to [T2 Chips Change the Backup Rules](#)). So you must either forgo encryption on your bootable duplicates or format the destination volume as APFS, create the duplicate, boot from the duplicate, and enable FileVault.

Full-Disk Encryption

FileVault can encrypt your entire startup disk. After booting from a duplicate, you can also enable FileVault on the duplicate in order to have an *encrypted* bootable duplicate; thereafter, any updates to the duplicate will also be encrypted.

Apart from FileVault, I'm aware of three software packages that let you encrypt an entire Mac hard drive—internal or external—in such a way that it remains bootable as long as you have the password. (I still prefer macOS's built-in method, however.) They are:

- ✦ [Check Point Endpoint Full Disk Encryption](#)
- ✦ [Sophos SafeGuard Disk Encryption for Mac](#)
- ✦ [Symantec Endpoint Encryption](#)

Another option is to use a hardware-encrypted drive, which doesn't need separate software and unlocks with a passcode or fingerprint scan. I list several of these in the [online appendixes](#).

Delta Encoding

In years past, almost all Mac backup software performed versioned backups on a file-by-file basis during incremental updates. In other words, if just 10 bytes of a 10 GB file change, that marks the file as modified, and thus the whole file must be copied on the next backup run. Increasingly, however, Mac backup tools (such as Backblaze, QRecall, Retrospect, and even macOS's Versions feature; see [Version Control](#)) have a capability called *delta encoding*, which you may also hear referred to by numerous other terms. By whatever name, it means that the software copies only the changed *portions* of files.

Tip: For more on delta encoding, see the [Delta encoding](#) Wikipedia article.

In some cases, the software copies only the individual *bytes* that have changed since the last backup, and in other cases it copies larger units called blocks (a *block* being a unit of storage typically equal to 4096 bytes—4K—on modern Macs). So, you'll sometimes see this feature referred to as block-level (or byte-level) incremental updates or words to that effect. With backup apps that use byte-level or block-level delta encoding, if only 10 bytes of a file change, only those 10 bytes, or the block(s) containing those 10 bytes, are added to the backup—a tiny amount of data.

The advantage of such an approach is that backups go much faster after the initial run and take up far less storage space. This is particularly important when backing up over the internet. The disadvantage is that restoring a file requires the backup software to reconstruct it by putting together the pieces from all its incremental backups. If even a single one of those incremental bits were to become damaged or lost, you might be unable to restore the file. However, backup software typically performs ongoing verification to ensure that all the necessary bits are present, alerting you or recopying data if any pieces should go missing or become corrupted.

Deduplication

You might have two or more identical copies of a certain file on your disk. Some backup software notices this and puts only one copy in your backup (along with a record that the file appears in multiple places). That way, you save storage space and speed up your backups considerably. Taking this concept further, many backup apps can look within files for *portions* of files that are identical to *portions* of other files and—thanks to delta encoding—copy only the unique parts of the additional files. This process of preventing duplicate data (at any level) from cluttering up your backups is called *deduplication*. Deduplication applies only to versioned backups, not to duplicates (you can see the contradiction in the name!) and is extremely useful.

Almost every online backup app offers deduplication, which is great when you're paying by the gigabyte or trying to push data over a slow internet connection. The result sometimes seems impossible: how did hundreds of megabytes of data just upload in a few seconds? That's deduplication magic at work. QRecall and Retrospect are among the desktop backup apps that can also prevent duplicate data from appearing in your backups—even, in some cases, from multiple computers.

Selectors and Exclusions

Versioned backups may not include every file on your disk. If storage space is at a premium or if you want to save time on network backups, you might choose to include only part of your data in versioned backups (while putting all of it in your bootable duplicates). You can almost always do this manually, by selecting one or more specific files or folders to include or exclude. But some backup apps go further, letting you create patterns indicating which files or folders should be included (selectors) or excluded (exclusions) from a particular folder or volume based on items' names, sizes, Finder labels, extensions, modification dates, and other factors. For example, you might want to include all Microsoft Word (.doc or .docx) files, regardless of their location, or exclude all files over 2 GB, even if they're in a folder that is otherwise backed up.

Snapshots and File Lists

When it comes time to restore files from a versioned backup, you must be able to locate the versions you're looking for easily. Some backup apps facilitate such restorations by offering *snapshots*—lists of all the files being backed up as they existed at the time of each backup. Even though a certain file may not have been copied during a particular backup run (because it hadn't changed since the previous backup), it will appear in the snapshot. You can typically restore all the files in a given snapshot, or delete a given snapshot, in a single operation.

One way of creating snapshots without relying on a separate catalog or file list is to use a Unix feature called a *hard link* (see the sidebar [The Magic of Hard Links](#)), which gives the appearance of a file or folder existing in more than one place even though only one copy is taking up any real space. When backup software creates hard links to all the files or folders it didn't copy in their entirety on a given run, you get a versioned backup that essentially functions as its own snapshot. Time Machine, Personal Backup, and Mac Backup Guru use this approach.

Note: Apple uses the term “snapshot” a bit differently in conjunction with its APFS file system. When your startup drive is formatted as APFS, your Mac automatically stores snapshots (which function much like full backups although they occupy very little space) on your startup volume unless a Time Machine disk is connected; you can access them just like Time Machine backups. I say a bit more about this in the sidebar [Local Snapshots](#); Jeff Carlson covers this feature extensively in [Take Control of Your Digital Storage](#).

Although snapshots are extremely useful, you may want to access your backed-up files in other ways too. Some backup software uses a hierarchical file list that shows you every file and folder you've backed up—and then, for each file, every version it's stored over time. Depending on your needs, this arrangement—starting from the file in question rather than a particular backup run—may be preferable. Time Machine has an elegant hybrid approach, letting you zoom forward or backward in time to see how any given folder appeared at the time of each snapshot.

Without either a snapshot or a file list, you'll need to locate each version of the file manually—often in a series of time- and date-stamped folders. This makes for a long and tedious restoration process, which brings me to...

Ease of Restoration

No matter how easy it is to back up your disk, if your software makes it difficult to restore files, you're going to be unhappy with it. After all, a backup that you can't restore is worthless. Backup apps typically offer one of three main approaches to restoration:

- **A Restore command:** The backup app (usually) tracks all the files you backed up during each session, allowing you to copy them back to their proper locations—or another destination of your choice—with a few clicks. In most cases, before starting the restoration, you can choose a subset of the files, or even pick out one version of a single file if that's all you need. Restore commands and snapshots tend to appear together.
- **Finder restoration:** The backup app has no Restore command; to restore files, you manually drag them (or copy and paste them) from the backup volume onto the original disk. This is fine for restoring an occasional file or folder if it's in a convenient place, but if you've done a versioned backup, you may have to sort through dozens or hundreds of folders to locate the right version of each of your files.
- **Reverse backup:** In this scheme, the backup app once again lacks a Restore command; instead, it expects that you'll swap the source and destination locations and perform your backup again—in reverse. While this may reduce manual effort somewhat, it's still a hassle when restoring files from a versioned backup (except, perhaps, in the case of apps that use hard links), especially when restoring from multiple locations.

I prefer apps with a Restore command; they usually make the restoration easier. Of course, the presence of a Restore feature does not, by itself, mean the process will be easy (for example, some products have

a Restore command that operates only at the level of individual files), but it's a hopeful sign.

Restoring a Full Versioned Backup So It's Bootable

If you're performing a full (rather than selective) versioned backup, bear in mind that not all backup software can restore your backup from an arbitrary point onto a blank disk in such a way that the resulting volume will be bootable. For a full versioned backup to be bootable upon restoration, several things must be true:

- All files needed for your Mac to start up—including many hidden files—must be included in the backup and restored later.
- The backup software must preserve Unix ownership, permissions, and symbolic links during the backup and restoration processes. (This feature requires you to enter an administrator password.)
- When restoring the files, the destination disk must not contain any extraneous files that could interfere with booting. Normally, this implies erasing the disk before restoring the backup.

Time Machine, along with Retrospect and most other backup apps that offer both duplication and versioned backup features, can restore a full versioned backup as a bootable volume, assuming that you set it up properly.

But there's another approach to mixing versioning and bootable volumes, which I cover next.

Bootable Duplicates with Versioning

Most backup apps that offer both versioning and bootable duplicates treat these two approaches as distinct modes, with the expectation that any given backup disk will hold one sort of backup or the other. But rather than storing two separate backups, wouldn't it be nice if a single backup could be bootable and have the added bonus of containing multiple versions of all your files?

As a matter of fact, you *can* do this with several backup apps. But even though that may sound like the best of both worlds, it might not be what you're looking for.

Here's how such a scheme typically works. An app starts by making a bootable duplicate in the usual way (copying all files and attributes to give you an exact copy). On the next and subsequent runs, new and modified files are copied to their respective locations on the duplicate; however, deleted files and older versions, instead of being deleted from the duplicate, are moved to a special location on the backup disk—usually time- and date-stamped folders within an Archive or Safety Net folder—that won't interfere with booting.

That's nifty, no doubt about it. But in the apps I've seen that create bootable duplicates with versioning, the archive of older versions and deleted files is awkward to navigate and restore files from. It's merely a series of folders—perhaps hundreds or thousands of them—in the Finder. And there's usually no Restore feature to help you locate and retrieve those older files.

Plus, even though the versioned files are stored in a location that shouldn't interfere with booting, the fact that you're not making an *exact* duplicate introduces a variable that could potentially complicate troubleshooting. (There's also the minor issue that if you create a bootable duplicate that includes versioned copies of your files and you later restore the duplicate to a blank disk, you'll want to *exclude* the archive folder in order to avoid duplicated files.)

For all these reasons—but mainly the awkwardness of restoring versioned files—I don't recommend using a versioned bootable backup as a *substitute* for a conventional versioned backup. As a *supplement* to a conventional versioned backup, however—or as a substitute for a conventional bootable duplicate—I can't object. If you're creating versioned backups and bootable duplicates already, the additional safety net of versioned bootable duplicates can't hurt.

Here are three apps I know of that offer bootable duplicates with optional versioning as I just described:

- **Carbon Copy Cloner:** My favorite app for bootable duplicates, [Carbon Copy Cloner](#) also offers a SafetyNet feature that stores old versions and deleted files. (See also [Create a Duplicate with Carbon Copy Cloner.](#))
- **ChronoSync:** An all-purpose syncing and backup app, [ChronoSync](#) can archive changed and/or deleted files on the destination, whether or not you're creating a bootable duplicate. (See also [ChronoSync Tips.](#))
- **Déjà Vu:** The optional Safety Net setting in [this backup app](#) lets you store a user-selected number of archives of changed and deleted files in the destination folder of your choice.

Even if a backup app doesn't offer a prebuilt "bootable duplicate with archived versions" option, you might be able to achieve the same effect with another app, by specifying the same destination volume for both bootable duplicates and versioned backups (with the versions stored in a folder at the top level of your backup disk). But because "bootable duplicate" normally means deleting anything on the destination that isn't on the source, these two backup operations might conflict with each other.

Note: Don't forget that if you're combining versioned backups with duplicates, your destination volume will need room to grow; see [Versioned Backup Size.](#)

A backup app called [Mac Backup Guru](#) lets you combine a bootable duplicate (which it calls a Synchronized Clone Backup) with a versioned backup (or Backup with Incremental Snapshots). Like Time Machine, this app creates hard links (see [The Magic of Hard Links](#)) to any files that are unchanged during a given backup run but creates complete copies of files that are new or different, and stores them all in date- and time-stamped subfolders of an Incremental Snapshots folder. The result is that the combination of bootable duplicate and versioned backup uses less disk space than the apps I listed just above,

but restoring individual files is still awkward and Mac Backup Guru offers no automated [Versioned Backup Pruning](#) of older backed-up files.

Ease of Use

In addition to ease of restoration, an app's overall ease of use is important. The interface should be self-explanatory—ideally, clear enough that you can figure out how to perform a basic backup and restoration without looking at a manual. (Time Machine stands out in this regard as being exceptionally easy to use, because it builds on the existing interface of the Finder rather than displaying your files in a completely different context. The downside, though, is that it's impossible to restore files from multiple locations at the same time.) After initial setup, the best backup software is virtually invisible, working silently behind the scenes until you need it.

Price

The backup software included in the [online appendixes](#) ranges in price from free to about \$120 (before discounts). The price does not necessarily correlate to capabilities, but I urge you not to skimp when it comes to backup software; buy the solution(s) that fit your particular scenario the best. Over the life of your data, the right backup software will surely pay for itself.

Choose Another Versioned Backup App

If Time Machine isn't right for you—or if, like me, you want to supplement it with a more robust and flexible option—you'll need to pick a different app for creating versioned backups, keeping in mind the features I've described in [Explore Versioned Backup Features](#), just previously.

I've tested oodles of apps that can create versioned backups (as well as many Mac backup apps that can't), and I've included a reasonably detailed feature comparison chart in the [online appendixes](#). Please

feel free to peruse that at your leisure, download demo versions, try them out, and draw your own conclusions.

Tip: Be sure to look for apps that are being actively developed. If an app hasn't had any updates in a year or more, I'd feel nervous entrusting my data to it.

But if you want my professional advice, I suggest choosing from among just a few that stand out for one reason or another.

Arq

[Arq](#) is an unusual backup app designed to work primarily with cloud storage from providers such as Amazon (Amazon Drive, S3, or Glacier), Backblaze B2, Dropbox, Google Cloud Storage, Microsoft OneDrive, and Wasabi, although it can also back up to SFTP servers, NAS devices, and other local and network locations. Arq supports versioning, encryption, and file-level deduplication, and it faithfully backs up and restores all Mac metadata (such as file ownership and permissions, access control lists, extended attributes, Finder tags, and aliases)—a rare capability among online backup tools. On the downside, it backs up only on a fixed schedule (with a maximum frequency of once per hour). For more information, see [Arq Tips](#).

Note: Recently, several other apps have sprung up with feature sets similar to Arq's, including versioned backups to your choice of cloud storage or local destinations. Although I haven't had a chance to test them extensively, a few that may be worth checking out are [CloudBerry Backup](#), [Duplicacy](#), and [Duplicati](#).

ChronoSync

As the name suggests, [ChronoSync](#) is an app designed mainly for synchronization. For years, it's been one of my favorite tools for syncing folders between my Macs. But it's also a powerful backup tool that can create not only versioned backups but also bootable duplicates (including *versioned* bootable duplicates!). It can also store backups on Amazon S3 or Google Cloud servers (with more cloud destinations

in the works). Thanks to an add-on app called ChronoAgent, it has even joined the rarefied ranks of apps that can create bootable duplicates over a network. See [ChronoSync Tips](#) for additional usage hints.

Farewell, Prosoft Data Backup

For many years, Prosoft's [Data Backup](#) was among my top picks in Mac backup software, but as I mentioned in [Prosoft Ends Development of Data Backup](#), it's no longer under development, has limited support, and is not fully functional on 10.13 High Sierra or later. I'm very sorry to see it go.

DollyDrive

[DollyDrive](#) started out as a way to store Time Machine backups in the cloud. But in just a few years, this Mac-only product has morphed into a full-blown versioned backup, syncing, and sharing service that *doesn't* require Time Machine. DollyDrive still offers cloud storage, but you can also use its software to store versioned backups—or even bootable duplicates—on a local hard drive. You can get a free 14-day trial that lets you store up to 100 GB of data. Monthly costs for unlimited Macs range from \$5 for 500 GB of data to \$25 for 2 TB, but there's also a plan for unlimited storage from a single Mac for \$6 per month, and discounts apply for one- and two-year subscriptions. Read [DollyDrive Tips](#) for additional information.

QRecall

[QRecall](#) can save space by deduplicating files from more than one computer. It offers encryption, compression, and delta encoding, so that large files need not be entirely duplicated every time they change. QRecall works with external hard drives and network volumes, and it has a long list of clever, useful features. However, it can't make bootable duplicates, and it has a peculiar interface that introduces several unusual terms (such as *capture*, *recall*, *layer*, and *timeline*) that force you to think about backups in unfamiliar ways. I help you make sense of these in [QRecall Tips](#).

Retrospect

When I started writing books about backups more than 15 years ago, [Retrospect](#) was my favorite backup app, and I recommended it unreservedly. But as time wore on and impressive competitors appeared—Time Machine, Backblaze, ChronoSync, and dozens of others—Retrospect’s status became more dubious as it stuck with an “old-school” approach to backups and an outdated interface. In recent years, however, Retrospect has enjoyed a comeback. It now has a much-improved interface; it also supports cloud storage destinations (such as Amazon S3, Backblaze B2, Google Cloud Storage, and Wasabi) and delta encoding (which Retrospect refers to as block-level incremental backups). I offer suggestions for using it in [Retrospect Tips](#).

My main complaint was that Retrospect was more complex and expensive than most individual users would prefer, but then its target audience was business users with multiple computers (whether a few or thousands) to back up—and support personnel with enough technical expertise that they wouldn’t be bothered by a bit of fiddling.

But that changed in 2018 with the release of [Retrospect Solo](#), a new version of the app without some of the bells and whistles only a network administrator would want, and with the consumer-friendly price of \$49. Retrospect Solo can do just about any sort of backup an individual Mac user might want, *except* back up to or from a NAS.


[Retrospect Desktop](#), the next step up, can handle NAS devices just fine. It excels at client-server network backups (for both Macs and Windows PCs), for both small groups and large organizations. It can combine multiple hard disks into a single logical backup device—no need for a RAID. It’s one of very few Mac backup apps that can create a bootable duplicate *over a network* (the others being Carbon Copy Cloner and ChronoSync). It also has good support for tape drives, magneto-optical drives, and other storage media that are common in large businesses. One copy of Retrospect Desktop includes five licenses for Retrospect Client—meaning it can back up the Mac it’s installed on plus up to five other computers. (Retrospect also makes editions of the app suitable for larger installations).

Version Control

Although versioned backups are tremendously useful, they store new versions of any given file only when your backup runs—whether once an hour or once a day. In some cases, that’s not enough. For example, if I’m writing a magazine article and something happens to the file, Time Machine might be able to restore a version from an hour ago, but that’s an hour of work lost.

Programmers often use version control software such as CVS (Concurrent Versioning System), Git, Perforce, and Subversion to eliminate all these problems. These tools can be configured to retain a copy of each file every time it’s saved (or as often as the user manually *commits* the file—that is, uses a command that copies it to the repository) and either prevent or coordinate changes to a single file made by more than one person. The Mac apps available for working with these systems are typically quite complex.

However, there are a few version control options that are friendly and convenient enough for ordinary people to use. For example:

- ♦ **Auto Save and Versions:** Many Mac apps (including most of those that support iCloud Drive) can save files automatically and keep copies of every saved version (up to a point, just like Time Machine). To access earlier versions, you can choose File > Revert To > Browse All Versions, or (oddly) choose Enter Time Machine from the Time Machine  menu or click the Time Machine icon in the Dock. To learn more, see Matt Neuburg’s article [The Very Model of a Modern Mountain Lion Document](#) (which still applies to newer versions of macOS). Note, though, that because these versions aren’t stored on a separate drive, they offer less protection than conventional versioned backups; I’d argue that you still need those, even with this feature.
- ♦ **NTI Shadow:** [This backup app](#) includes a version control capability that’s easy enough for anyone to use, works with any file type, and stores copies of your files every time you save them. (Note that as of publication time, the latest version available, 5.0.0.55, appears not to be fully compatible with Mojave.)

Choose a Bootable Duplicate App

I've already mentioned several apps that can create bootable duplicates, including ChronoSync, Data Backup, Déjà Vu, DollyDrive, Retrospect, and SmartBackup. All these apps get the job done, and if you happen to like one of them for any reason, I won't try to talk you out of it. However, I do want to call your attention to two apps that specialize in bootable duplicates and do an impressive job with extra features you may appreciate:

- [Carbon Copy Cloner](#) is my favorite tool for bootable duplicates. It can back up and restore hidden Recovery HD volumes, create a bootable duplicate over a network, and archive old file versions and deleted files (although not, admittedly, in the most convenient way).
- [SuperDuper!](#) includes a Sandbox feature that lets you make a special duplicate in which some key folders are linked, rather than copied, to the destination. The result is that, as long as you keep both the backup drive and the original mounted, you can install software or modify documents on either one, and the changes are reflected on both.

I discuss these special features further and offer more advice about choosing an app for bootable duplicates in my Macworld article [Drive-cloning utilities: The best Mac apps for making a bootable backup](#). And I provide instructions for using them later in this book; see [Create and Use a Bootable Duplicate](#).

Choose Backup Hardware

You're almost certainly going to need one or more external hard drives for your backups. (Even if you use a Time Capsule, other network storage, or a cloud backup service, you'll need a separate external hard drive at least to store a bootable duplicate.) You can find hard drives with every imaginable combination of capacity, speed, interface, and case design—and the selection changes constantly.

In this chapter, I start by walking you through the calculations of how much storage capacity you'll need for backups (see [Decide on Capacity](#)). Then, in [Decide on a Storage Configuration](#), I help you understand whether you should be looking for standalone hard drives, a RAID or other multi-drive enclosure, a NAS or similar network storage device, or drives that you'll hook up to another computer on your network that will function as a backup server.

I end the chapter with a few thoughts on [Hardware You Should Probably Avoid](#).

Tip: In this chapter I'm concerned exclusively with hardware for storing backups, but if you want to know about storage devices more generally—or if you want far more information than I can provide here about file systems, RAIDs, and other storage topics—I recommend reading Jeff Carlson's [*Take Control of Your Digital Storage*](#).

Decide on Capacity

The most important consideration in a backup drive, by far, is its capacity—how many gigabytes or terabytes of data it will hold. In general, the bigger, the better. In fact, I could simply recommend, as a rule of thumb, that you get the largest hard drive you can afford.

However, if you can't afford an especially large drive, or if the amount of data you have to back up is exceptionally large, you may want more

guidance. So, figure out the size you'll need for duplicates, then the size you'll need for versioned backups, and finally the total size to look for.

Duplicate Size

You'll store, on your external hard drive (or a partition thereof), an exact, bootable copy of your Mac's regular startup volume. (If you use a Time Capsule, NAS, or other network storage destination that can't store bootable duplicates, you'll need an entirely separate drive for this purpose.) But the volume that stores your duplicate needs to be only as large as the amount of data on your startup volume, not necessarily the whole disk. For example, if your Mac came with 1 TB of storage but you've filled up only 500 GB of that space, you can fit a duplicate on a 500 GB disk or partition. (If you're creating [Bootable Duplicates with Versioning](#), you'll need to add more space to accommodate the older versions.)

Over time, though, you'll add more files to your Mac, so if you cut it that close, you'll soon outgrow your backup drive. Therefore, I suggest that you allot at least one and a half times the amount of space currently occupied on your startup volume for a duplicate. So, if you have 500 GB of data on your startup volume, you want at least 750 GB for the duplicate. More space is perfectly fine, to give you even more room to grow.

To find out how much space on your startup volume is being used, select the your disk's icon in the sidebar of any Finder window. Then press ⌘-I to display the Info window (**Figure 1**). The number after "Used" is the amount of space currently occupied on the disk.

Tip: If you can't locate your startup volume in the Devices category in the sidebar, go to Finder > Preferences > Sidebar and select the "Hard disks" checkbox.

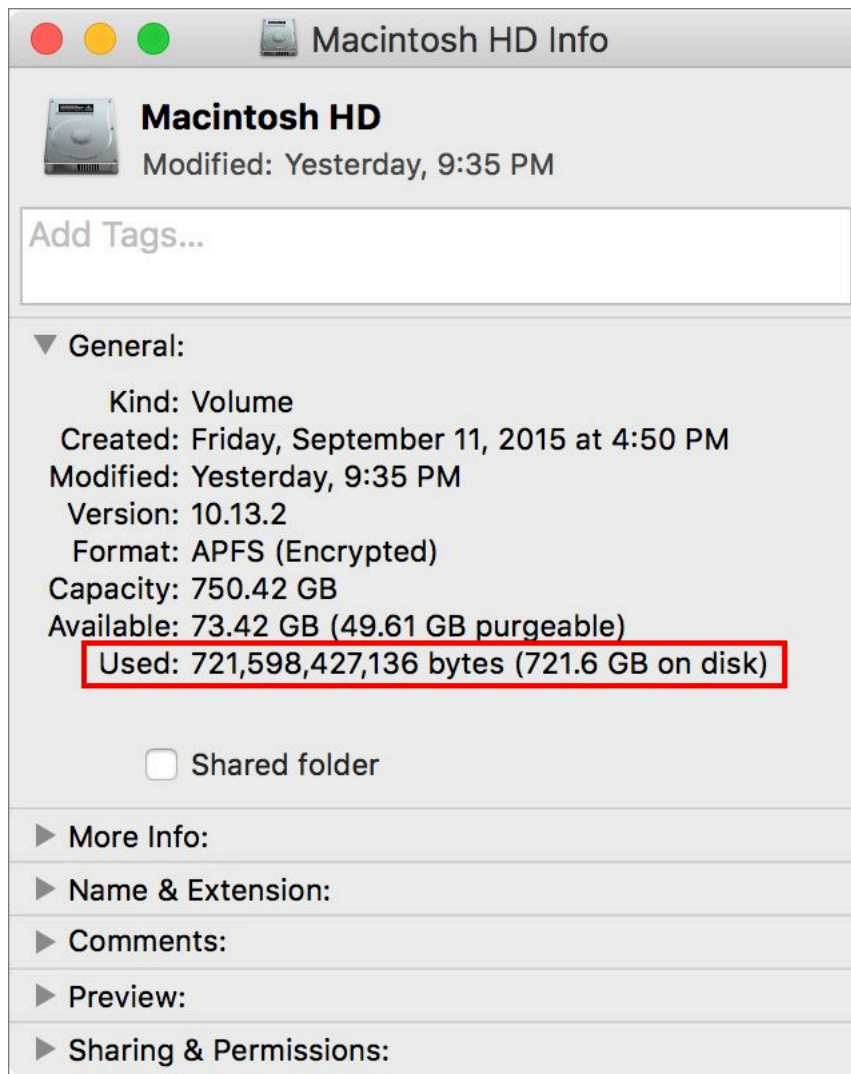


Figure 1: To see how much space is occupied on a disk, select it, press ⌘-I, and look at the number after “Used.”

If you choose to make duplicates of non-startup volumes (such as external disks used for supplemental storage; see [Duplicates of Non-Boot Volumes](#)), follow the same procedure. You can either add the figures and buy a single huge drive (but see also [Consider RAIDs and RAID-Like Tech](#)) or buy separate backup drives for each one.

Versioned Backup Size

Time Machine requires that your destination volume have, as a bare minimum, 1.2 times the space occupied by the data you’re backing up. (That gives some extra space to store multiple versions of at least some files.) So, as a first pass, multiply the “Used” value you saw in the Get Info window by 1.2 to find out the smallest partition size Time Machine

can use. (If you plan to back up additional disks, be sure to factor in their sizes before multiplying by 1.2.)

I must emphasize that 1.2 times is an absolute rock-bottom minimum. You'll be far better off setting aside 1.5, 2, or even 3 times the amount of space used on your disk for backups. The reason is simple: the more space Time Machine has to work with on the destination drive, the more backups it can store—and the farther back in time you can reach when you restore data.

What if you're not using Time Machine? Well, the general principle still holds that you'll want more free space than is currently occupied on your drive, with a bit of a cushion. But a twist is that most other backup software offers compression, deduplication, and/or delta encoding, all of which make your files take up less space on the backup drive than they otherwise would. So, for most people, having free space equal to 1.5 times the amount of data you want to back up should be adequate. But, again, more space is *always* better.

Total Size

Unless you're using a Time Capsule or other network storage device, in which you'll have a separate drive just for a duplicate, your duplicate and versioned backups will ideally live on the same physical disk, so you must now add those two numbers together. For example, if you have 500 GB worth of data, you might choose to allot 750 GB for a duplicate and another 750 GB for versioned backups, bringing the total to a tidy 1.5 TB. That means you should look for a 1.5 TB or larger-capacity drive. But also consider the next-larger size, which is typically 2 TB. If the cost difference is small, as it probably will be, you'll be glad for that extra capacity later on.

You can use a single drive to back up more than one Mac (as I discuss later, in [Choose Local or Network Backups](#) and, more specifically—in the context of Time Machine—in [Use a Single Backup Disk with Multiple Macs](#)). And if you have a few Macs, each with only a modest amount of data to back up, combining backups on a single drive makes sense. Be sure to calculate the space needed (for both duplicates and

versioned backups) for all the Macs you intend to back up and add them together before deciding which drive to buy.

Note: If you intend to store bootable duplicates for more than one Mac on the same drive, each duplicate will need its own partition. I explain how to set this up in [Prepare Your Hard Drive](#).

Now that you have a total, keep that number handy as you go through the rest of the chapter. If you're looking at a very large number for your total storage capacity—that is, more than you can fit on even the largest hard drive you can find—don't panic. We'll address that issue shortly.

Decide on a Storage Configuration

Back in [Choose Local or Network Backups](#), you decided whether you'll attach your backup storage directly to your Mac, access it over your network, or do both. Now that you also know how much storage space you'll need, you have additional decisions to make:

- **For local (directly connected) devices:**
 - ▶ Will you use one or more individual hard drives, or a multi-drive enclosure of some sort? Read [Decide How Many Drives to Buy](#), followed by [Consider RAIDs and RAID-Like Tech](#).
 - ▶ What interface should you use? Read [Choose an Interface](#).
- **For network backups:**
 - ▶ Will you use a standalone device (such as a NAS)—and if so, which one? Read [Network Storage Devices](#).
 - ▶ Or, will you use external drives connected to a Mac on your network? Read [Local Network Servers](#).

If you already know your area of interest, use the links above to jump right to a topic; otherwise, feel free to read through them all in turn.

Decide How Many Drives to Buy

Regardless of whether you plan to do your backups locally or over a network, you'll need at least one external hard drive, because that's necessary for a bootable duplicate.

A single, sufficiently large drive can be divided into two partitions—one for your duplicate and the other for versioned backups. So, assuming you have a modest amount of data, a single hard drive could meet all your backup needs. However, that drive could break down or get stolen, leaving you with no backups. So for extra safety, I suggest having a secondary backup of some sort that can be kept in another location, as I describe in [Store an Extra Backup Offsite](#).

One way to get a secondary backup is to use an internet backup service. If that's the way you choose to go, you can indeed get by with a single external drive and not significantly compromise your data safety.

Another option is to buy a second drive and then switch between the two drives every so often, moving one of them offsite each time. In that case, the optimal number of hard drives is two. Of course, you can do lots of useful things with a hard drive besides storing backups, so having a second one, on general principle, is not a terrible idea.

Note: Although you can use a spare hard drive for many things besides backups, I recommend that you don't mix backups and other data on any given *partition*, because doing so increases the risk of accidentally deleting or overwriting your backups (or that other data).

If you want to be extraordinarily cautious, or if you're paranoid, or if you've had bad experiences with hard drive failures, then you could go a step further and get three hard drives. (I think three is excessive for most people these days.)

But before you hand over your credit card, you might want to skim through the rest of this chapter to explore other hardware options. In particular, if you have a great deal of data to back up, if you demand the highest possible performance, or if you want extra, *extra* protection

against hardware failures, you might consider, in lieu of an individual hard drive, a RAID or other multi-drive enclosure, as I discuss next.

Consider RAIDs and RAID-Like Tech

RAID stands for Redundant Array of Inexpensive Disks (or, more commonly now, Redundant Array of Independent Disks); it's a way of combining several physical hard drives into a single logical volume using either software or a special hardware controller. Of the numerous ways to configure a RAID, two are particularly relevant to the discussion of backups:

- **Striped:** A *striped* RAID (RAID 0) alternates between two or more disks when writing segments of data. (So, the capacity of the RAID is equal to the *total* capacity of the member disks.) Striped RAIDs let you combine multiple disks into larger volumes with faster performance (since all disks can be accessed in parallel), but if an error occurs on any disk, the entire RAID will fail.
- **Mirrored:** A *mirrored* RAID (or RAID 1) writes the same data simultaneously to two or more disks. (So, the RAID capacity equals the capacity of the smallest member disk.) If any one drive fails, another can take over instantly and seamlessly with no loss of data and no down time; you can then replace the faulty drive at your leisure.

RAIDs with more than two disks can have other configurations, including RAID levels 2 through 6 and several combinations of levels. (You can read about the various forms of RAID in [Wikipedia](#).)

Before I explain why you might care about a striped or mirrored RAID, I want to mention a few technologies that look superficially like RAID but are in fact quite different underneath:

- **JBOD:** Some manufacturers sell enclosures for multiple disks that share a power supply, controller, and interface(s)—but each of these disks is independently accessible from your computer. Although you could use software to combine them into a RAID, in their native state they're JBOD (Just a Bunch of Disks).

- **Concatenation:** You can also use either hardware or software to combine two or more independent disks into a single logical volume whose size is the total of all the disks combined. That might sound like a striped RAID, but the data doesn't alternate between disks; it's stored sequentially, so there's neither a performance benefit as with RAID 0 nor data redundancy as with RAID 1—and if any one drive fails, the whole volume can fail. Concatenated disks sometimes go by the names BIG or SPAN (which don't stand for anything) and are sometimes incorrectly referred to as RAIDs. The size of a concatenated volume is equal to the sum of the sizes of all its member disks.
- **BeyondRAID:** Data Robotics uses the trademarked name BeyondRAID to refer to a method of combining disks into a larger volume that provides data redundancy while maintaining the capability to use disks of different sizes and to dynamically change the array's configuration, things you can't ordinarily do with a RAID. I say more about this ahead, in [Drobo Storage Devices](#).

Why You Might Care About a Striped RAID, JBOD, or Concatenated Storage

The highest-capacity individual drive mechanism available to the general public in early 2019 holds 14 TB. (At publication time, prices start around \$500.) But you might have more than 14 TB of data to back up, or be unable to afford a single jumbo-sized drive. There's a solution: a number of companies sell devices that appear to be external hard drives but hold *more* than 14 TB, because their cases contain *multiple* drive mechanisms (for example, two 8 TB disks). The enclosure's circuitry combines the two disks into a larger volume; sometimes it's a high-performance striped RAID 0 volume, sometimes it's merely concatenated, and sometimes it's JBOD but with hardware or software features that let you reconfigure it as a RAID (perhaps even a mirrored RAID 1, for more fault tolerance but half the capacity).

The good news is that such devices offer the benefit of a large, fast disk without making you cobble together your own hardware- or software-based RAID and deal with lots of boxes and cables. The bad news is that if you use RAID 0 and a mechanism in your enclosure dies, you

could lose *all* the data on *both* drives. Even in the best case, you'll have to send the device back to the manufacturer for repair. And, if one of two or more concatenated disks fails, you may not be able to get the data on the remaining disk(s) without the manufacturer's intervention.

I'm not saying you should avoid such devices; I'm saying you should know what you're getting into if you rely on them. Mathematically, your chances of losing the data on RAID 0 or concatenated disks are at least double that of a single mechanism of the same type. So if you get a multi-drive enclosure and have the choice, I suggest that you use RAID 1 or higher, because all levels of RAID beyond 0 offer redundancy to protect data in case of drive failure (along with a reduction in capacity).

Why You Might Care About a Mirrored RAID

Mirrored RAIDs have at least two copies of your data, so, unlike striped RAIDs, they protect you against drive failure. The downside is that you need twice as many disks for a given amount of capacity. Some people believe that a mirrored RAID consisting of their Mac's internal drive plus an external drive of the same capacity is effectively the same thing as a duplicate—only better, because it's always 100% up to date. I beg to differ.

I have nothing against mirrored RAIDs. However, a RAID, by itself, is no substitute for multiple duplicates as described in this book. A mirrored RAID's best feature is also its Achilles' heel: because changes are reflected on all drives at once, an accidentally deleted (or damaged) file will be immediately deleted (or damaged) on your "backup" drives too! (Standalone duplicates—especially if you maintain two or more of them—reduce this risk greatly.) RAIDs address the problem of drive failures but provide no insurance against human error, theft, or any of the other catastrophes that make backups so important. And, like backups stored on extra internal hard drives, RAIDs do you no good if your computer is stolen or in the shop for repairs.

So, if you use a mirrored RAID to protect yourself against drive failure, that's fine...but you still need a separate bootable duplicate. (A mirrored RAID with *more* than two disks *can*, in certain situations,

substitute for a bootable duplicate; I explain one way to set this up ahead, in [Creating a RAID with SoftRAID](#).)

The BeyondRAID system used in Drobo devices also provides data redundancy, and can also (in some cases) be used as a bootable duplicate. However, Drobo's benefits and limitations are fundamentally different from those of a conventional mirrored RAID, as I explain in [Drobo Storage Devices](#).

Creating a RAID with SoftRAID

Geek alert: If you're technically inclined, have a bit of money, and want a RAID-based backup system that makes your friends in IT jealous, read on. If none of that sounds like fun (or even English), feel free to skip over this topic and jump ahead to [Drobo Storage Devices](#).

I said earlier that you can join multiple external disks into a RAID using either software or a special hardware controller. Apple's Disk Utility lets you create simple software RAIDs. (This capability disappeared in 10.11 El Capitan but was restored in 10.12 Sierra.) For anyone needing more flexibility than what Disk Utility offers (or for Mac users running El Capitan), the best tool for the job is [SoftRAID](#). Install this software (included free with some multi-drive enclosures) and you can create a RAID with any of several configurations and modify it as necessary if you add or replace hard drives.

For the purpose of this book, what I find most interesting about SoftRAID is that when it comes to bootable duplicates, it lets you have your cake and eat it too. You can create a RAID in which your internal disk is mirrored onto *two or more* external drives at once. Then, periodically rotate one of the drives offsite, where it will function as a standalone duplicate of your disk at an earlier state. When you plug it back into your Mac, it will automatically synchronize with the remaining drives in the RAID. The beauty of this approach is that you never have to set up, schedule, or run backup software to make duplicates; it happens automatically and is always perfectly up to date.

You'll still need a separate way to handle versioned backups, of course, such as Time Machine or ChronoSync. One extremely clever configuration is to split each of your external drives into two partitions—one for your mirror and one for your versioned backups. That way, you don't have to maintain separate drives for each purpose—whichever drive you have connected at any moment will be both a mirror (and, when disconnected, a bootable duplicate) and a versioned backup.

To pull this off, you'll need the full version of SoftRAID and two or more external drives, each with plenty of capacity (ideally, three or more times that of your internal drive). For example, if I were doing this on a Mac with a 1 TB SSD, I'd use 4 TB external drives. I refer you to the SoftRAID documentation for the details of each step, but the broad outline is as follows:

1. With SoftRAID installed on your Mac, create a bootable duplicate of your startup volume (see [Create and Use a Bootable Duplicate](#)).

Tip: I'd make two duplicates at this point, to be safe—you're about to erase your internal drive!

2. Boot your Mac from the duplicate.
3. Connect the (blank) external drive you'll use for the RAID.
4. Use SoftRAID to initialize your Mac's internal disk and the external disk.
5. Create a mirror (RAID 1) volume with these two disks.
6. Still using SoftRAID, create a second volume with the remaining partition space on the external drive. This is what you'll use for your versioned backups.
7. Use whichever app you employed in step 1 to clone your current startup volume (the bootable duplicate) back onto the new RAID.
8. Open SoftRAID again, select the newly cloned volume, and choose Volume > Rebuild Boot Cache. (Without this step, your Mac won't boot from the RAID.)

9. Go to System Preferences > Startup Disk, select the newly created RAID as your startup disk, and click Restart.

Once your Mac has restarted from the RAID, you can set up Time Machine (or another backup app) to store versioned backups on the external drive's spare partition. Then, if you want to include another external drive in the RAID, you can connect it and use SoftRAID to initialize it and add it to your existing RAID volume.

Whenever you disconnect an external drive from your RAID, your Mac continues running from the internal drive (and the remaining external drives, if any), but if you disconnect all the external drives, Time Machine won't run until one of them is reconnected. Reconnecting a drive that's part of the RAID causes it to rebuild itself automatically, so that it matches the internal drive.

This configuration amounts to a nearly bulletproof backup system. As long as you remember to swap external drives periodically (say, once a day), you'll have all the benefits of a mirrored RAID, a bootable duplicate, *and* a versioned backup. Great, right? (Granted, this solution works better for desktop Macs than for laptops, because it requires you to keep at least one external drive attached much of the time.)

There are, however, some [limitations in SoftRAID 5.7.3](#) (the latest version shipping at publication time) and earlier that you'll want to be aware of:

- SoftRAID 5.x doesn't support APFS drives at all, so if you're running High Sierra or Mojave and your startup disk is formatted as APFS, SoftRAID would be useful only for other, non-startup volumes.

Note: At publication time, version 6.0 of SoftRAID—which will fully support APFS drives—was in beta testing, and had been for well over a year. You can [ask to be a beta tester](#).

- SoftRAID does not support any disk configuration that depends on Apple's CoreStorage technology, which includes both Fusion drives and FileVault when the drive is formatted using the HFS Plus file system. (Again, SoftRAID 6 running on APFS drives should fix this.)

- If you're using one or more hard drives in a mirrored RAID along with an SSD startup volume, your overall performance could suffer since the hard drives will be unable to read and write data as quickly as the SSD. Of course, you can add external SSDs to a RAID...if you can afford them!

I can't wait for version 6.0 to appear, because a multi-drive, bootable, encrypted, mirrored RAID setup with versioned backups as I've described here has been a goal of mine for a number of years!

Drobo Storage Devices

[Drobo](#) storage devices are much like RAIDs, in that they let you combine multiple disks into a single, higher-capacity volume. Depending on the model, a Drobo can hold anywhere from five to eight hard drive (or SSD) mechanisms. Some have local interfaces such as USB 3.0, Thunderbolt 2, or Thunderbolt 3; others have gigabit Ethernet interfaces. Although the models have various other differences too, they all have the following in common:

- You can hot-swap drives.
- You can mix and match drives—any number, capacity, speed, or manufacturer.
- Part of the space on each drive is set aside for data redundancy, so if any single drive fails, all the data remains intact. You can simply swap out the malfunctioning drive as if nothing happened.
- The Drobo automatically reconfigures itself as you add or remove drives; no manual intervention is required at all.

This set of capabilities (along with a few other niceties) is collectively known as BeyondRAID. That's an apt name, because Drobo does all the things a RAID can do and then some. With a conventional RAID, for example, all disks must have the same capacity, and adding or removing a volume requires lengthy, tedious reconfiguration.

As a result, a Drobo is a good way to ensure you always have enough capacity for your backups. All Drobo models work with Time Machine, and those with local interfaces can also be used as Mac boot volumes.

You can even partition a Drobo into two volumes, one for bootable duplicates and the other for versioned backups.

However, even though you can use a Drobo for bootable duplicates and can remove one (or in some cases two) of them without data loss, you *cannot* boot from any individual drive, nor can you use the drives apart from the entire set to reconstruct your disk. That means the trick I described earlier with SoftRAID—using two or more mirrored disks and rotating one offsite in lieu of maintaining separate bootable duplicates—*isn't* feasible with a Drobo. And although you could back up to two or more Drobos and rotate one offsite, the hassle and expense of doing so may be prohibitive.

So, while it could be a valuable component of a backup system, especially if you work with extremely large files, a Drobo alone probably won't meet *all* your backup needs.

Choose an Interface

Your hard drive, RAID, or other multi-drive enclosure will use one of several interfaces to connect to your Mac: Thunderbolt, Thunderbolt 2, Thunderbolt 3, USB 3.0, USB 3.1 Gen 1, or USB 3.1 Gen 2 (see the sidebar [USB 3.1, USB-C, and Thunderbolt 3](#), ahead). You can buy hard drives with various combinations of these interfaces. In general, drives with a single interface are less expensive than drives with more than one, and as single-interface drives go, USB 3.0 drives are nearly always the cheapest, while Thunderbolt 3 is the most expensive. However, money isn't the only consideration.

When considering which interface(s) to get, keep in mind the following factors:

- **Speed:** In general, the faster the interface's transfer speed, the less time it will take to back up and restore files. However, after an initial full backup, extra speed offers much less benefit for backups than it does for, say, real-time video editing; since backups typically happen in the background anyway, you may not notice the speed boost from a faster interface.

On paper, the theoretical speed with which these interfaces can transfer data goes in this order, from slowest to fastest: USB 3.0 and USB 3.1 Gen 1 (5 Gbps); Thunderbolt and USB 3.1 Gen 2 (10 Gbps); Thunderbolt 2 (20 Gbps); and Thunderbolt 3 (40 Gbps). However, note that theoretical speeds don't necessarily match up to real-world performance. In addition, be aware that for nearly all modern hard drives, the bottleneck is their built-in SATA III interface, which maxes out at 6 Gbps. That means that for single drives, a higher-speed interface (such as Thunderbolt 2 or 3) won't provide speed benefits over Thunderbolt or USB 3.1 Gen 2.

- **Hardware support:** Recent Macs have ports supporting one or more of the following standards: USB 3.0, USB 3.1, Thunderbolt 2, and Thunderbolt 3 (see the sidebar [USB 3.1, USB-C, and Thunderbolt 3](#), ahead). Macs can boot from external drives connected to any of these ports.

Think about not only what interface(s) your *current* Mac has but also what your *next* Mac will have. Apple has completely phased out the old FireWire and USB 2.0 interfaces. USB 3.0 is still hanging on, but barely, while USB 3.1 and Thunderbolt 3 (which share the same connector) are the interfaces most likely to be with us for years into the future.

So what's the bottom line? Nowadays, USB 3.x is generally your best bet, because USB 3 drives are extremely fast (even if not quite up to Thunderbolt speeds), plus cheaper and far more plentiful than Thunderbolt drives. And remember, even though Thunderbolt is faster, individual drives can't take advantage of that speed; only RAIDs and similar devices will benefit from that speedy Thunderbolt throughput.

Given the choice, a drive with a USB-C connector and support for USB 3.1 Gen 2 is the highest-performance and most future-proof option, and you can easily connect such a drive to a Mac with a USB 3.0 port using an adapter cable. A USB 3.0 drive can still be plenty fast, however, and you can use that very same adapter cable to connect it to a newer Mac with a USB-C or Thunderbolt 3 port.

USB 3.1, USB-C, and Thunderbolt 3

The 12-inch MacBook (Retina, 2015) was the first Mac model to feature a port that supports the USB 3.1 specification. The first generation of USB 3.1 (Gen 1) has the same throughput as USB 3.0 (5 Gbps)—indeed, it’s exactly the same, except for the connector—and that’s the version the 2015 (and 2016) MacBook uses. USB 3.1 Gen 2 is twice as fast: 10 Gbps, the same theoretical speed as the original Thunderbolt. (The late-2016 MacBook Pro models were the first Macs to support Thunderbolt 3 and USB 3.1 Gen 2.) Like previous versions of USB, 3.1 is backward-compatible: you can hook up USB 1.1, 2.0, or 3.0 devices to a USB 3.1 port (though the older devices won’t benefit from USB 3.1’s higher speed).

Appearing at the same time as USB 3.1 is a new USB Type-C (or USB-C) connector, which joins the Type-A, Type-B, mini-USB, and micro-USB connectors we’ve all been using for years. The USB-C connector is interesting in that it’s both compact and symmetrical (unlike the rectangular USB Type-A connectors, which go in only one way but hardly ever the first way you try). In addition, USB-C can handle more current (for charging) than earlier connector/cable varieties and can transfer USB data and other data simultaneously. For example, a single USB-C connector can be used for charging, transferring data, and delivering audio and video output (with an adapter or hub).

Even more interesting, Thunderbolt 3 uses the USB-C connector and supports the USB 3.1 protocol natively. That means you can plug a USB 3.1 peripheral into a computer with a Thunderbolt 3 port and it will work just fine. Unfortunately, that support doesn’t work in the other direction; a computer (like the 2015 or 2016 MacBook) that supports only USB 3.1 won’t let you use a Thunderbolt 3 peripheral, even though the connector is identical.

External USB 3.1 hard drives, flash drives, and other devices with USB-C connectors are becoming easier to find, and if your Mac has such a connector (with or without Thunderbolt 3 support), those are fine choices. Note that a USB-C connector also works with any USB 2.0 or 3.0 device, as long as you have an adapter.

Evaluate Network Storage Options

If you know that you'll be using network backups—alone or in combination with local drives—you'll next want to figure out whether to use a standalone appliance for this purpose, and if so, which one (see [Network Storage Devices](#), next); or whether you want to use another computer on your network as a backup server (see [Local Network Servers](#)).

Network Storage Devices

The term *NAS*, or network-attached storage, typically refers to a box containing one or more hard drives, a bit of computing power, and a wired or wireless network interface—sort of a minimalist file server. (Sometimes NAS devices are simply called *network drives*.)

Ethernet-equipped Drobo models are examples of NAS devices. Apple's Time Capsule was also a type of NAS device (more on this in a moment). Similarly, an Apple AirPort Extreme Base Station with an external USB drive (an AirPort Disk) could be considered a NAS, but only the most recent (tower-shaped) AirPort Extreme models let you use an AirPort Disk for Time Machine backups.

NAS devices are frequently marketed as backup (and all-purpose file storage) solutions for small networks. The idea is that you can set up a centralized file server without needing an additional computer, and every computer on your network can back up files to it. Some NAS equipment can also communicate with your home entertainment system, providing storage for audio and video. And newer NAS devices that use the Btrfs file system can take snapshots of your data manually or at scheduled intervals, which produces an effect similar to storing versioned backups: you can at any time restore your data to its state when a snapshot was taken.

Although a NAS device can indeed be useful in many situations, you should keep in mind a few important considerations when thinking about using one as a backup destination:

- Some NAS models can run their own backup software (that is, the NAS runs the server app, and each of your Macs runs a client).

That's a perfectly valid setup, but because you can't install just any arbitrary backup software on any given NAS, you may be stuck with whatever app the manufacturer offers, or whatever third-party options may be available for that particular platform. This approach may limit your flexibility and prevent you from setting up your backups in precisely the way you'd prefer.

- If your NAS can't run its own backup software—or if you're unhappy with the software it offers—you can still use it for push backups (see [Network Backup Approaches](#)) and run the backup app of your choice on each Mac. Performance and reliability may take a hit over what client-server backups offer, however.
- Irrespective of the points above, some NAS models—mostly newer ones—support Time Machine. If the model you choose does, you can follow the manufacturer's instructions to set it up as a destination for your Macs. But be sure to confirm compatibility before you make your purchase.

Tip: I list a number of NAS devices that support Time Machine in the [online appendixes](#).

- Some older NAS devices can only be formatted using FAT32, a Windows file system. Although macOS can read from and write to FAT32 volumes, some metadata may not be stored properly. Your backup software may address this limitation by storing data in a special archive file, but if it backs up files in a Finder-readable format, you risk losing data.
- You can't create a bootable duplicate onto a NAS (and even if you could, you wouldn't be able to boot your Mac from it). The only way to create a bootable duplicate over a network is to back up to a drive connected to a Mac running one of a very few backup apps specially designed for this purpose (Carbon Copy Cloner, ChronoSync, or Retrospect).
- And don't forget, your NAS itself should be backed up to another destination; see [Back Up a NAS](#).

All that said, with the right hardware and software a NAS can make an excellent storage medium for versioned backups of several computers' files, and thus a valuable component of a broader backup strategy.

For those wanting to use Time Machine to back up to a NAS, Apple's AirPort Time Capsule was once the optimal solution. Even though it was more expensive than competing products, it was expressly designed to work in this configuration. Unfortunately, as I mentioned in [Time Capsules Officially Bite the Dust](#), since the previous version of this book was published Apple stopped selling the Time Capsule and all other AirPort products. If you still have one, you can use it (until the hardware eventually fails), but it's no longer a good long-term solution.

Local Network Servers

If, in your home or office, a Mac or PC is functioning as a file server, it's worth considering whether you could use a network volume as a backup destination. After all, a full-blown computer is likely to give you both better performance and greater flexibility than even the fanciest NAS. (And, if you have the computer already, you won't need to buy another device.)

In general, if you have control over the server yourself and it's not already bogged down with other tasks, using it for backups is a fine idea. I strongly recommend adding a separate physical hard drive, and either configuring the server—if it's a Mac running High Sierra or later—as a Time Machine server (see [Use a Mac as a Time Machine Server](#)) or installing client-server backup software (see [Network Backup Approaches](#)). Otherwise, your backups will be commingled with other files, making it difficult to store them offsite and potentially creating a security risk.

If you do not personally have control over the server (for example, if it's a shared company server), resist the urge to use it for backups. You could easily use up more space and network bandwidth than you should (thus incurring the wrath of your IT department), and you'll have less control over your data than if you use local media.

Hard Drive Selection Tips

There are zillions of hard drives to choose from, with every imaginable combination of physical size, capacity, speed, interface, price, and other factors. Beyond choosing an affordable drive with the capacity you need, here are some extra tips:

- ✦ **Go for bus power:** If you spend a lot of time on the road, you'll appreciate the extra portability of a 2.5-inch drive, especially if you get one that can draw power from a USB or Thunderbolt port without requiring a separate AC adapter (I list some examples in the [online appendixes](#)). In fact, I prefer bus-powered 2.5-inch drives even for my home backups because they reduce cable clutter and noise. But be aware that these drives have a smaller maximum capacity than 3.5-inch drives: at publication time, the highest-capacity 2.5-inch drives available hold only 5 TB.
- ✦ **Check the warranty:** Most hard drives (of any brand) come with a one- or two-year warranty and can be expected to have a useful life of at least five years. (A few drives have warranties as long as five years, and that's certainly a strong selling point.)
- ✦ **Investigate reliability:** According to some reports, such as [one published periodically by cloud backup provider Backblaze](#), drives by HGST tend to have the best long-term reliability, while Seagate drives are the least reliable—though the specifics depend on the exact model. Your mileage may vary, because these reports study drives in constant, high-stress use. Still, all things being equal, you might prefer to buy a brand with better reliability statistics.

Hardware You Should Probably Avoid

One final word before we move on to the next chapter. I've said that hard drives of one kind or another are your all-around best bet as a storage medium and that online storage is worth considering as an easy, secure alternative to rotating physical media offsite. But there are other kinds of backup hardware, and I want to head off all the "Yeah, but what about..." inquiries.

So let me give you a quick rundown of hardware I think you should probably *not* consider:

- **Optical media:** The various flavors of recordable CDs and DVDs are collectively known as *optical media*. Apple has moved past optical drives in Macs, and even if your older Mac does have an optical drive, it will be slower and have a much smaller capacity than a hard drive. The data on optical discs can deteriorate to the point where it's unreadable, sometimes in just a few years (see [Consider Long-Term Archive Storage](#)). And who knows if you'll be able to attach an optical drive of any kind to the Mac you might own in five or ten years? If you used optical media in the past, I recommend moving to hard drives for backups *right now*.
- **Flash drives (including external SSDs):** You can buy USB 2 or USB 3 “thumb” drives that will store as much as 2 TB in a very small space. These drives are handy for moving data from place to place, and they're fine for making quick extra backup copies of truly critical files as you work. But for regular backups, the cost per gigabyte is still way higher than even a high-end hard drive, making them unattractive as the primary storage medium for full backups. The same goes for higher-speed external SSDs packaged in USB and Thunderbolt enclosures (although, admittedly, prices are finally starting to drop). If you can afford them, knock yourself out. On the other hand, I think flash drives are an increasingly logical choice for *partial* backups while on the road, and as prices fall even further and capacities increase, I wouldn't be surprised if they eventually become an even more economical choice than hard drives.
- **SD cards:** Some Mac models include built-in SD card slots, which are primarily designed to let you easily transfer data from your digital camera or camcorder. But since the SD card mounts as a regular Finder-accessible volume, you can easily use it to store backups, too. What I said just previously about USB flash drives applies here too: there's nothing wrong with them in principle, but they're currently too limited in capacity, and too expensive per gigabyte, to use as one's main backup medium. That said, where a

flash drive would work for a quick backup on the go, an SD card should work equally well.

- **Tape drives:** Drives that store your data on digital tape cartridges of one kind or another are common in big businesses, but they're more cumbersome than hard drives, they require a lot of media swapping (or a robot to do it for you), and they're relatively expensive (that is, the *drives* are expensive; the media itself isn't). For home or small-office users, they're a poor choice.

Prepare Your Hard Drive

You’ve just unpacked your brand-new hard drive (or two), and you’re ready to get busy backing up. You might be able to plug in the drive and start working with it immediately, but it depends. Some hard drives come formatted for Windows computers, for example, while others might be formatted for a Mac—or not at all. Some come preloaded with utilities and demo software. Some might use the wrong partition map scheme for your computer, possibly preventing Time Machine from being able to see or use the drive. And if you’re not going to plug a hard drive directly into your Mac, but rather put it inside, or attach it to, a network storage device, still other considerations apply.

In short, because each situation is different, you should take a few minutes, before you do anything else, to make sure any new hard drives you’ve obtained are configured correctly for your needs.

If you have a NAS, Time Capsule, or other network device, its built-in drive(s) should come preconfigured as needed, so you don’t have to worry about anything in this chapter for that device (but skip ahead to [Network Backups](#) for additional factors to consider). However, you must still follow these steps for the external drive you use to store your bootable duplicate, and any external drive(s) you decide to attach to your Time Capsule or NAS.

Note: For a RAID, Drobo, or other locally attached, multi-drive enclosure, the rules are highly variable; consult the manufacturer’s instructions or website to learn whether or how you must format the drives.

Choose a Partition Map Scheme

Your hard drive contains a tiny block of information called a *partition map* or *partition table* that describes things like how many volumes

the drive has, how large they are, and where they're located. The way information is stored in this little block of data is called the *partition map scheme*, and the choice of scheme is crucial to how the drive can be used. Windows PCs generally use a scheme called the Master Boot Record (MBR) Partition Table; pre-Intel Macs used a scheme called Apple Partition Map; and Intel-based Macs by default use a newer and more advanced scheme, GUID Partition Map (or GUID Partition Table). The partition map scheme affects the entire drive, regardless of how many partitions it has or how those partitions are formatted.

The majority of hard drives are configured at the factory to use the MBR scheme, because that's the norm on Windows. In most cases that's fine; if you plug such a drive into your Mac, it will most likely work as a backup drive without any intervention. However, it's worth noting that Time Machine can't use volumes larger than 512 GB on an MBR-partitioned drive. (That's because Time Machine requires the Mac OS Extended format, also known as HFS Plus, and HFS Plus volumes can't be larger than 512 GB on an MBR-partitioned drive.)

You normally need not worry about this; if you select a disk to use as a Time Machine destination and it's partitioned using the MBR scheme, macOS will offer to repartition it for you as a GUID disk automatically. But, if you don't want to use the *entire* disk for Time Machine backups—for example, if, as I suggest, you want to divide the disk into a partition for Time Machine (or other versioned backups) and a partition to hold a bootable duplicate—then you should manually repartition the disk *before* handing it over to Time Machine. As you do, you should check the partition map scheme, because changing it requires erasing all the data on the disk; that's obviously something best done before you've copied any of your personal files onto it.

Although there are a couple of ways to check your drive's partition map scheme, I recommend using Disk Utility—and then just leaving it open, because you'll be using it to format your drives in just a moment (see [Configure Your Drive](#)). Follow these steps:

1. Open Disk Utility (in [/Applications/Utilities](#)).
2. In High Sierra or later, choose View > Show All Devices.

3. In the list on the left, select your external drive. (The drive may have icons for one or more volumes, indented underneath it; if so, select the device's topmost icon, representing the drive as a whole.)
4. Look near the bottom of the window next to "Partition Map" or "Partition Map Scheme" (**Figure 2**). It should say GUID Partition Map (or GUID Partition Table) or Master Boot Record.

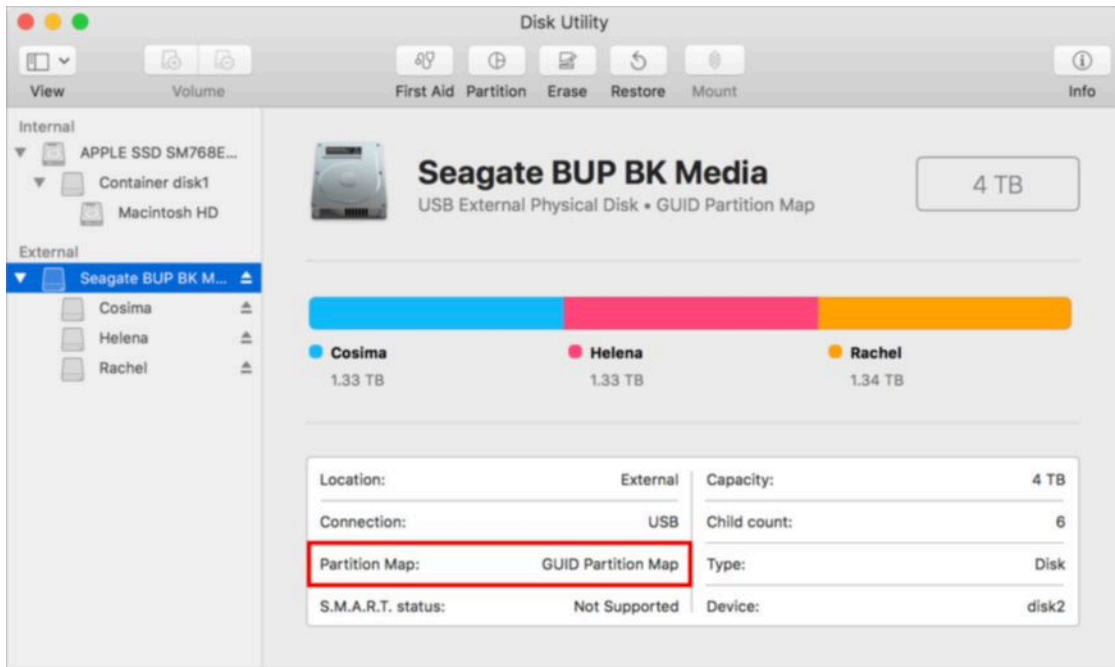


Figure 2: Not sure which partition map scheme your drive uses? Look here. (Your version of macOS may look a bit different.)

Which partition map scheme do you want? The rules are as follows:

- If your backup drive has a capacity of 512 GB or more, or if you plan to partition it such that any volume will be 512 GB or more, choose GUID. This is by far the most common choice for Mac users.
- If your backup drive has a capacity of less than 512 GB—or if you plan to partition it such that each volume is less than 512 GB (see [Decide How Many Partitions to Make](#), next)—any scheme, including MBR, is acceptable; however, if you use Time Machine keep in mind my earlier comments about it and MBR. And if you ever want to use a volume on this drive to boot a Windows PC, MBR is mandatory.

For now, simply keep in mind which scheme you chose, whether GUID or MBR. You'll apply it, if necessary, in a few moments.

Decide How Many Partitions to Make

Wait, didn't we already decide this? Well, yes. Back in [Understand Joe's Basic Backup Strategy](#), I described how you can partition your external drive into two volumes—one each for duplicates and versioned backups. However, in some cases you might want to have just one partition, or more than two:

- **NAS or Time Capsule:** If you're using a third-party NAS device or a Time Capsule to store your versioned backups, you'll be using the external drive just to hold your duplicate, so it may need only one partition.
- **Lots of data:** If you have so much data to back up that you can't fit two adequately sized partitions on the drive, then you'll stick with one, using separate drives for your duplicate and versioned backups.
- **Not so much data:** If you have only a small amount of data to back up but a truly humongous drive, you might feel that you'll never fill all that space with backups and you might therefore want to use some of it for something else. In that case, feel free to make three (or more) partitions, with the first two sized as I discussed in [Decide on Capacity](#).
- **Bootable duplicates for multiple Macs:** If you want to store bootable duplicates for more than one Mac on a single drive, you'll need a separate partition for each, as I discuss later in this chapter, in [Choose Local or Network Backups](#). *Versioned* backups for all your Macs, however, can live on a single partition.
- **Bootable duplicate with versioning:** If you're creating [Bootable Duplicates with Versioning](#) instead of separating the two (a less than ideal strategy, in my opinion), you'll need just one partition.
- **Duplicate(s) of non-boot volume(s):** If you choose to make non-bootable duplicates of external drives (see [Duplicates of Non-Boot Volumes](#)), you'll need a partition for each of those, too.

Keep Time Machine Backups Separate from Other Data

When you're deciding how to partition a drive, I strongly suggest that whichever volume you use as a destination for Time Machine should be used *only* for Time Machine.

In certain situations, having Time Machine backups and other data (such as your Photos library) on the same partition can result in permissions problems and other errors that could lead to data loss. So, If you need to store other data on an external drive besides Time Machine backups and bootable duplicates, the safest policy is to segregate Time Machine backups onto their own partition.

Configure Your Drive

Now that you have those two vital pieces of information—which partition map scheme to use and how many partitions you need—you have only to click a few buttons to configure your drive.

Warning! This procedure totally and irrevocably erases everything on your external drive. You knew that, but this being a book about backups, one can never have too many copies of crucial data!

The steps you'll follow depend on your operating system version.

Configure a Drive in El Capitan or Later

Follow these steps:

1. If Disk Utility isn't already running, open it now (it's located in [/Applications/Utilities](#)).
2. In the list on the left, select your external drive.
3. Click Erase. A dialog (**Figure 3**) appears.

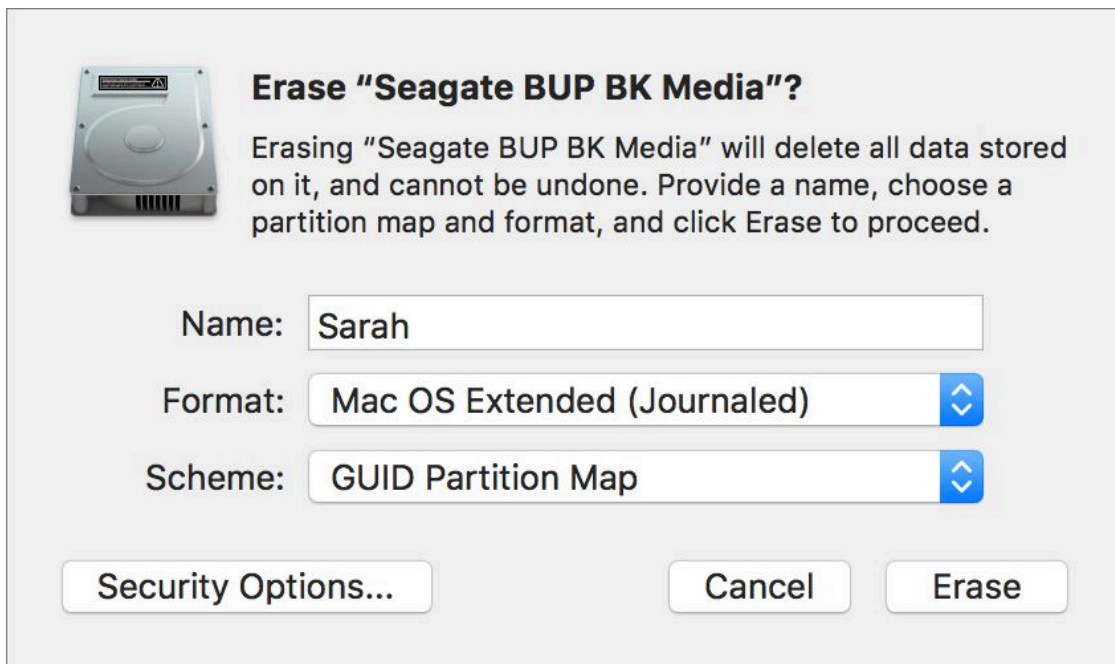


Figure 3: In El Capitan or later, choose the options for erasing a drive in this dialog (High Sierra version shown here).

4. Type a name for your disk and choose your desired scheme (most likely GUID Partition Map) from the Scheme pop-up menu
5. Choose a format from the Format pop-up menu:
 - ▶ If you're running High Sierra or later, *and* you'll be using this partition for a bootable duplicate, *and* you intend to encrypt the duplicate with FileVault (see [Encryption](#)), *and* you might want to be able to boot a newer Mac containing a T2 chip with it ([see full list here](#)), choose APFS (not APFS Encrypted).
 - ▶ Otherwise (and especially if you'll be using this partition for Time Machine), leave it set to Mac OS Extended (Journaled)—or, in El Capitan, OS X Extended (Journaled).

Note: If you're running High Sierra or later and you aren't reading this book linearly, you may be wondering why I don't tell you always to choose APFS as the format. See [APFS Evolves in Mojave](#) for details. (If Apple eventually supports APFS for Time Machine disks and performance improves, I'll be only too happy to change my advice.)

6. Click Erase. If you want your disk to have a single partition, you're done; skip the remaining steps.

7. To add a partition, leave the drive selected on the left and click Partition. A dialog (**Figure 4**) appears with a pie chart showing a single partition on the disk (and, sometimes, an extra, tiny “uninitialized disk” that you don’t have to worry about at all—trust me).

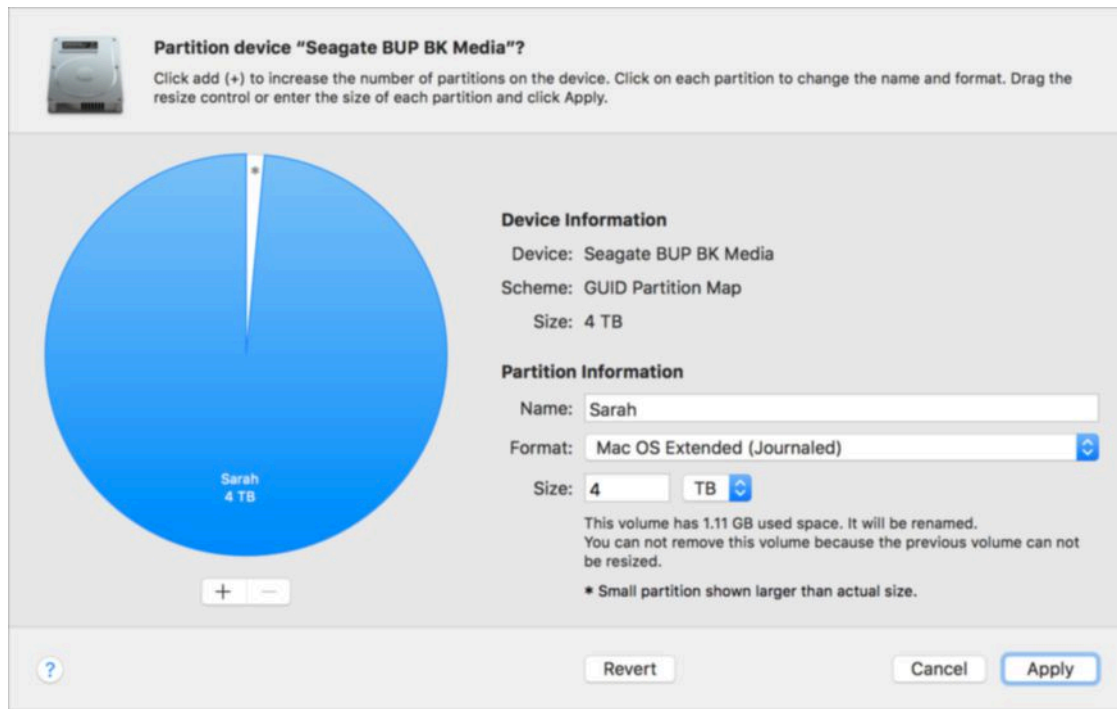



Figure 4: Here’s where you partition a disk in El Capitan or later.

8. Click the plus  button to add a partition (**Figure 5**). Type a name for the second partition and follow step 5 again to choose the format. If necessary, adjust the size by dragging the handle on the pie chart or by typing a new number in the Size field. Repeat this step as desired to add more partitions.

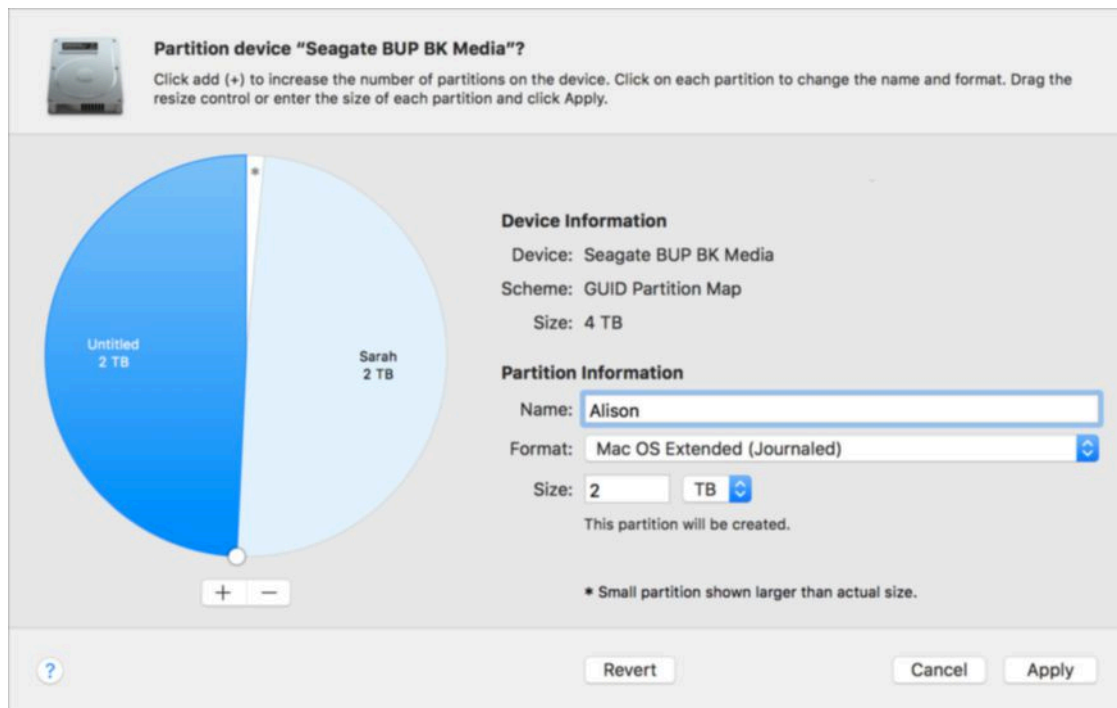


Figure 5: Configure a secondary partition like so.

9. Click Apply.

Disk Utility partitions your disk and applies the correct format to each partition. If you have more than one external drive, repeat all these steps for each one.

At this point, you may see a dialog like the one in **Figure 6**. (If the disk has more than one volume, the dialog also shows a pop-up menu that enables you to choose one of them.) If you've decided to use your new volume for Time Machine, feel free to select it and click Use as Backup Disk now. Or click Decide Later and wait until you've read [Configure and Use Time Machine](#) for details.



Figure 6: If you see this, you can turn on Time Machine with one click.

You're now ready to use your drive(s) for bootable duplicates, Time Machine, or other versioned backups, as discussed in the next few chapters.

APFS Bootable Duplicates on HFS Plus Volumes

I want to make this quite clear, because I've received enough email about it to know that there's considerable confusion: you *can* create a bootable duplicate of an APFS startup volume onto a disk formatted as HFS Plus, and your Mac will happily boot from such a volume—even under Mojave. Although the Mojave installer insists on converting your boot drive to APFS, a Mojave system cloned onto an HFS Plus drive will still boot and run correctly. There's just one exception: on Macs with T2 chips, *encrypted* HFS Plus volumes are not bootable (see [T2 Chips Change the Backup Rules](#)).

Configure a Drive in Yosemite or Earlier

Follow these steps:

1. If Disk Utility isn't already running, open it now (it's located in [/Applications/Utilities](#)).
2. In the list on the left, select your external drive.
3. On the Partition pane, choose the number of partitions you want to have from the Partition Layout pop-up menu. (Don't leave it set to Current, even if you plan to keep the same number of partitions.)

4. Initially, the partitions will be sized equally. If you want them to be differently sized, drag the divider bar between them to resize them.
5. Click Options. In the dialog that appears, select the scheme you want to use (most likely GUID Partition Table) and click OK.
6. Click inside the first partition (initially named Untitled 1) to select it. Enter a name (which you can change later); be sure to use a name that's different from your usual startup disk. From the Format pop-up menu, choose Mac OS Extended (Journaled).

Don't worry about any of the other formats in that menu. The best all-around choice, for all but a handful of computer geeks who want to do something unusual or risky, is Mac OS Extended (Journaled). (Remember, Mac OS Extended is also known as HFS+.) Mac OS Extended (Case-sensitive, Journaled) will also work for Time Machine backups, but isn't a good choice for bootable duplicates because some apps work unpredictably with a case-sensitive file system. Note that unlike the partition map scheme, which affects the whole drive, the format (or file system)—that is, the manner in which files are stored on disk—can vary from one individual partition to another. Therefore you must be sure to select a format for each partition on your disk.

7. Repeat step 6 for each partition.
8. Click Apply, and in the confirmation dialog that appears, click Partition.

Disk Utility sets the partition map scheme, partitions your disk, and applies the correct format to each partition. If you have more than one external drive, repeat all these steps for each one.

If you see an alert asking whether you want to use the new volume for Time Machine and you're not sure you want to do so, click Decide Later; you can set that up later in [Configure and Use Time Machine](#).

You're now ready to use your drive(s) for bootable duplicates, Time Machine, or other versioned backups, as discussed in the following few chapters.

Configure and Use Time Machine

If you’ve decided to use Time Machine for versioned backups, read this chapter to learn everything you need to know about using it. (If you’ve chosen other software for versioned backups, skip ahead to [Use Other Versioned Backup Software](#).)

Apple says it takes just one click to set up Time Machine; while that may be true in rare cases, it’s usually a bit more involved. This chapter walks you through the details of setting up Time Machine, backing up and restoring files, and other activities.

As I explained in [Decide If Time Machine Is Best for You](#), my enthusiasm for Time Machine is not what it once was. I still use it, but not as my only form of versioned backups, and not on all my Macs. Therefore, even though this chapter is fairly long, I make no attempt to be comprehensive here, especially when it comes to troubleshooting.

Time Machine Basics

Time Machine has three visible components:


- A preference pane in System Preferences (**Figure 7**).
- An app found in the Applications folder, in Launchpad, and, optionally, in the Dock (**Figure 8**).
- A Time Machine  menu in the main menu bar. (You can enable or disable this menu with the “Show Time Machine in menu bar” checkbox on the Time Machine preference pane.)



Figure 7: Specify backup drives and ignored volumes on the Time Machine preference pane. (This figure is from High Sierra; Yosemite and earlier have a somewhat different appearance.)



Figure 8: The Time Machine icon in the Dock. You can add it by dragging the icon from your Applications folder to the Dock. (It was there by default in older installations of macOS.)

Choose a Destination

Assuming you've followed the steps in the previous chapter, you already have a hard drive formatted and ready to go; this could be a standalone device connected to your Mac, a NAS, a Time Capsule, or a drive attached to another Mac on your network. (If you're planning to use another Mac as a Time Machine server and you haven't set that up yet, you should do so first—see [Use a Mac as a Time Machine Server](#)—

and then come back to this topic.) In any case, the next step is to tell Time Machine which destination(s) to use:

1. Open System Preferences > Time Machine.
2. Click Select Backup Disk.

A dialog appears (**Figure 9**), listing all volumes eligible to be a destination disk and the amount of free space on each local disk.

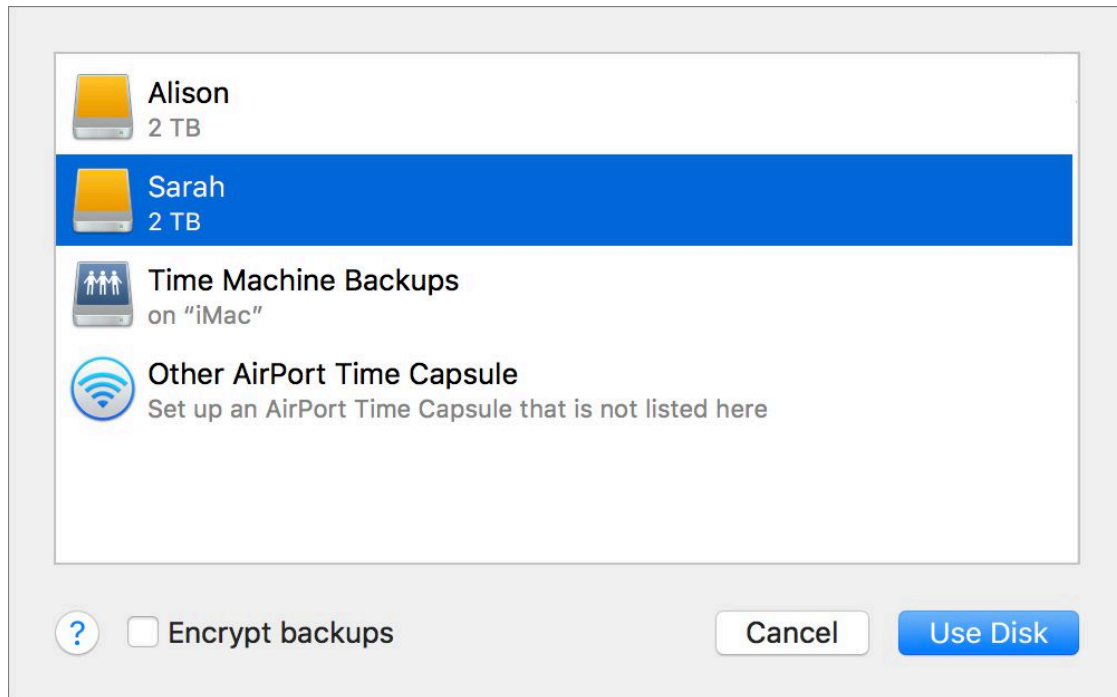


Figure 9: Available local and network volumes appear in this dialog; select the one you want to use and click Use Disk.


3. Select a volume and click Use Disk. (If you're using a Time Capsule for the very first time, select Other AirPort Time Capsule and follow the instructions to set it up.)

Note: Curious about that "Encrypt backups" checkbox? I tell you about it in [Encrypt Your Time Machine Backup](#).

4. You can optionally select more than one destination. If you do, Time Machine alternates destinations with each hourly run. To select another destination, click Select Disk, select another disk, and click Use Disk. You'll be prompted to choose whether you want to replace the previous backup disk or back up to both disks. Click Use Both.

(To add still more destinations, scroll down in the list of destinations and click Add or Remove Backup Disk. If you select more than two destination disks, you won't be asked again whether you want to replace the existing destination.)

On the Time Machine preference pane, the Back Up Automatically checkbox is selected (in El Capitan and earlier, the master switch moves from Off to On), and a timer begins a two-minute countdown before your first backup begins. (You may prefer to turn it off until you've excluded files from Time Machine, which I discuss next.)

Your only visible indication that Time Machine is currently backing up files is a subtle change to the Time Machine  menu—a little triangle appears at the bottom of the icon—but you can click the icon to display more information about current progress in the menu.

During each of Time Machine's hourly runs, it backs up only the files that have changed since its previous run (except files you've excluded, as I discuss next). If an app stores its data as a *package* (that is, a folder that looks like a file in the Finder), Time Machine backs up only changed items *within* the package. (Among many other apps, Keynote, GarageBand, and DEVONthink use packages for their data.)

Note: If you're using a Drobo Gen 3 device as a destination, read Drobo's support article [Using Drobo with Time Machine or backup software](#) for important details.

Exclude Files from Time Machine


By default, Time Machine backs up all the files on your startup disk as well as any other locally connected volumes, which is usually exactly what you want. However, in a few situations you may want to exclude certain items from being backed up.

One obvious reason is a lack of space: if you have too much data on your main disk(s) to fit comfortably on your backup destination, something has to go. Out of concern for privacy or security, you may

prefer to leave certain sensitive files out of your backups. Another big reason is performance: some files are so large and change so frequently that they keep Time Machine busy doing virtually continuous backups. Yet another reason: if you have a drive attached that contains a bootable duplicate, you don't want Time Machine to back that up too! Read [Items to Consider Excluding](#), shortly ahead, for advice about what Time Machine should not back up.

How to Exclude Items

To make sure an item doesn't get backed up:

1. Open System Preferences > Time Machine and click Options.
2. In the dialog that appears, click the plus  button, navigate to the item you want to exclude, select it, and click Exclude. (To find files that are normally invisible, check "Show invisible items.") Alternatively, you can drag any item (a file, folder, or volume) from the Finder into the "Exclude these items from backups" list. When you're finished, click Save.

Unfortunately, Time Machine offers no way to automatically exclude files that meet certain criteria, regardless of their location—for example, all files over 2 GB or all disk images. The only way to automatically exclude a set of files whose members may change over time is to exclude the folder that contains them. However, see the sidebar [Using Smart Folders for Exclusions](#), just after these steps.

3. If the item has *already* been backed up and you want to remove it from your backup disk (for example, because it's quite large and you want the disk space for other files), follow the instructions ahead, in [Delete Files from a Time Machine Backup](#).
4. If you had previously turned Time Machine off, click On now.

If you use multiple destination disks for Time Machine, bear in mind that whatever you exclude from Time Machine will be omitted from *all* Time Machine backup disks.

Tip: If you exclude an item from Time Machine in this way and then move that item in the Finder, Time Machine won't realize it's the same item and will start backing it up! But there's a way to make exclusions "sticky" such that they follow items even if you relocate them. See Kirk McElhearn's explanation at [Mac OS X Hints](#).

Using Smart Folders for Exclusions

Having trouble locating files you want to exclude? Using the Finder's Smart Folder feature, you can create a saved search for files that meet certain criteria (such as "size is greater than 2 GB"). In Time Machine's Options window, you can then locate that smart folder and select its contents (hold down the Shift key to select multiple files at once) to add them to the Exclude These Items from Backups list. (Don't add the smart folder itself, because that excludes only the tiny file representing the saved search.) From time to time, be sure to repeat this procedure, as the smart folder's contents may change and the list of excluded files won't update itself dynamically.

Items to Consider Excluding

If you're using *only* Time Machine for backups—and in particular if you don't also have a bootable duplicate—then you shouldn't exclude anything, because Time Machine can only restore what it backed up.

However, assuming you do have a bootable duplicate, you can save space and improve Time Machine's performance by excluding certain items, such as these:

- **Virtual machine disk images:** Apps that let you run Windows (or other operating systems) on your Mac typically store your entire virtual machine installation in a special disk image file. These files can reach tens of gigabytes, and since they change every time you run the virtual machine, Time Machine attempts to back them up with each run, bogging down your Mac and wasting space on your backup disk. I suggest excluding them from Time Machine and backing them up separately—except note the following:

- ▶ Parallels Desktop lets you disable Time Machine backups for all your virtual machines without using the Time Machine preference pane. (With a virtual machine running, go to Actions > Configure > Backup and select “Do not back up with Time Machine.”) Alternatively, you can select SmartGuard in the same window to enable automatic snapshots, which reduce the amount of data a backup app must copy on each run; you can make Time Machine even more efficient when backing up these snapshots, by clicking Details and then selecting Optimize for Time Machine.
- ▶ VMware Fusion by default stores disk images in `~/Documents/Virtual Machines`, with the extension `.vmwarevm`. Technically, the file with the `.vmwarevm` extension is a package (again, a special folder that looks and acts like a file); the actual disk image file inside the package has an extension of `.vmdk`. But it’s easiest to exclude the entire `.vmwarevm` file.
- ▶ VirtualBox keeps its disk images in `~/Library/VirtualBox/VDI` with an extension of `.vdi`.

Note: The tilde (~) in the paths above refers to your home folder—that is, `/Users/your_name`. The user Library folder (`~/Library`) is hidden by default, but you can open it by Option-clicking the Finder’s Go menu and choosing Library

- **Certain other large disk images:** Disk images (typically with the extension `.dmg` or `.sparseimage`) serve many useful purposes, such as providing a convenient way to package and distribute downloadable software. You can also create your own disk image using Disk Utility, optionally encrypting it so that all the files within are protected with a password. However, most disk images that you may have created yourself, for whatever reason, have the same defect as virtual machine disk images: every time any file inside changes, the whole file changes, forcing Time Machine to back up the entire image again. That’s not a big deal if the image is small, but if it’s in the range of hundreds of megabytes or larger, it will cause problems with Time Machine.

So, you might want to add such files to the Exclude These Items from Backups list and back them up in a different way (at the very least, as part of your bootable duplicate)—but see the sidebar [\(Sparse\) Bundles of Joy](#), shortly ahead, for a potential way to have your cake and eat it too.

- **TechTool Pro’s directory backups:** A popular disk utility called TechTool Pro can optionally store backups of your disk’s directory to help you recover from disk errors. But these files can be *quite* large, and because they change all the time, Time Machine shouldn’t back them up. They’re located in `~/Library/Application Support/TechTool Pro 8` (for TechTool Pro 8) or `~/Library/Application Support/TechTool Protection` (for TechTool Pro 9 or later); if you use TechTool Pro, I suggest excluding that entire folder from Time Machine.

Beyond the items just listed, you might in some cases want to think about whether to exclude the following:

- **System files:** The files that make up macOS—the contents of your `/System` and `/Library` folders, various invisible files and folders at the main level of your disk, and the apps included with macOS, such as Mail and Safari—are all included by default in a Time Machine backup. That’s a good thing, as it enables Time Machine to restore your whole system, or any part of it. However, if you’re running out of space on your backup disk and you already have a bootable duplicate or two (see [Create and Use a Bootable Duplicate](#)), you could exclude the system files to save space. You may especially want to do this if you’re backing up several Macs over a network, because those additional files can chew up a lot of disk space and network bandwidth.

To exclude system files, add the folder `/System` to the Exclude These Items from Backups list. The alert shown in **Figure 10** appears; click Exclude All System Files.

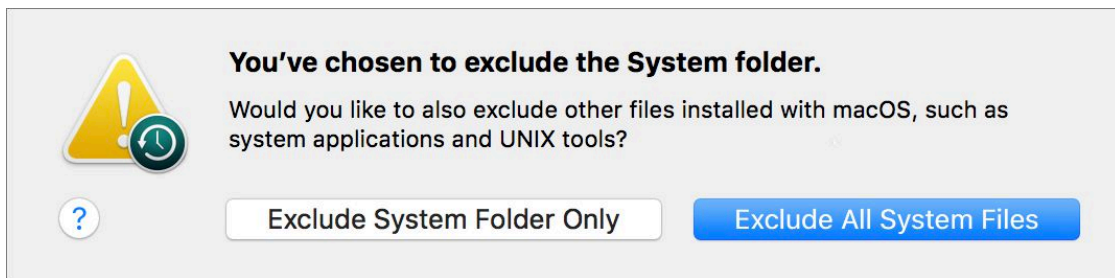


Figure 10: When you tell Time Machine to exclude your System folder, this alert asks if you want to exclude all of macOS.

- **Other local volumes:** Time Machine doesn't back up other *network* volumes mounted on your Mac. However, it normally does back up other local volumes, including external USB and Thunderbolt drives and additional internal drives. If the data on any of these volumes isn't particularly valuable—I'm thinking, for example, of disks mainly used as scratch space for Photoshop—you can save a significant amount of space on your backup disk by adding them to the Exclude These Items from Backups list. In addition, if the drive containing your bootable duplicate is connected to your Mac, you should tell Time Machine to avoid backing up that volume; it already *is* a backup, so backing it up again wouldn't be particularly helpful, and it would massively increase the amount of storage space and time that Time Machine needs.
- **Downloads:** Your `~/Downloads` folder may contain a number of large files that disappear quickly (because you delete them after you install software or relocate the files to other folders). If so, exclude that folder.
- **Video:** If you download movies or TV shows regularly and then delete them right after you watch them, you can save tons of space on your backup drive by excluding the folder containing these files (typically `~/Music/iTunes/iTunes Media/Movies` and `~/Music/iTunes/iTunes Media/TV Shows`). But do this *only* if you're sure you can download the movies again if necessary. (Movies and TV shows purchased from the iTunes Store, for example, can be downloaded again for free as long as they're still in Apple's catalog.)

(Sparse) Bundles of Joy

macOS has long supported several disk image varieties, one of which is the *sparse image* (extension `.sparseimage`). Unlike conventional disk images with a `.dmg` extension, sparse images don't have a fixed size; they can grow (up to a preset maximum size) as their contents change. This helps avoid wasting space on your disk.

One type of disk image, the *sparse bundle* (which has the extension `.sparsebundle`), looks and behaves almost exactly like a sparse image, but with an interesting twist: behind the scenes, this image is a bundle (hence the name) of smaller files called *bands*, each only 8 MB in size. As a result, when you modify files in a sparse bundle image, only the band(s) used to store that particular data change—and only those, much smaller, files need to be backed up when Time Machine next runs.

Like sparse images, sparse bundles can be encrypted. To create an encrypted sparse bundle:

1. In Disk Utility, choose File > New Image > Blank Image (or, in Yosemite or earlier, File > New > Blank Disk Image).
2. Fill in the filename, and choose a location, volume name, and maximum size; leave the format as Mac OS Extended (Journaled).
3. Choose either 128-bit or 256-bit AES encryption from the Encryption pop-up menu. Leave Partitions set as it is.
4. From the Image Format pop-up menu, choose “sparse bundle disk image.”
5. Click Save (or Create, in Yosemite or earlier). Enter and verify a password and click OK.

You can then mount the image by double-clicking it in the Finder and entering its password (optionally storing the password in your keychain).

Local Snapshots

Time Machine has an extra feature that's normally invisible: it can save local snapshots of new and changed files in a hidden folder on your startup disk (`/.MobileBackups`) even when your normal Time Machine destination is unavailable.

This feature is designed for users of Mac laptops, who may spend a great deal of time disconnected from the drive, Time Capsule, or server where their Time Machine backups are ordinarily stored. In fact, by default, *only* Mac laptops have this feature enabled. But it creates the illusion that you're always connected to your destination disk; you can even restore files directly from your local snapshots.

Local snapshots require no setup; as long as you have a Mac laptop with Time Machine enabled, local snapshots happen automatically—but just once per day, and only if you have enough free space. Once you connect to your regular Time Machine destination volume again, the local backups are added to it, with the net result being an unbroken series of stored snapshots. Meanwhile, Time Machine purges extra local copies when you start running low on disk space—so you need not worry that local snapshots will be responsible for your running out of room to store your regular files.

In High Sierra and later, Macs with APFS startup volumes save these snapshots *hourly*, and can store more of them in less space; see [Mobile Time Machine and its transformation in High Sierra](#) or, better yet, Jeff Carlson's [Take Control of Your Digital Storage](#) for details.

Although the local snapshot feature is a neat trick and could come in handy on many occasions, don't let it lull you into a false sense of security. Because these snapshots are stored on your startup disk, you can lose them—along with all your other files—in a disk crash or if your Mac is stolen. So be sure to connect to your regular backup disk regularly, just as if local snapshots didn't exist.

If you're dead set against having local snapshots and want to turn them off, open Terminal (in `/Applications/Utilities`) and enter this:

```
sudo tmutil disablelocal
```

Press Return, and enter your administrator password when prompted. To turn them back on—or to enable them on a desktop Mac where they'd be disabled by default—instead enter this:

```
sudo tmutil enablelocal
```

Restore Data with Time Machine

Once you have Time Machine set up and running, it normally does its thing silently in the background, without intruding on your work. (Depending on several variables, such as the speed of your CPU, how your backup volume is connected to your Mac, and how much data you're backing up, Time Machine may in some cases slow down your Mac—and perhaps also your network connection—while it's running.) You can continue ignoring it until you need to restore something—a missing file or folder, or a previous version of a file you still have. This is where Time Machine's unique 3D restoration interface comes in; you should try restoring some files now, whether you need them or not, partly to make sure your backup is working properly—but mostly for the experience of flying back through time!

Tip: With Time Machine as with other backup apps, remember that if you discover data is missing from an app, you should restore the data files—not the app itself! See the sidebar [Restore the Data, Not the App](#) for more details.

Restore Files and Folders in the Finder

If you notice that a file or folder is missing, or that you've accidentally changed it and need an older version, follow these steps to retrieve an item from your Time Machine backup:

1. In the Finder, make sure the window that contains the item you want to restore (or the one that used to contain it, if it's been deleted) is frontmost. You can do this by clicking anywhere in the window. (Not certain where the missing item was stored? Skip ahead to [Restore Files and Folders Using Spotlight](#).)

Note: If you've set up multiple destination disks, Time Machine restores files from the one it used most recently. To use a different disk instead, see [Switch to Another Time Machine Backup](#).

2. Click the Time Machine icon in the Dock or choose Enter Time Machine from the Time Machine ⌚ menu.

The frontmost window moves to the center of the screen, the background blurs, and additional copies of the window recede into the background in a 3D “time warp” display (**Figure 11**). (Prior to Yosemite, the appearance was a bit different, with a swirling, animated outer space background and chunky, stylized buttons.) In this book, I refer to this view as the Time Machine screen.

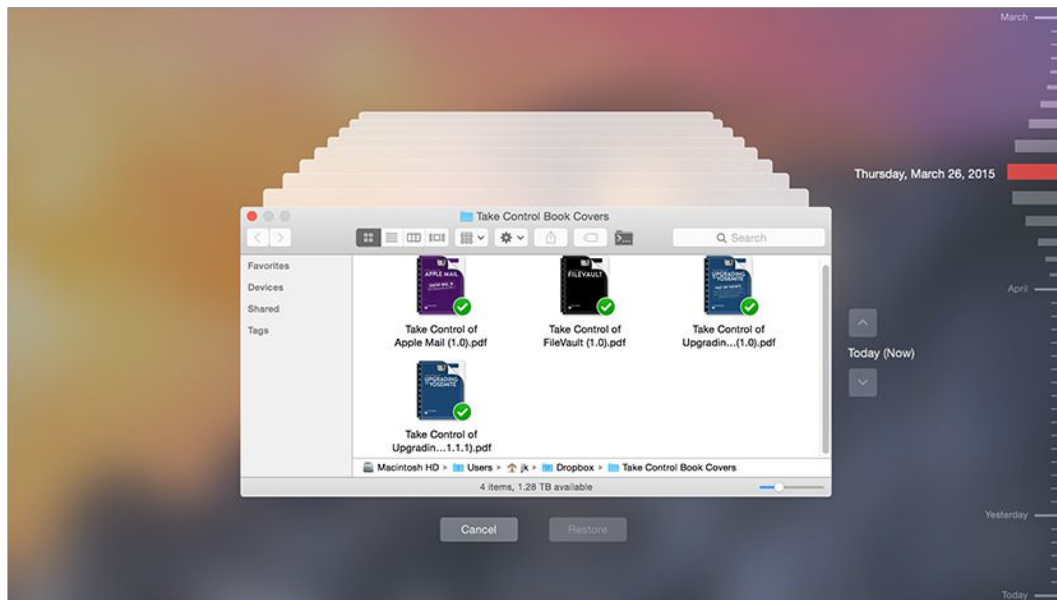



Figure 11: Go “back in time” to a previous version of your data.

3. To locate the file or folder you want, do one of the following:
 - ▶ To the right of the stacked windows (or, in Mavericks, at the bottom of the screen), click the top arrow (for “back in time”). Time Machine zooms back to the most recent backup in which that window’s contents were different. Keep clicking to continue zooming back through previous versions of that window. Click the bottom arrow to move forward in time.
 - ▶ Use the controls along the right edge of the screen to jump to a particular backup. As you hover your pointer over the small horizontal lines, they zoom in to display the date and (for recent backups) time of each backup. Click a line to jump right to that version of the window. (If you’ve only just set up Time Machine,

you won't see many dates here.) As you zoom backward or forward in time, the date and time of the backup you're currently viewing is shown at the right between the arrow buttons (or, in Mavericks, at the bottom of the screen in the middle).

4. If you're unsure whether a file is the one you want, click once to select it and press the Space bar to activate Quick Look, which gives you a live, full-size preview of the file. To close the Quick Look window, click the X  icon in the upper-left corner.

Tip: When navigating on the Time Machine screen, avoid following aliases (whose icons have arrow in their lower-left corner) to files, folders, and volumes. Aliases point to the current versions of files, not backups on your Time Machine volume, so you may end up in the wrong place or with the wrong version of a file.

5. Once you've selected the item you want to restore, decide whether you want to restore it to its original location or somewhere else:
 - ▶ To restore to the original location, click the Restore button. Time Machine immediately restores the selected item, and returns you to the Finder. (Time Machine may prompt you to enter an administrator password for certain items.)

You can use this procedure even if you want to restore an older version of a file but keep the current version. After you click Restore and the Finder reappears, you'll see an alert asking whether you want to replace the existing file, keep both copies (in which case the one already in that location is renamed with "(original)" at the end), or keep the original (thus canceling the restoration).

- ▶ To restore to a different location from the original, right-click (or Control-click) the item and choose "Restore *filename* to" from the contextual menu, navigate to the desired destination, and click Choose.

If you decide against restoring any files, instead click the Cancel button or press Esc (Escape).

Note: Time Machine cannot back up files from network servers, so the icons for those volumes are dimmed.

Restoring Photos Data Using Time Machine


Although iPhoto once enabled you to restore individual photos from a Time Machine backup, that's not the case with Photos. Assuming you've backed up your Photos Library along with the rest of your data, you can restore the *whole* library if need be—but that's your only option. For details, see Apple's article [Restore a library from Time Machine in Photos on a Mac](#).

Restore Files and Folders Using Spotlight

Although you can, on the Time Machine screen, navigate around your Mac manually, you could spend a lot of time searching for a file at different times in different locations on your disk if you don't know where it is. No worries: Spotlight to the rescue!

Note: Remember, if you've set up multiple Time Machine destination disks, Time Machine restores files from the one it used most recently. To use a different disk, see [Switch to Another Time Machine Backup](#).

If you know something about a missing file or folder, such as a word in its title or its contents, you can use Spotlight to find it within your Time Machine backups. Follow these steps:

1. Click the Time Machine icon in the Dock or choose Enter Time Machine from the Time Machine  menu. The Time Machine screen appears.
2. Type something in the Spotlight search field in the toolbar of the window, optionally specifying additional search criteria.

Note: Although Spotlight searches in the Finder normally include items such as messages in Mail and contacts in Contacts, these do not appear by default when you do a Spotlight search on the Time Machine screen.

3. Using the back and forward arrows or the controls on the right of the screen, navigate to an earlier point in time. Each time you move to another backup, the Spotlight window changes to reflect the results of the search at the time that backup was performed.
4. When you find the desired file, select it and click Restore. Time Machine copies it to its original location. To restore to a different location, right-click (or Control-click) the item and choose “Restore ‘*filename*’ to” from the contextual menu, navigate to the new location, and click Choose.

Time Machine and Spotlight

Spotlight always maintains an index of your Time Machine disk so you can search in your backups. You may be tempted to prevent Spotlight from indexing that disk by adding it to the Privacy list in System Preferences > Spotlight, but don’t bother. It doesn’t work; Spotlight keeps indexing your Time Machine disk even if it’s on the list. But this is nothing to worry about, because Spotlight searches don’t normally display matching items on your Time Machine disk except when you’re on the Time Machine screen.

Restore Data Within Apps


When Time Machine was first introduced, Apple made a big deal about how it could restore not only entire files in the Finder but also individual items within apps, such as pictures in iPhoto, contacts in Address Book (later renamed Contacts), and messages in Mail. GarageBand 4 through 6 (a.k.a. GarageBand ’08 through GarageBand ’11) could also restore projects from within the app using Time Machine. But Apple dropped in-app Time Machine support from GarageBand 10 and iPhoto ’11 (version 9.2 and later), and never included it in Photos (which replaces iPhoto). Thus, as far as I know, Contacts and Mail are now the *only* apps with built-in Time Machine support.

Note: macOS’s Versions feature, which is superficially similar to Time Machine—and indeed, uses the very same 3D interface—*does* let you restore multiple versions of files from within many other apps. I say more about it in [Version Control](#).

Note: If you've set up multiple Time Machine destination disks, Time Machine restores data from the one it used most recently. To use a different disk, see [Switch to Another Time Machine Backup](#).

Restore Within Contacts


To restore one or more contacts in Contacts:

1. In Contacts, switch to any view in which the contact you're looking for should appear—for example, a search for that contact name.
2. Click the Time Machine icon in the Dock or choose Enter Time Machine from the Time Machine  menu. Contacts becomes the center of the Time Machine screen.
3. Using the arrow buttons, or the navigation controls on the right side of the screen, browse your backups until you find one in which the desired contact(s) appears.
4. Select one or more contacts and click Restore.

Unfortunately, restoring contacts with Time Machine doesn't restore *groups*. In addition, contacts restored from a Time Machine backup can, in some cases, later be overwritten by iCloud, which may think its version of the data is more recent. I know of no other way to restore individual entries from Contacts, but if you use iCloud to sync your contacts, you can restore *all* your contacts from an earlier version of iCloud's archive. To do this, log in to your [iCloud](#) account in a web browser, click Settings, click Restore Contacts (at the bottom, under Advanced), and follow the instructions.

Restore Within Mail

To restore one or more mailboxes or messages in Mail:

1. With Mail in the foreground, click the Time Machine icon in the Dock or choose Enter Time Machine from the Time Machine  menu. Mail becomes the center of the Time Machine screen.
2. Navigate to a mailbox you want to restore, or a mailbox in which a message you're looking for should appear. (You can't select smart mailboxes, unfortunately.)

3. Using the arrow buttons, or the navigation controls on the right side of the screen, browse your backups until you find one in which the desired mailbox(es) or message(s) appears.
4. Select one or more mailboxes or messages and click Restore.

When restoring messages, Mail creates a new local mailbox (in the On My Mac section of the sidebar), and inside that, a second mailbox called Recovered Messages; the restored items are put in this mailbox. From there, you can drag them to another location. (Restored mailboxes are put directly in the On My Mac section of the sidebar.) If you later restore more messages in Mail without first deleting the Recovered Messages mailbox, Mail creates yet another mailbox, Recovered Messages 1—incrementing the number each time. (Not the most intuitive system, eh?)

Switch to Another Time Machine Backup

If you're backing up just one Mac to just one Time Machine disk, you can skip this section. But if you're backing up multiple Macs, or backing up to more than one destination disk, you may need a way to tell Time Machine to show you a different set of backups from the one you're currently using, in order to restore (or delete) items from it. (You might also need to use this procedure to see backups from your existing Mac if you've recently restored your entire disk from a Time Machine backup, if you've changed its name in System Preferences > Sharing, or if your logic board has been replaced.)

To browse other Time Machine backups:

1. Make sure the volume with the backups you want to view is mounted in the Finder.
2. Right-click (or Control-click) the Time Machine icon in the Dock and choose Browse Other Time Machine Disks from the contextual menu, or Option-click the Time Machine icon in your menu bar and choose Browse Other Backup Disks from the contextual menu.
3. In the window that appears, select the backup you want to use and click Use Selected Disk. The Time Machine screen appears.

You can now recover or delete items in the usual way.

Restore a Disk Using Time Machine

If you've experienced a major disk crash or other catastrophe that requires you to restore an entire disk rather than merely individual files or folders, you can do so with Time Machine, by way of macOS Recovery (assuming you let Time Machine back up your system files):

1. Make sure the drive containing your Time Machine backup is attached to your Mac:
 - ▶ If you normally back up to a drive connected to another Mac, I suggest disconnecting the drive from that computer and plugging it directly into the Mac you want to restore.
 - ▶ If you back up to a NAS or Time Capsule, I suggest connecting to it with an Ethernet cable (if your Mac has an Ethernet port or adapter) rather than using Wi-Fi, as that will speed up the restoration. In addition, anecdotal evidence suggests that you'll get better performance if, after connecting the Ethernet cable, you turn off your Mac's Wi-Fi for the duration of the process.
2. Restart your Mac, holding down \mathbb{R} until the gray Apple logo appears. A few moments later, a macOS Utilities window should appear.
3. Select Restore from Time Machine Backup and click Continue. Read the instructions, then click Continue again.
4. Select your Time Machine backup disk. If the disk was encrypted, enter its password when prompted. (If you selected a Time Capsule or other network destination, click Connect. You may be prompted to enter its Disk password; do so, and click Connect again. Then select the volume you want to restore.) Click Continue once more.
5. If the Time Machine disk contains backups for more than one volume, select the one you want from the Restore From pop-up menu. Then select the particular backup you want to restore—likely the most recent one (the first one in the list). Click Continue.

6. On the Select a Destination screen, select your internal disk. Click Restore. If prompted, confirm that you want to restore your data.

Time Machine restores your data. When it finishes, follow the instructions to restart your Mac.

Note: When setting up a new Mac or installing macOS on a blank disk, Setup Assistant gives you the option to restore files from a Time Machine backup. You can also do this after the fact by running the Migration Assistant utility.

Restarting Time Machine Backups After a Restore

Once you've restarted after restoring your entire disk, Time Machine will start over from scratch with a new, full backup, essentially ignoring all your previous backups. Apple [claims this is "normal" behavior](#), though it may not be what you expect or want. (If you use Setup Assistant or Migration Assistant to restore a Time Machine backup to a new Mac, you can avoid this problem and continue with your existing Time Machine disk by clicking Inherit Backup History when prompted.)

If it *is* what you want—that is, to keep your new backups separate from your old ones—then let Time Machine proceed on its own (or, if using Setup Assistant or Migration Assistant, click Create New Backup when prompted); if you want to see your previous backups from before the restoration, follow the procedure in [Switch to Another Time Machine Backup](#).

If, however, you want your restored system to continue using your existing Time Machine backups, you can use a special procedure to reconnect them—but (fair warning) it requires a lot of fiddling on the command line in Terminal. You can read about the process in the article [Inherit TimeMachine Backups](#) by Johannes Neubauer; note that in every command that includes a string starting with `$` (such as `$path_to_sparsebundle`), you'll need to replace that string with the path, identifier, or other item it describes.

Restore Files Without Time Machine

If you ever need to restore files and Time Machine isn't working for some reason, you can browse the contents of your Time Machine disk in the Finder and then drag any file to your desktop (or another folder) to copy it to your main disk. (You should always avoid opening files directly on your backup disk.) But be aware that Time Machine stores files on your backup disk in two different ways:

- When you connect a drive directly, Time Machine stores backups for your computer in a folder like this:

[volume_name/Backups.backupdb/computer_name](#)

Inside that folder, you'll find a date- and time-stamped folder for each individual backup Time Machine is currently storing. (There's also an alias named Latest that, when opened, shows you the latest backup.)

- By contrast, when Time Machine backs up a Mac over a network, it puts a sparse bundle disk image at the top level of the volume whose name is similar to your computer's name, as in:

[volume_name/MacBook_Pro.sparseimage](#)

If you double-click that disk image to mount it in the Finder, you'll see the list of folders with each stored Time Machine backup.

The Magic of Hard Links

If you look in the folder or disk image on your Time Machine backup disk, you'll see subfolders corresponding to each hourly, daily, and weekly backup. Inside each of those subfolders you'll find what appears to be the entire contents of your drive, yet the total space occupied on your backup disk (which you can check using the Finder's File > Get Info command) may be only a bit larger than the space occupied on the disk you're backing up. At first glance, this suggests a paradox: those files should take up much more space!

Time Machine accomplishes this nifty trick using a Unix mechanism called *hard links*. (Mac Backup Guru and Personal Backup also use hard links.) Hard links are basically pointers to files or folders, and those pointers take up just a tiny bit of space. You may be thinking this sounds like aliases, but in fact they act differently. With an alias (or its Unix relative, the *symbolic link*), if you copy the alias, you get only a copy of the alias—not of the original file; if you delete the original file, the alias no longer functions. By contrast, a hard link behaves in almost every respect like a separate instance of the original file: copy a hard link and you get the whole file; delete any instance—the original file, or the hard link—and all other instances remain.

How does this sleight of hand work? Technically, every file on your computer is already referenced by a hard link; what's neat is that files can have more than one hard link, so altering one doesn't affect the others. (To learn more, consult [Wikipedia](#).) After Time Machine runs the first time (during which it copies all your files), it simply creates a new hard link to the previous version of any folder or file that didn't change at all since the last run.

Unfortunately, as of publication time, APFS supports hard links only for files, not for folders. And that's the reason (or at least a big part of the reason) that Time Machine can't currently use an APFS-formatted disk as a destination—though it can certainly back up an APFS volume to an HFS Plus-formatted destination.

Delete Files from a Time Machine Backup

When your backup volume gets close to being full, Time Machine automatically deletes old backups to make space for new ones. It doesn't warn you about this, but the first time it happens—and optionally thereafter—Time Machine does inform you that it has just deleted some backups, suggesting that you select a different disk to avoid having more files deleted. (If, instead, you'd like to migrate your Time Machine backups to a larger volume, see [Migrate to a Larger Time Machine Disk](#), later.) Be that as it may, these automated deletions may not occur in the way you expect; I lay out the details in [The Time Machine Schedule Problem](#), ahead.



Sometimes you may need to remove files from Time Machine's backup before they would automatically be deleted. For example:

- A large file you've already deleted and will never need again (say, a gigantic disk image for a software installer) has been backed up—perhaps multiple times.
- You're concerned about sensitive information being stored in a backup that other people might be able to access.
- You decide to exclude a file from Time Machine (see [Exclude Files from Time Machine](#)) after Time Machine has already backed it up, and you want to remove the backed-up versions.

Contrary to what the user interface implies, Time Machine doesn't let you purge just one instance of a particular file from your backups. You have two choices: delete *a single entire snapshot* (that is, all the files from a particular hourly run of Time Machine) or delete *all instances of a single file from a certain location*, regardless of how many times that file was backed up.

Delete an Entire Snapshot

To delete all the files Time Machine backed up during a particular hourly run, follow these steps:


1. Click the Time Machine Dock icon or choose Enter Time Machine from the Time Machine  menu to show the Time Machine screen.
2. Using the arrow buttons or the timeline control on the side of the screen, navigate to the snapshot you want to delete. Note that if it occurred within the last day, you'll delete just that hourly run; if it occurred earlier, you'll delete the only remaining backup for a particular day or week. You can verify which backup you'll be deleting by looking at the large bar at the bottom of the window.
3. From the pop-up Action  menu, choose Delete Backup. (It doesn't matter whether you have any file or folder selected.)


Time Machine removes that entire snapshot from its backup. (You may be prompted to enter an administrator password first.)

Note: If you use multiple Time Machine disks, deleting a snapshot from one doesn't affect the other backup disks. Follow the procedure in [Switch to Another Time Machine Backup](#) to select a different disk, and then repeat these steps to delete snapshots from it.

Delete All Instances of a Single File

To delete every backed-up copy of a given file from your Time Machine backup, follow these steps:

1. In the Finder, navigate to the folder that contains (or once contained) any version of the file you want to delete; if you're unsure where it is (or was), do a Spotlight search.
2. Click the Time Machine Dock icon or choose Enter Time Machine from the Time Machine  menu to show the Time Machine screen.

3. Using the arrow buttons or the timeline control on the side of the screen, navigate to any previous version of the folder that contains the file you want to delete. Click the file once to select it.
4. From the pop-up Action  menu, choose Delete All Backups of “filename”. (You can also right-click or Control-click the item and choose Delete All Backups of “filename” from the contextual menu.)
5. Click Done (or Cancel) to exit the Time Machine screen.

Time Machine removes from its backup every copy of that file, in that location, that it ever backed up. (For some files, you may be prompted to enter an administrator password first.)

Note: If you use multiple Time Machine disks, deleting all instances of a file from one doesn’t affect the other backup disks. Follow the procedure in [Switch to Another Time Machine Backup](#) to select a different disk, and then repeat these steps to delete files from it.

Encrypt Your Time Machine Backup

Using the same underlying mechanism as FileVault, Time Machine can encrypt local Time Machine backup disks, Time Capsule backups, and most other network backups. Once you’ve enabled encryption, if an unauthorized person were to get access to your backup disk, they’d be unable to read any of your files without your password.

Warning! Do not turn on encryption if you use a *networked* Drobo device as a destination for Time Machine, as it may cause serious damage. Certain direct-connect Drobo models do support Time Machine encryption, but only on dedicated backup volumes; see the article [Backup Volume: Encryption](#) for details.

Turning on encryption is a piece of cake:

1. Open System Preferences > Time Machine and click Select Disk.

2. With your destination volume already selected, check “Encrypt backups” (see **Figure 12**). Then click Use Disk.

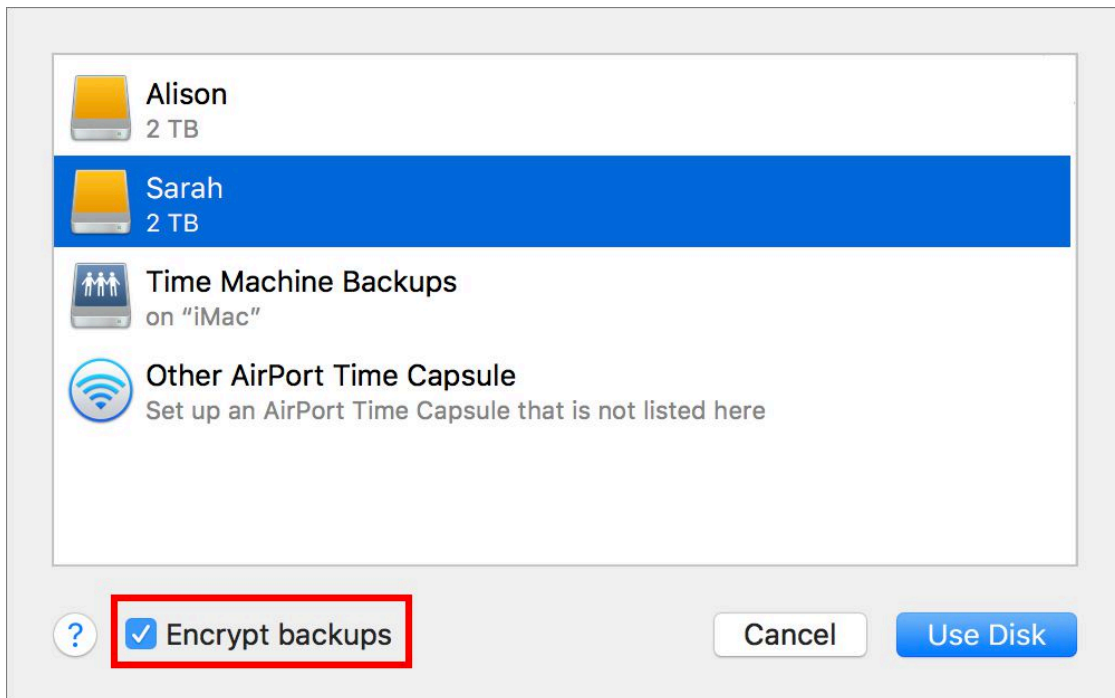


Figure 12: To encrypt a Time Machine backup, you need only check this box and then enter a password and a hint.

3. In the dialog that appears (**Figure 13**), enter and verify a password for your Time Machine backups, enter a hint (keeping it vague to thwart guessing by others) and click Encrypt Disk.

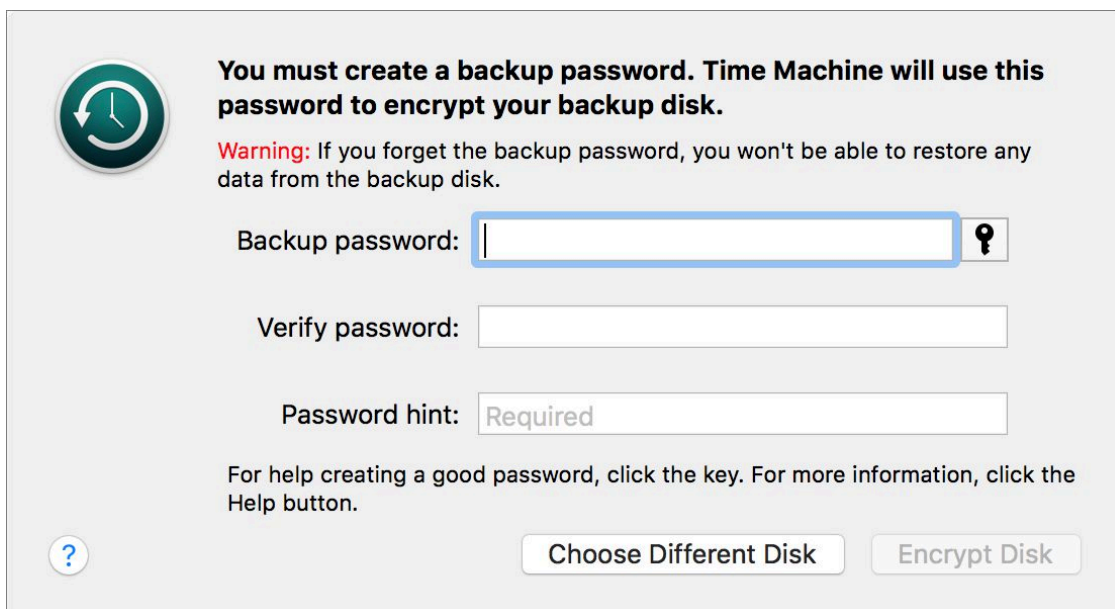



Figure 13: Set your encryption password here.

Encryption may take some time (progress is shown in the Time Machine  menu), but you can continue to back up and restore data with Time Machine while it's happening.

Note: Keep in mind that this encryption affects the entire volume (disk or partition) containing your Time Machine backups.

Tip: If you've already set up Time Machine without encryption and want to switch to an encrypted backup, Apple recommends that you remove your backup disk and reselect it with Encrypt Backups checked.

Increase Time Machine's Performance

According to the article [Massively speed up Time Machine backups](#) by Keir Thomas at Mac Kung Fu, you can use Terminal to enter an obscure command that prevents Time Machine from reducing its priority in the background, thus making it run much faster. (The article details a separate procedure to ensure that this change survives a restart.)

I tried this tip myself and found that it did indeed make Time Machine much zippier. Some of the article's comments suggest there could be undesirable side effects (like other processes besides Time Machine running at high priority), but the change is easy enough to undo if you discover problems after running it.

Use a Mac as a Time Machine Server

If you plan to hook up your external drive(s) directly to each Mac, or if you use a NAS or Time Capsule, there's nothing to see here; skip ahead to [Use a Single Backup Disk with Multiple Macs](#). But if you'd like a Mac on your network to function as a Time Machine server for the rest of your Macs, read on.

It has long been possible to use Time Machine to back up one or more Macs over a network to another Mac that's sharing a folder in just the right way. However, "possible" does not mean it's easy, convenient, or

reliable, and in the past the process was none of these—*unless* that other Mac happened to be running a copy of Apple’s macOS Server software. But starting with 10.13 High Sierra, Apple has baked the full-blown Time Machine server capability right into macOS—no separate Server app required. Any Mac running High Sierra or later can (with enough storage space and the right settings) host Time Machine backups for all the rest of the Macs on your network. And this capability is not fiddly, like its predecessor; for example, you no longer have to make sure the server’s shared folder is mounted in the Finder on all the client Macs.

The only catch is that you have to know where to find this rather well-hidden feature. Here’s how you set up a Mac as a Time Machine server:

1. Make sure the Mac that will function as the server is running High Sierra or later. For best results, this Mac should also be left on and awake all the time, because other Macs will be able to back up and restore data using Time Machine only when that’s the case.
2. Check to see that the server Mac has *plenty* of free disk space, since it will hold the Time Machine backups for the rest of your Macs (see [Decide on Capacity](#)). Preferably, you should connect an external drive to this Mac for Time Machine backups—partly so you can use it to back up the server as well, and partly to prevent Time Machine from slowing down your internal disk.
3. Confirm that the volume on which your Time Machine backups are stored is formatted as HFS Plus—*not* as APFS (see [APFS Evolves in Mojave](#) and [Prepare Your Hard Drive](#)).
4. On the volume where you want to store your Time Machine backups, create a new folder. The name of this folder and its location on the volume are up to you, but you may find it helpful to give it an obvious name such as “Time Machine Backups.”
5. Go to System Preferences > Sharing > File Sharing, and make sure the File Sharing checkbox is selected (**Figure 14**).

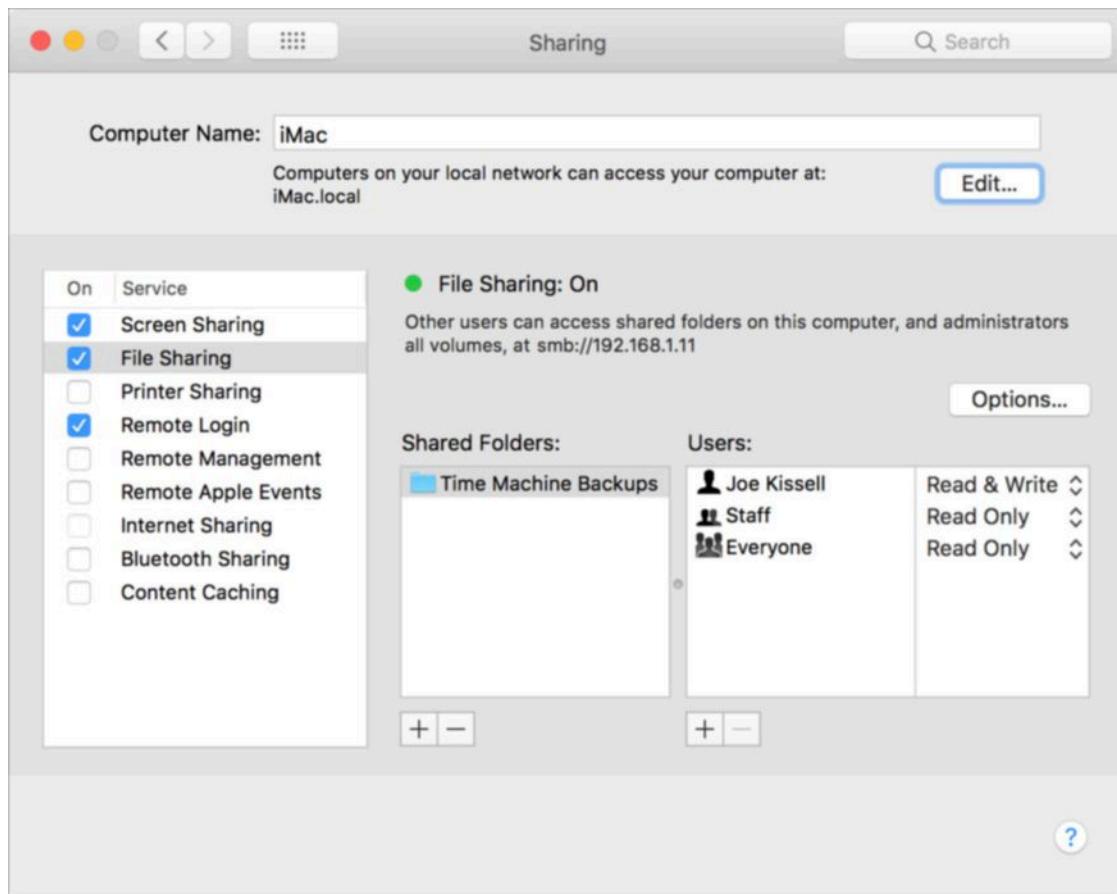



Figure 14: You configure a folder as a network Time Machine destination in System Preferences > Sharing > File Sharing.

6. Click the plus  button under the Shared Folders list, navigate to the folder you created in step 4, select it, and click Add. The folder appears in the list.
7. With the newly added folder selected, click Options. Select “Share files and folders using SMB,” and deselect “Share files and folders using AFP.”
8. Right-click (or Control-click) the newly added folder in the Shared Folders list and choose Advanced Options from the contextual menu (**Figure 15**).

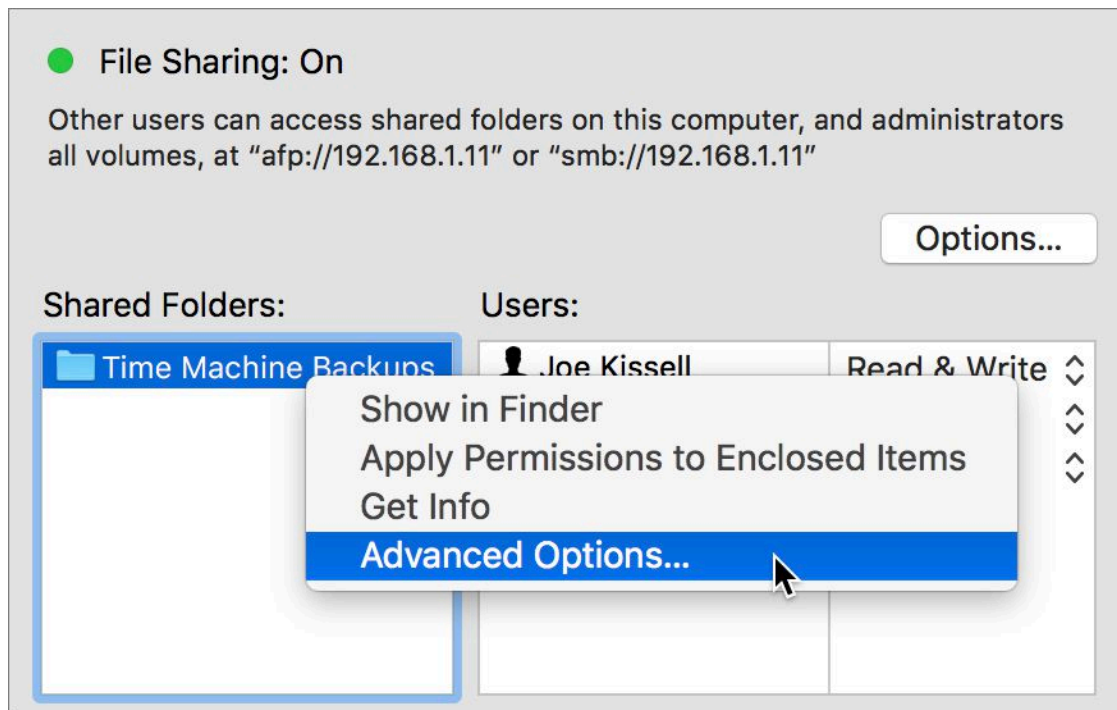


Figure 15: This is where the magic happens—and Apple didn’t make it excessively obvious!

9. In the dialog that appears (**Figure 16**), select the “Share as a Time Machine backup destination” checkbox.

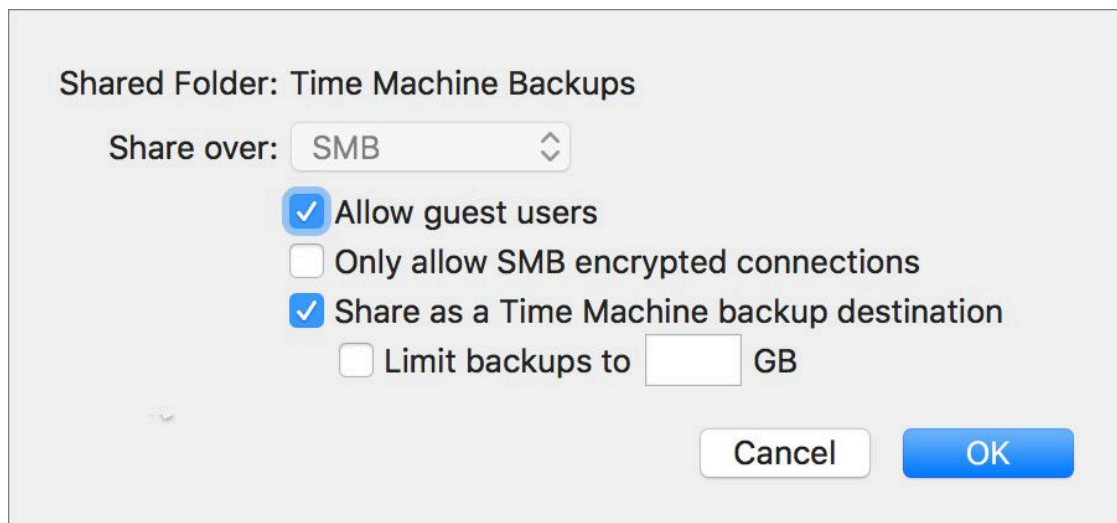


Figure 16: Configure options for your shared Time Machine folder here.

All other settings here are optional:

- ▶ If you followed step 7, the “Share over” pop-up menu should be dimmed, and can therefore be ignored.

- ▶ If you want people without accounts on this Mac to be able to use it as a Time Machine destination (and you probably do), leave “Allow guest users” selected, as it is by default.
- ▶ For increased security using the SMB protocol, select “Only allow SMB encrypted connections.”
- ▶ To make sure Time Machine backups don’t expand to fill every last bit of space on your drive, check “Limit backups to” and enter the maximum total size of Time Machine backups. (But be as generous as you can afford to be, because it’s difficult to change this allotment later.)

Click OK when you’re done, and then close System Preferences.


Once you’ve done all this, you can select this folder as a network destination in Time Machine on all your other Macs, following the instructions in [Choose a Destination](#).

One last thing: the Macs in your home or office can use your Time Machine server only when they’re on your local network. If a Mac is going to be used elsewhere for an extended period of time, make sure you have alternative backup arrangements (see [Back Up While on the Road](#)).

Use a Single Backup Disk with Multiple Macs

You can use Time Machine to back up more than one Mac to a given drive (with or without a Time Capsule or other network destination). A single partition can store backups for any number of Macs, without getting them confused, as long as it has enough free space. In most cases, you don’t have to do, or know, anything special; just plug in the drive (or connect to it over your network), select it on the Time Machine preference pane, and let the backup run; repeat the procedure with each Mac you want to back up. If you’re physically moving the drive between machines, Time Machine should automatically recog-

nize each Mac and back up on its regular schedule, without further intervention, after the first backup.

Note: Before you detach a drive's cable from your Mac, eject the volume by clicking the eject  icon next to its name in the Devices section of the Finder sidebar. If you fail to do this, you could interrupt macOS in the process of writing data, potentially damaging your Time Machine backups.

However, Time Machine has an idiosyncrasy that may cause some unexpected behavior if you move a given drive between local and network connections.

As I mentioned in [Restore Files Without Time Machine](#), Time Machine stores your backups in a *folder* if you've selected a locally connected drive but in a *disk image* if you're backing up over a network. Now say you want to save time on your initial backup by *seeding* it onto an external drive and then moving that drive to another computer where you'll share it over the network. When you connect a drive locally and let Time Machine back it up, you get a folder for that machine inside the `Backups.backupdb` folder. So far so good.

Then you move the drive over to another Mac and share it over the network. On the first Mac, you tell Time Machine to use that shared disk. It will do so, happily, *but* it won't recognize your existing backup; instead, it will start a new one, from scratch, in a freshly created disk image! The reason for this behavior is simple: Time Machine has no way to know that the computer you're backing up over the network is the same one you were backing up locally. (But don't worry, I provide a solution just ahead.)

Now let's reverse the situation. You back up over the network *first*, then later plug the drive directly into your Mac and select it as a Time Machine destination. In this case, Time Machine does recognize that you're backing up the same Mac, and does pick up with the existing backup where you left off, because it sees the MAC address of the computer's Ethernet card (regardless of which network interface you're using at the moment) in the disk image on the backup disk.

So, to seed a local drive with a Time Machine backup and then continue your backups over the network, you just need to add a couple of steps:

1. Start an initial backup over the network, but abort it as soon as it begins copying files by turning Time Machine off.
2. Switch the drive to a local connection and turn Time Machine back on to finish the backup.

After one full backup has been made, reconnect the drive to the Mac that shares it over the network.

Use Power Nap

If you have a laptop Mac that came with solid-state storage, you can use a feature called Power Nap. (For details about which models are supported, whether firmware updates are needed, and more, see Apple's support article [How Power Nap works on your Mac](#).) With this feature enabled, your Mac periodically performs a variety of background tasks even while it's asleep. One of these tasks, which occurs only when your Mac is connected to AC power (even though other aspects of Power Nap also work on battery power), is backing up with Time Machine.

To turn Power Nap on or off, open System Preferences > Energy Saver. Then:



- To specify whether Power Nap (including Time Machine backups) will function while your computer is plugged in, click Power Adapter and then select or deselect “Enable Power Nap while plugged into a power adapter.” (It's selected by default.)
- To specify whether Power Nap (*not* including Time Machine backups) will function while your computer is running on battery power, click Battery and then select or deselect “Enable Power Nap while on battery power.” (It's deselected by default.)

Your selection takes effect when your Mac next sleeps.

Manage Your Time Machine Schedule

Apple believes that most Time Machine users will back up either to a local drive that's always connected or to a network volume that's always available. However, if you travel with a laptop, or if for any other reason your destination disk isn't always available, don't worry: Time Machine still works fine—with some qualifications.



If you have a laptop Mac, Time Machine puts its regular snapshots in a hidden location on your startup disk even when your destination disk is disconnected, and then transfers those locally stored snapshots to your usual Time Machine disk once it becomes available (see [Local Snapshots](#)).

However, if you don't have a Mac with local snapshots enabled, then whenever your backup disk isn't available your files won't be backed up at all—and the only notice Time Machine gives, for the first few days, is a discreet change in its menu bar  icon. (A similar  icon appears if a backup failed for some other reason.) So if you expect to spend long periods of time during which your regular Time Machine destination disk is unavailable, consider using a supplemental backup, such as a cloud backup service or a portable hard drive.

Prevent or Force Time Machine Backups

Sometimes you may want Time Machine *not* to run, even though its destination disk is connected. You may, for example, want to make sure every last bit of your computer's CPU and disk speed is available to devote to some important task, or you may want to keep a noisy external drive quiet for part of the day. Any time you want to suspend Time Machine from running backups, open the Time Machine preference pane and move the big switch from On to Off. Time Machine remembers all its settings, and resumes backups whenever you turn it back on.

On the other hand, in some situations you may want to make sure Time Machine immediately backs up your files. For example, you may have recently saved or downloaded an important document, but the

next scheduled Time Machine run isn't for another 45 minutes. No problem: you can force an immediate backup, *even if Time Machine is off*, by choosing Back Up Now from the Time Machine  menu or right-clicking (or Control-clicking) the Time Machine icon in the Dock and choosing Back Up Now from the contextual menu. (To immediately stop a backup in progress, choose Stop Backing Up from Time Machine's Dock menu or Skip This Backup from the Time Machine  menu.) Note that this doesn't work with local snapshots (again, see the sidebar [Local Snapshots](#)); it applies only when your regular Time Machine volume is available.

Backing Up on Battery Power

In System Preferences > Time Machine > Options on a Mac laptop, you can enable or disable a "Back up while on battery power" checkbox. When this option is enabled, Time Machine normally runs every hour, even when you're not connected to AC power, as long as your destination drive is available. When the option is disabled, Time Machine pauses while you're running on battery. Note that this is distinct from Power Nap, which applies only when your Mac is asleep; this setting is for when your Mac is awake.

Regardless of how regularly you have Time Machine turned on or how frequently you run manual backups, you should be aware that the method Apple uses to automatically purge older backups can, in some cases, delete files you thought were backed up. Read the sidebar [The Time Machine Schedule Problem](#), next. If you want to alter the frequency of Time Machine's regular backups to something other than hourly, skip ahead to [Modify the Hourly Backup Interval](#).

The Time Machine Schedule Problem

Time Machine says it saves hourly backups for 24 hours, daily backups for a month, and weekly backups until your disk is full. That seems reasonable, but if you look at the details, there's a catch.

Time Machine makes a new backup every hour that your Mac is on and awake. With each run, Time Machine also *deletes* the hourly backup from 25 hours ago, unless it was the first backup of that particular day. Thus you always have hourly backups for the last 24 hours, as well as a *single* hourly backup (from just the last hour of the day) for each of the past 30 days. After a month, Time Machine deletes the oldest of the daily backups, but it preserves the first daily backup from each week as long as there's disk space available.

Now picture this: At 8:30 P.M. on Monday you create an important file. When Time Machine runs next (at, say, 9:00 P.M.) it backs up that file; so far, so good. At 9:30 P.M., you delete the file, either intentionally or otherwise. No problem: it's still in your backup. Of course, none of the hourly backups for the next 24 hours includes your file, because it had already been deleted, so the only copy Time Machine has is in that first hourly backup. At 10:00 P.M. on Tuesday, Time Machine erases that backup from 25 hours ago—the only one, from 9:00 P.M. on Monday, that contained your important file. Because that file wasn't in the *last* hourly backup of that day, it won't be there tomorrow if you suddenly realize you need it, even though Time Machine backed it up yesterday! (Indeed, this very thing happened to me just a few days before I updated this book to version 3.1!)

So, there are ways that files can fall through the cracks. Time Machine backs them up, sure, but because of the way it deletes old backups, it may *remove* an essential file from the backup before you need it. (The same goes for when Time Machine deletes old daily and weekly backups.) Plus, if a file exists for less than an hour and therefore isn't around for a single backup, Time Machine won't help at all.

The lesson? First, supplementing your Time Machine backups is a good idea. And second, get in the habit of hanging on to files for at least 24 hours before you delete them!

Modify the Hourly Backup Interval

Time Machine normally runs every hour, but what if you'd like it, instead, to run every three hours or twelve hours? You can adjust the backup interval using a free utility. [TimeMachineEditor](#) lets you set Time Machine's backup interval to any number of hours and choose arbitrary recurring backup times (such as hourly on Mondays and Fridays, or every Saturday and Thursday at 6:15 A.M.). And you can opt to have backups run automatically when the Time Machine disk is mounted, when your Mac wakes up, or both. One oddity is that TimeMachineEditor automatically deselects the Back Up Automatically checkbox on the Time Machine preference pane (or, in older versions of macOS, turns Time Machine's master switch to Off). But don't worry about this, because that checkbox (or switch) affects only Time Machine's default hourly backups.

Migrate to a Larger Time Machine Disk

When your Time Machine backup volume fills up, Time Machine will delete old files to make room for new ones, but sooner or later you may want to have more backup capacity—whether for more files, a longer history, or files from multiple users. So the natural solution is to switch to a bigger disk (or maybe from a local drive to a network destination with a larger disk). If you simply switch disks on the Time Machine preference pane, you'll have to start over with a brand-new full backup. If you prefer to keep the continuity of your existing backups on the new drive, you can—but you'll have to jump through a few hoops.

The procedure is somewhat different depending on whether you're migrating to a new local disk (discussed next) or to a Time Capsule or other network destination (see [Migrate to a Network Volume](#), ahead).

Migrate Between Local Drives

If you're moving your Time Machine backups from one local drive to another, make sure both the old drive and the new one are connected and mounted in the Finder.

Then follow these instructions:

1. In System Preferences > Time Machine, deselect the Back Up Automatically checkbox (or, in El Capitan or earlier, move the switch to Off).
2. Follow the steps earlier in [Prepare Your Hard Drive](#) to partition the *new* disk as a single volume using Disk Utility's GUID Partition Table option.
3. Follow the instructions for the operating system you're using.

El Capitan or later:

- a. In High Sierra or later only, choose View > Show All Devices.
- b. In the Disk Utility sidebar, select your *new* backup volume (the indented volume name, not the higher-level disk name).
- c. Choose Edit > Restore.
- d. Choose your *current* backup volume from the "Restore from" pop-up menu.

Yosemite or earlier:

- a. In the Disk Utility sidebar, select your *current* backup volume (the indented volume name, not the higher-level disk name).
 - b. Click the Restore tab. The name of your current backup volume should appear in the Source field.
 - c. From the sidebar, drag your *new* Time Machine backup volume (again, the indented volume name, not the higher-level disk name) into the Destination field. If you see an Erase Destination checkbox (which appears only in older versions of OS X), select it.
4. Click Restore. If a confirmation alert appears (which should happen only in Yosemite or earlier), click Restore again.

Disk Utility copies your existing backup volume onto the new volume. Depending on the amount of data you have and the type of

interface your drives use, this process could take anywhere from hours to days.

5. When the copying is finished, quit Disk Utility, and eject the old backup volume in the Finder.
6. In System Preferences > Time Machine, select the new backup volume and make sure that the Back Up Automatically checkbox is selected (or, in El Capitan or earlier, that the switch is set to Off).

Time Machine should pick up where it left off the last time you backed up to your local drive.

Migrate to a Network Volume

If you've been backing up to an external drive for a while and then you buy a NAS—or decide to set up a Mac to function as a Time Machine server—you may want to move your existing Time Machine backups to the new network volume rather than start over from scratch. Likewise, if you already have a NAS or Time Capsule and switch to a larger one, you may again want to move your backups to the larger volume—or you may want to migrate from a local drive to a network volume. Use the same procedure for any of these situations:

1. Follow the steps earlier in this chapter (see [Choose a Destination](#)) to select the new network volume as your backup destination, and let the first backup begin. This process will generally go much faster if you have your Mac connected to the NAS, Time Capsule, or network via Ethernet; even if you later switch to Wi-Fi, use a wired connection for this initial backup if possible.
2. As soon as Time Machine gets past the “Preparing backup” stage and starts copying data, deselect the Back Up Automatically checkbox (or, in El Capitan or earlier, move the switch to Off).
3. In the Finder, select your new NAS, Time Capsule, or network volume and double-click the folder inside it that contains your Time Machine backups; the name may vary, but it's likely the only folder on the disk. (If a Time Capsule doesn't mount automatically, click Connect As and enter your username and password.) In this folder

is a disk image containing the backup you just started and then quit. Double-click the image, which should then mount in the Finder.

4. If you're moving from a local drive to a NAS or network volume, make sure the local drive is connected and mounted in the Finder.
5. Open Disk Utility (in [/Applications/Utilities](#)).
6. Follow the instructions for the operating system you're using.

El Capitan or later:

- a. In the Disk Utility sidebar, select the mounted disk image for your *new* backup volume (which should be named "Time Machine Backups").
- b. Choose Edit > Restore.
- c. Choose your *current* backup volume from the "Restore from" pop-up menu.

Yosemite or earlier:

- a. In the Disk Utility sidebar, select your *current* backup volume (the indented volume name, not the higher-level disk name).
 - b. Click the Restore tab. The name of your current backup volume should appear in the Source field.
 - c. From the sidebar, drag the mounted disk image for your *new* Time Machine backup volume (which should be named "Time Machine Backups") into the Destination field. If you see an Erase Destination checkbox (which appears only in older versions of OS X), select it.
7. Click Restore. If a confirmation alert appears (which should happen only in Yosemite or earlier), click Restore again.
 8. Disk Utility copies your existing backup volume onto the new volume on your NAS, Time Capsule, or network server. Depending on the amount of data you have and whether you use a wired or a wireless network, this process could take anywhere from a few hours to several days.

9. When the copying is finished, quit Disk Utility, and eject your NAS, Time Capsule, or network volume in the Finder.
10. In the System Preferences > Time Machine, turn Time Machine back on by selecting the Back Up Automatically checkbox (or, in El Capitan or earlier, moving the switch to Off).

That's it. Time Machine should pick up where it left off the last time you backed up to your previous destination.

Avoid or Solve Time Machine Problems

Although Time Machine has a very simple user interface, behind the scenes it's doing some highly complex tasks. Like any sophisticated piece of software, it has bugs and flaws. Review these tips to prevent problems or fix ones that have already occurred.

Check for Hidden Exclusions

If a file or folder that you believe should be backed up is not appearing on the Time Machine screen (see [Restore Data with Time Machine](#)), first check to see that the item in question isn't on the Exclude list (see [Exclude Files from Time Machine](#)).

Note, however, that under certain circumstances, Time Machine can exclude files and folders *without* showing them on the Exclude list! To check the inclusion/exclusion status of a file or folder, follow these steps:

1. Open Terminal (in [/Applications/Utilities](#)).
2. Type `tmutil isexcluded` followed by a space (but don't press Return yet).
3. From the Finder, drag the file or folder you're wondering about into the Terminal window. This puts the full path to that item on the same line, right after the command you just entered.
4. Press Return.

The next line will start with either `[included]` or `[excluded]`, indicating whether the item is included in your Time Machine backups or not. If an item is excluded and you want it to be included, type `tmutil removeexclusion` followed by a space. Drag the item into the Terminal window, and press Return.

Restore Files After a Hardware or Name Change

Because of the way Time Machine stores its data, certain changes to your system could cause Time Machine to “lose” its backups—to seemingly forget which backups go with your disk, such that no existing backups appear when you visit the Time Machine screen, and your next backup starts over from scratch. Among the changes that could trigger this condition are:

- Restoring your entire disk (not just a few files or folders) from a Time Machine backup
- Having your logic board replaced
- Changing your Mac’s name in System Preferences > Sharing

In these cases, you can retrieve files from that previous set of backups and even reconnect Time Machine to your current disk. See the sidebar [Restarting Time Machine Backups After a Restore](#), earlier, for details.

See What Time Machine Is Really Up To

To find out how much data (number of files or size) Time Machine backs up with each run, get details on any errors it encounters, or find clues to solving random problems, open Console (in `/Applications/Utilities`). Make sure the list of available logs is visible on the left (if not, choose View > Show Sources in Sierra or later, or click Show Log List in El Capitan or earlier) and select `system.log` in the list under Reports (Sierra or later) or FILES (El Capitan or earlier). Then type `backupd` in the Search (or Filter) field to display only the entries involving Time Machine.

Note: To view the system log, you must be logged in with an account that has administrator privileges.

If you notice that Time Machine is regularly backing up much more data than what should have changed in the past hour, first follow the suggestions in this section and in [Items to Consider Excluding](#). Then look for other especially large files that may be causing problems.

One easy way to find such files is to use [BackupLoupe](#), which lists every snapshot that your Time Machine volume currently holds. Select any snapshot in the list and the app displays only the files and folders that were copied during that particular run, along with their sizes.

If you want even more detail about what Time Machine is doing, you can try [Back-In-Time](#). This utility comes from Tri-Edre, the same company that makes Tri-Backup. When I first saw this app, I was confused because I thought it did nothing more than show me the same files as on the Time Machine screen, only with a different interface. But in fact it lets you dig deeply into your Time Machine backups to see information that would be difficult to learn in any other way.

You can:

- See at a glance how many copies of each file Time Machine is storing
- See at exactly which point in time a file appeared in, or was deleted from, a certain folder
- List all the files copied during a certain backup run
- Compare any two snapshots (in part or whole) to see what's different between them, and even two versions of the same file to see what's changed

You can also restore files or delete data from Time Machine—with more flexibility than Apple's interface offers—directly in Back-In-Time.

Use Other Versioned Backup Software

If you’ve decided to create versioned backups using an app other than (or in addition to) Time Machine, set that up now. I wish I could give you step-by-step instructions for using each one of those apps, but that would take too many pages (and you can read the app’s documentation for help). Instead, I want to give you a few tips for each of several good choices, all of which I mentioned back in [Choose Another Versioned Backup App](#). Although I’ve used and can recommend each of the apps I mention here, I don’t pretend that this is an exhaustive list. There are many other excellent options, and you can read about them in the [online appendixes](#).

Later in the chapter, I also give several general pointers about things like power management and testing versioned backups.

Arq Tips

Arq is an increasingly popular choice for people who want the benefits of cloud storage but also want greater control over their data than cloud backup providers offer—and the freedom to choose inexpensive cloud storage. If you use Arq for your versioned backups (or are considering doing so), keep the following in mind:

- **All cloud storage is not created equal.** Arq supports lots of different cloud storage providers, some of which are so inexpensive that they seem almost too good to be true. As I point out later, in [BYOS \(Bring Your Own Software\) Internet Backups](#), some cloud storage services limit your upload rate—perhaps only after you’ve transferred a given amount of data or number of files in a certain month. The result can be that backups are disappointingly slow. So read your provider’s fine print and try some speed tests with a few gigabytes of data before you start to upload files by the millions.

- **Backups run on fixed schedules.** Compared to, say, Backblaze, which backs up your data continuously, Arq can run any given backup no more often than once per hour. So, if you're moving to Arq from a competitor that backs up files as often as you save them, you might need to adapt your thinking and behavior, because Arq won't make such frequent copies. (In addition, running less frequently means each backup is likely to take longer.) You can, however, work around this somewhat by setting up multiple backups to the same destination; make them identical except for the time. (For example, make the first one hourly on the hour and the second one hourly on the half hour.)
- **Mind your settings.** Arq helps you avoid unexpected expenses by letting you set a budget (the maximum amount of storage space your backups can occupy on any given cloud service), but this feature is disabled by default—and even when it's on, your budget is enforced only at an interval you set (such as every 30 days). So review the settings carefully for each destination and make sure you're taking advantage of Arq's money-saving features.
- **Arq supports local backups too.** Although Arq is best known as a backup app to be used with cloud destinations, you can also choose local hard drives, network volumes, or NAS devices as destinations. That makes it much more versatile than most cloud backup apps and lets you use the same app for both local and cloud-based versioned backups. Alas, Arq lacks the capability to make bootable duplicates, so you'll still need a separate app for that.

Note: Although I haven't tested them in any detail, a number of newer backup apps are broadly similar to Arq (in the sense of focusing on versioned backups to user-supplied cloud storage, but with the option to do local backups too), and if that's the general path you want to take, you might also consider looking into [CloudBerry Backup](#), [Duplicacy](#), and [Duplicati](#).

ChronoSync Tips

If you've selected ChronoSync for versioned backups, please do the following:

- **Put synchronizers in containers.** ChronoSync is designed around the concept of documents called *synchronizers*, which contain the instructions for backing up or synchronizing something.

When you set up a backup or sync operation, you're creating a synchronizer, which the app prompts you to save when you close the window or quit the app. Although ChronoSync gives you a wealth of options for each synchronizer, one fundamental limitation is that a synchronizer can apply to only a single volume or folder (and everything inside it). If you want to back up items from more than one location (perhaps even with different options) in a single operation, create one synchronizer for each folder or volume, save them individually, and then choose File > New > Container and add each synchronizer to the list. You can then run all the synchronizers in one pass, and even schedule the entire container to run at a predetermined time.

- **Take the easy way out.** ChronoSync is amazingly flexible, but the flip side of that flexibility is a somewhat complex user interface; for example, you have to choose one of 11 backup or sync operations for each synchronizer, but the names and functions of these operations are far from self-explanatory. But I have good news! In a recent update, ChronoSync added a Setup Assistant, which walks you through each step of the process and creates the synchronizer you need without overwhelming you with technical terminology. To use this tool, just click the "Use a setup assistant" button in the main ChronoSync Organizer window.
- **Look for new destinations.** ChronoSync can now back up to Amazon S3, Backblaze B2, Google Cloud Storage, and SFTP servers, and support for more cloud destinations is reportedly in the works. Although ChronoSync can't yet work with as many cloud destinations as Arq can, it's moving in that direction.

- **Dissect away.** ChronoSync can optionally look inside a *package* (a special folder that acts like a file) when performing a sync, so that if just some of the contents have changed, only those items are copied. This is crucial for things like your Photos library, because without using this feature, the entire library must be copied if even a single photo is added or changed. For reasons that are unclear to me, this feature is turned off by default, and you must re-enable it manually whenever you create a new synchronizer. To do so, click Options, choose Custom from the pop-up menu under Special File/Folder Handling, and choose Dissect from the “Package handling” pop-up menu.
- **Use archives for versioned backups.** To create a synchronizer that produces versioned backups, choose Backup (either Left-to-Right or Right-to-Left, depending on your setup) from the Operation pop-up menu and check the “Archive replaced files” box. Then click Options, and in the Archive Handling section, select the options you want (such as how many copies of each file to keep and when to purge older versions). (If you used Setup Assistant, as I recommended above, you may not need to do this manually, but it may be useful to know what’s happening behind the scenes.)
- **Get a good agent.** ChronoSync, by itself, can back up the Mac it’s on, and it can optionally use mounted network volumes as the source or destination. However, to back up to or from another Mac on your network with administrative privileges, keeping ownership and permissions intact—crucial for, among other things, creating a bootable duplicate over the network—you must install the add-on app [ChronoAgent](#) on the other Mac.

Note: Are you looking for information on CrashPlan, which should appear here in alphabetical order? I’m sorry to say it’s gone; read [CrashPlan for Home Is Finally Gone](#) for details.

DollyDrive Tips

If DollyDrive is your preferred tool, consider these things:

- **Local and remote:** DollyDrive is best known for its online storage, but its software can (like Arq and ChronoSync) also back up your data to a local hard drive. As I’ve said elsewhere in this book, I’m a big believer in having both local and offsite backups, and DollyDrive can cover both needs.
- **Cloned like Dolly:** In addition to creating versioned backups, the DollyDrive software can store a bootable duplicate on an external drive using its Clone feature.
- **Sync and share too:** DollyDrive isn’t just for backups; it can also enable multiple Macs and iOS devices to sync files with each other via the cloud and share files with other people, in much the same way as Dropbox.

In short, DollyDrive is the complete package—the only tool I know of that offers versioned local and online backups, bootable duplicates, cloud syncing, *and* file sharing in a single piece of software. (That doesn’t necessarily mean it’s the *best* tool for each of those jobs—for example, at the moment, the most frequent backup interval is hourly—but it’s nice to have so many capabilities rolled into a single package.)

QRecall Tips

If you use QRecall for versioned backups, I suggest the following:

- **Learn the lingo.** QRecall has its own special vocabulary. You may find the app easier to use if you translate its jargon into more familiar words. When you see *capture*, just think “store a versioned backup.” (QRecall uses *archive* to mean a special file in which versioned backups are stored.) When you see *recall*, think “restore,” and when you see *restore*, think “restore to the *original* location.” A *layer* is essentially a snapshot that contains only the items copied during a particular incremental update of a versioned backup. You

can *merge* (combine) layers for convenience; you can also do a *rolling merge*, in which layers are combined according to your specifications after a certain number of days.

- **Let the Assistant help.** To get help setting up complex options in QRecall, Choose Help > Capture Assistant.
- **Use multiple keys to save space.** Although you can use a single QRecall license key on multiple computers, doing so means each computer must store its data in a separate archive. If you purchase an individual license for each Mac, they can all share a single archive—significantly reducing the overall size of the backup, because QRecall doesn't store *any* duplicated data.

Note: As of publication time, the latest version of QRecall (2.1.12) mostly works with Mojave, but [see this thread](#) for some qualifications.

Retrospect Tips

If Retrospect is your weapon of choice, consider these tips:

- **Get the right edition.** If you're backing up a single Mac (whether to one or more external hard drives, to the cloud, or both), you now want [Retrospect Solo](#). If you want to back up multiple Macs over your network to shared storage—or if you want to back up to or from a NAS—you'll need [Retrospect Desktop](#). But note that the same software is used for all editions; the license you enter determines which features are enabled.
- **Understand the terminology.** Retrospect has always had a somewhat odd way of referring to certain activities, and starting with version 8.x—it's at 15.6 as of publication time—quite a few terms changed (some for the better, others not so much). On the plus side, what older versions called *selectors* (which could either *include* or *exclude* files) are now called *rules*, and the ambiguously named Backup Server feature is now called Proactive Backup. However, what was formerly *duplicate* (namely, the operation you

choose if you want a bootable duplicate) is now the less-specific *copy*, while *scripts*—specifications for backup operations—keep the same name, even though they don't resemble what the rest of the world calls scripts (procedures written in a language such as AppleScript).

- **Parts is parts.** Even if you use the app only to back up a single Mac, you must install and configure both Retrospect Engine (which does the work of copying the files, and is turned on and off via System Preferences > RetrospectServer) and the Retrospect app itself (sometimes referred to as Retrospect Console), which lets you configure and control backups. The first thing you must do after running Retrospect is to tell it where to find the engine you want to work with—which, in the case of the one running on the same Mac as the console, is at the address `127.0.0.1`.

Don't Let Backups Cause Data Loss!

What? Backups are supposed to *prevent* data loss, right? Yes, of course, but as TidBITS publisher Adam Engst found, a combination of poor app design and user error can lead to a situation where you're not backing up the data you think you are, and as a result every backup *overwrites* the data you want to keep with old data, rather than making a copy!

In Adam's case, this happened as a result of accidentally setting iPhoto to use the copy of his iPhoto Library stored on his bootable duplicate. He tells the story—and explains how to avoid this problem by configuring your backup software to automatically mount your disk when needed and unmount it after the backup completes—in [Clone Wars, or How My Backups Ate My Photos](#).

Power Management and Backups

A scheduled backup will not run unless your computer is turned on and awake at the scheduled time. (A few backup apps—including Carbon Copy Cloner, Data Backup, and QRecall—can wake up or turn on your Mac when it's time for a scheduled backup. You can find others with this capability in the [online appendixes](#). Time Machine doesn't have this problem, since it doesn't operate on a fixed schedule—and it can also run when your Mac is asleep, thanks to Power Nap; see [Use Power Nap](#).)

Some people leave their Macs running all the time, perhaps setting the display to dim or the hard drive to spin down after a certain amount of idle time to save energy. However, if you normally turn off your Mac or put it to sleep when you're done using it—or if you've set it to go to sleep automatically—you may run into problems with scheduled backups when your backup app can't wake up or turn on your Mac for you. In most cases, these problems are easily solved with a bit of foresight.

Your Mac's power management is controlled using System Preferences > Energy Saver. If you click the Schedule button, you'll see a checkbox labeled "Start up or wake." If you select that checkbox and enter the days and times corresponding to your backup schedule (say, every day at 2:00 A.M.), the machine will turn on or wake up at the appropriate time.

Some words of caution, however:

- ✦ Select times at least five minutes before your backups are scheduled, to allow your Mac time to start up completely.
- ✦ If you set your Mac to request your password when you turn it on or wake it up, the Mac may get stuck at the login screen when you're not there. You can turn off this prompt—trading the convenience of unattended backups for the security of requiring your password—by going to System Preferences > Users & Groups > Login Options and choosing your username from the "Automatic login" pop-up menu. But...
- ✦ If you use FileVault, automatic login is unavailable. Your Mac will wake up or turn on at the scheduled time but be unable to continue without someone to enter your password.

Test Your Versioned Backup

When your first full versioned backup is complete, test it by choosing a few random files or folders to restore. If your backup software has a Restore feature, use it; if not, you'll have to restore the files manually (usually with drag-and-drop).

To test your backup, follow these steps:

1. **Restore to a different location.** Most backup software lets you restore files either to their original locations or to another location of your choice. For this test, restore your selected files to a *different* location—say, your desktop, where you can find them easily.
2. **Check the restored files.** Compare the restored files to the originals using the Finder's File > Get Info command. Each pair of files should match exactly: same name, size, icon, creation date, and modification date. You should also confirm that the files open correctly. If the files were not copied, were not identical, or didn't open, then either your backup software or its user made a mistake! Check your software's documentation, and if necessary contact the developer's technical support department for assistance.
3. **Try an in-place restoration.** Temporarily move one of the original files you backed up to a different location (again, your desktop works well for this), then use your app's Restore feature (if it has one) to restore the file to its original location.
4. **Check the restored files.** Again, check each file carefully to make sure it's correct.

If the files are correct regardless of the location to which you restored them, your versioned backup is working properly.

Test Backups Regularly

Even if your initial test of a backup succeeds, test your backups regularly to confirm that they're still intact and that all the required files are being updated as they should be. If you're unaware of an error that has been preventing your backups from running properly, the consequences could be severe.

How often should you do this? Once every few months or so is a good idea. Adam Engst has declared Friday the 13th (every one of them) [International Verify Your Backups Day!](#)

In addition to verifying your backups, you might want the security of a service that monitors your backup software constantly and informs you if backups fail to run or encounter other serious errors. One such service is [Watchman Monitoring](#). Although it's geared mainly toward businesses, you can use the company's [Provider Locator](#) to find a local IT service that will sell you an individual subscription (typically in the range of \$5 to \$10 per month). Supported software includes Time Machine, Backblaze, and Carbon Copy Cloner.

Note: Sooner or later, the disk containing your versioned backups is bound to get full. But don't worry; I explain what to do a bit later, in [What to Do When Your Disks Fill Up](#).

Create and Use a Bootable Duplicate

Along with versioned backups, bootable duplicates are a key component of a complete backup plan. They let you get back to work quickly in the event of a hard drive failure, give you a useful troubleshooting tool, and make upgrading to a new version of macOS safer.

You can't make a bootable duplicate by copying files in the Finder; you need a special utility. Lots of apps can do this, but in this chapter I focus on two—Carbon Copy Cloner and SuperDuper!—that specialize in this one task and do an excellent job at it.

Warning! Remember, you cannot store duplicates of two drives on the same volume, even if you put them in separate folders; the result will not be bootable. They must be on separate partitions or on entirely separate drives. Oh, and let me reiterate yet again: you cannot create a bootable duplicate onto a NAS or a Time Capsule (or even an external drive connected to one of these).

Carbon Copy Cloner and SuperDuper! can make one-off duplicates, but they can also run automatically on a schedule, updating the duplicate with just the files that are new or changed since the last run, and deleting files on the destination that are no longer on the source disk. I recommend scheduling your duplicate to update itself at least once a week (daily is even better) as well as right before any macOS update.

I should mention that by default, making a duplicate of your startup disk will *not* also duplicate the hidden Recovery HD partition that Apple installs automatically with macOS. That is to say, if you boot from your duplicate or restore an entire disk from your duplicate, you won't be able to use macOS Recovery unless you reinstall macOS on the disk—something you should never have to bother with if you have a bootable duplicate. That's not a serious concern, though, in that the point of Recovery is to give you a way to repair and restore your Mac if

you don't have another bootable disk—a situation you won't find yourself in if you have a bootable duplicate! However, Carbon Copy Cloner can duplicate the Recovery HD partition if you so choose; consult the app's documentation for instructions. (Unfortunately, SuperDuper! can't do this trick.) In addition, a free utility called [Recovery Partition Creator](#) can add a Recovery HD partition to an existing disk.

Duplicates of Non-Boot Volumes

This chapter is about making an exact copy of your startup volume so that you can boot from it later. But you may have other internal or external drives as well, and although duplicating them wouldn't result in a *bootable* backup, it may still be worth considering (either instead of or in addition to versioned backups for those drives).

I say this for two reasons:

- ✦ If a secondary drive dies and you urgently need to get back to work with the data that was on it, having a duplicate that you can swap out in minutes is better than waiting the hours it would take to restore a whole drive from a versioned backup. (This is the same reasoning I apply to bootable duplicates.)
- ✦ Some types of data you may store on a secondary drive don't lend themselves well to versioned restoration. For example, if you restored a single photo from your Photos library, the Photos app might not display it. Photos relies on a database to tell it what items are where, and restoring the photo wouldn't modify the database. You need to restore the *entire* library from a backup, not just an individual photo. And restoring that much data will likely go quicker from a duplicate than from a versioned backup.

You can create and update duplicates of non-boot volumes following exactly the same procedure you use for your startup volume.

Give the Destination Volume a Unique Name

If you didn't do so when partitioning the drive (see [Configure Your Drive](#)), rename the destination volume for your bootable duplicate so that it's different from your Mac's regular startup volume. This will help eliminate confusion later on, especially when you're testing your duplicate and restoring files. To change the name, select the volume in the Finder, right-click (or Control-click) it, choose Rename “*Volume Name*” from the contextual menu, type a new name, and press Return.

Create a Duplicate with Carbon Copy Cloner

[Carbon Copy Cloner](#) was one of the first tools available for creating a bootable duplicate of a macOS volume, and it has undergone numerous revisions over the years.

Carbon Copy Cloner was originally designed only for creating bootable duplicates, but it has gradually added more features. It now also optionally creates versioned backups (although, to be honest, they're not particularly easy to restore). To do this, Carbon Copy Cloner moves any outdated or deleted files safely aside on the destination disk—meaning the duplicate actually contains extra data, but that's fine because the archived versions of old files won't prevent booting or normal operation. Carbon Copy Cloner now has several other safety features too, which can protect you from the consequences of accidental file deletion.

In the instructions that follow, I deliberately avoid most of these safety features, and instead show you how to create a standard, run-of-the-mill duplicate that's a true clone of the source volume. Consult the documentation that comes with Carbon Copy Cloner to learn about other ways of using the software to back up your disk.

To create a duplicate with Carbon Copy Cloner, follow these steps:

1. Launch Carbon Copy Cloner (**Figure 17**).

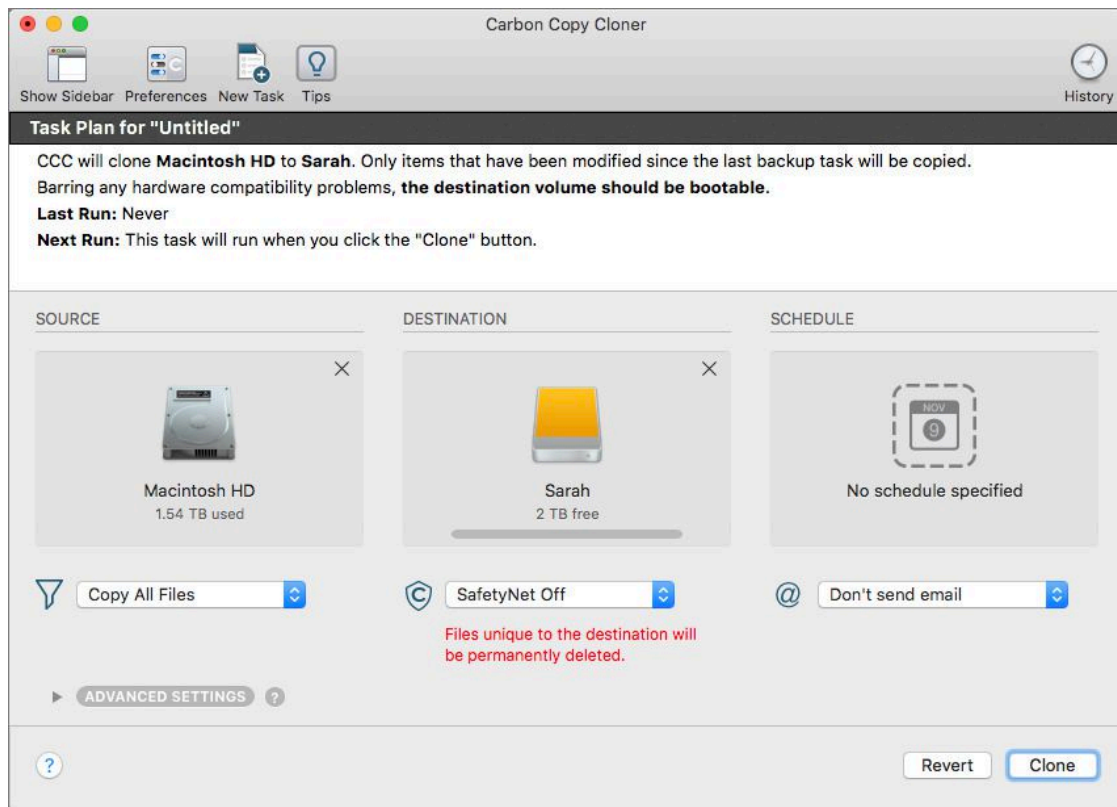


Figure 17: Carbon Copy Cloner shows you the basic elements of your backup—source, destination, options, and schedule—and a plain-English explanation.

2. Click in the SOURCE area and select your startup volume from the popover that appears.
3. Click in the DESTINATION area and, from the popover that appears, select the disk or partition set aside for duplicates on your external disk.
4. Choose SafetyNet Off from the pop-up menu under DESTINATION.
5. Optional but recommended: click in the SCHEDULE area and, in the popover that appears, choose a frequency for scheduled updates of your bootable duplicate from the “Run this task” pop-up menu. Click Done.

6. Click Clone, enter your administrator password, and click OK to make an immediate duplicate. Then be prepared to wait; it will take a while.
7. Click Save when prompted to do so. You can then quit Carbon Copy Cloner. (In fact, you can quit even if a backup is in progress; Carbon Copy Cloner can finish the backup even when the app is not running.)

If you set up a schedule in step 5, Carbon Copy Cloner updates your duplicate automatically (as long as the drive is available).

Creating a Bootable Duplicate over a Network

I've stated a few times that Carbon Copy Cloner can perform the useful and unusual trick of creating a bootable duplicate over a network. You could, for example, have a bunch of external drives connected to a central Mac and set up all the other Macs in your home or office to store their bootable duplicates on those drives. Particularly for people with laptop Macs, this arrangement might be more convenient than constantly plugging and unplugging drives.

The process for setting up network duplicates with Carbon Copy Cloner, however, is far from obvious. You can see the complete details in the article [Using Carbon Copy Cloner to back up to/from another Macintosh on your network](#). It may seem like a lot of steps, but bear in mind that setup is a one-time process, and thereafter your network backups can proceed without intervention.

Create a Duplicate with SuperDuper!

[SuperDuper!](#) has a well-deserved reputation for its ease of use and reliability. The software comes in a full-featured paid version and a free version that lets you create duplicates but not update them incrementally. (Let me say that the incremental update capability is well worth the price!)

To create a duplicate with SuperDuper!, follow these steps:

1. Launch SuperDuper!.

2. You'll see two pop-up menus at the top of the window (**Figure 18**); choose the source (your internal disk) from the one on the left and the destination (the disk or partition set aside for duplicates on your external disk) from the one on the right.

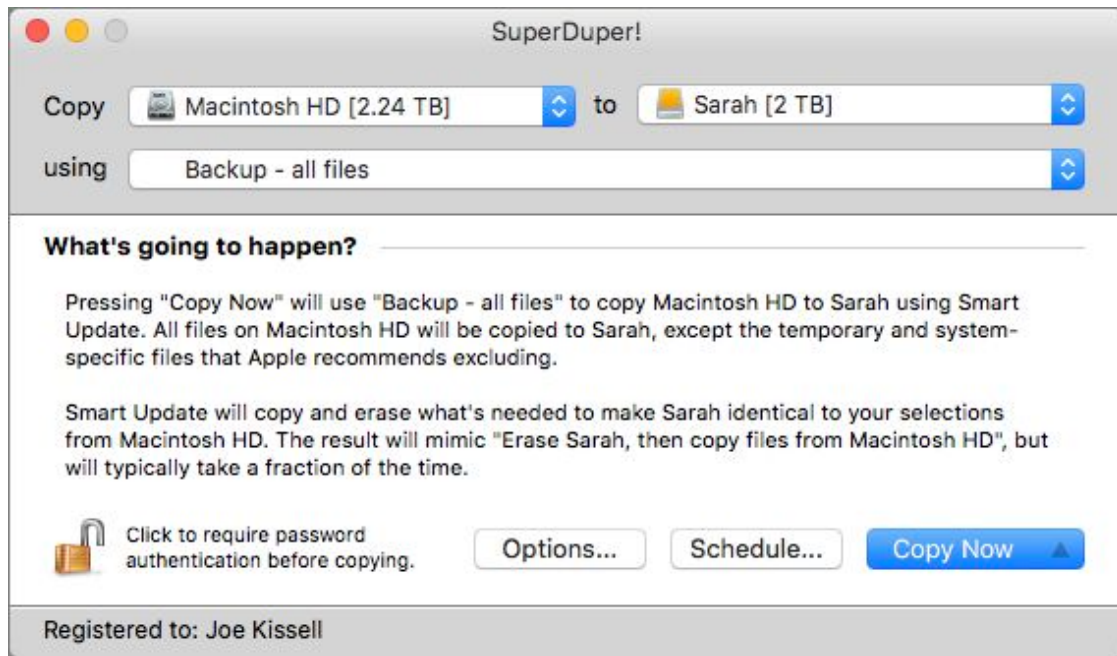


Figure 18: Much like Carbon Copy Cloner, the SuperDuper! window asks you for just a few pieces of information, and clearly explains what will happen in plain English.


3. From the “using” pop-up menu, choose “Backup - all files.”
4. If the lock icon in the lower-left corner is in the locked position, click it, enter your password, and click OK.
5. Click Options. In the General view, choose “Smart Update *Destination* from *Source*” from the “During copy” pop-up menu. Click OK. (Bear in mind that this option, which provides incremental updates, is available only in the paid version of SuperDuper!)
6. Do either of the following:
 - ▶ To make a duplicate immediately, click Copy Now, then click Copy to confirm that you really want to do this. (Be prepared to wait; your first duplicate will take quite a while.)
 - ▶ To set this duplicate to occur on a schedule, click Schedule and select the day(s), week(s), and time to run the schedule; I recom-

mend at least one day per week but preferably once a day, at a time when you aren't actively using the Mac. Click OK.

Immediately or on the schedule you selected, SuperDuper! duplicates your internal drive to your external drive.

Test Your Duplicate

After you've made your first bootable duplicate, be sure to verify that you can indeed start your Mac from it. To do this, follow these steps:


1. Make sure your bootable duplicate is connected to your Mac. Then restart your Mac by choosing Apple  > Restart and clicking Restart when prompted.

Be aware that since you're going to be switching to a different startup drive, deselecting the "Reopen windows when logging back in" checkbox may not have the desired effect; windows and apps may still reopen when your Mac finishes booting. If you want to avoid that, instead open System Preferences > Startup Disk, select your duplicate, and perform a safe boot. See the sidebar [Perform a Safe Boot](#) for details.


Note: If you have a newer Mac with a T2 chip ([see full list here](#)), before you perform step 2 you must [follow these instructions](#) to reboot in macOS Recovery, choose Utilities > Startup Security Utility, and select "Allow booting from external media" under External Boot. Then restart your Mac. (You should *not* change the Secure Boot setting, however.)

2. As soon as your Mac begins to restart, press and hold the Option key.
3. When your screen shows the volumes available for booting your computer, release the Option key, use the arrow keys to select your duplicate, and press Return. Your Mac should boot from the duplicate—but be aware that this may take considerably longer than booting from your regular startup disk; if your backup disk uses a

slow interface, such as USB 2.0, it might take a very long time indeed.

4. To verify that your Mac has indeed started from the duplicate and not from your regular startup disk, choose Apple  > About This Mac. The name of the current startup disk appears next to the label “Startup Disk.” (You *did* give your duplicate a different name from your regular startup disk, right?)

Warning! Unless you’re planning to run your Mac from the duplicate for an extended period of time, avoid checking your email and performing any other tasks that might add or change documents on the duplicate that should instead be added or changed on your regular startup volume. If you do, those changes will be overwritten the next time you update your duplicate.

5. If you selected your duplicate as your startup disk in step 1, repeat the process to select your regular startup disk.
6. Choose Apple  > Restart (without pressing any keys this time) to start from your internal disk again. Once again (as in step 4), confirm that you’ve booted from the correct startup disk; if you accidentally keep using your duplicate, problems and confusion could arise.


Note: If you keep your duplicate drive connected (which you probably should, to facilitate scheduled updates), I suggest excluding the duplicate from Spotlight; otherwise, searches may lead you to files from your backup rather than your startup disk. To do this, go to System Preferences > Spotlight > Privacy and drag your backup drive into the list.

If your Mac does not start from the duplicate, go to System Preferences > Startup Disk, select the duplicate, restart, and again check to see that your Mac has started from the correct volume. (Be sure to set your startup disk back to its customary volume afterward!) If not, verify that the drive’s partition map scheme and format are correct (see [Prepare Your Hard Drive](#)) and try creating the duplicate again.

Perform a Safe Boot

When you perform a *safe boot*, macOS temporarily disables most low-level third-party software (plus several Apple products), disables login items (specified in System Preferences > Users & Groups > Login Items), clears certain caches that normally load at startup, and performs some additional checks and maintenance.

To perform a safe boot, follow these steps:

1. Restart your Mac by choosing Apple  > Restart.
2. As soon as your Mac begins restarting, press the Shift key and hold it down until the login window appears.

Your Mac will finish the startup process, which may take much longer than usual. You'll eventually see the words "Safe Boot" on the screen. After running any tests you have to do in safe mode, reboot normally.

Running Backups from a Duplicate

Ordinarily, you'll run your Mac from the duplicate just long enough to verify that everything worked correctly. But what if, while you're booted from the duplicate, your versioned backup software runs automatically? Won't that cause problems? Short answer: no.

Since a clone is an exact duplicate, your other backup software likely can't tell the difference between a clone and the original volume. It definitely can't tell whether you intend to continue running from the clone, or whether you might want to avoid backing up when you're running from the clone. So when your backups start again while you're booted from the clone, they'll typically pick up with any changes made to the clone. This is normally a good thing, because you might clone your drive in order to move to a bigger disk, replace a dead disk, or whatever, in which case you'll want the new disk to behave exactly as the old one did.

If you create or change files when running from the clone, your software should back them up, and if you later go back to using the original drive, it will notice that some things don't match. That might prompt it to rescan your disk and take some extra time to update your backups, but it won't delete those recently backed up files, so all your data should be safe either way.

Store an Extra Backup Offsite

No matter how many backups you have or how often you update them, they do you no good if they disappear along with your Mac—as they likely will in the case of theft, fire, or any other serious disaster. I urge everyone to take the precautionary step of keeping a second copy of their backups safely away from their Mac, preferably in another building altogether. You can do this with a second hard drive—or, more easily and economically, with a cloud backup service.

Which type(s) of backup should you store offsite? As you'll recall, the main purpose of a bootable duplicate is to get you back up and running immediately after a disk failure or other crisis, and it can't perform that function if it's offsite. So, although you're welcome to store an extra duplicate offsite if you like, I think of offsite storage as being more appropriate for versioned backups.

Use an Extra Hard Drive

If you purchase two or more hard drives, you can set each of them up the same way. Then, back up to one drive for a week, switch to the other one, and take the first offsite. Repeat this rotation every week or so, and you'll be safe in the knowledge that if you lose your first backup, a second one is still available that's no more than a week out of date.

Although you can use this process with just two drives, having three is more convenient (although, of course, more expensive). At any time, you'll have one drive (A) in use, your next-most-recent one (B) onsite, and your oldest one (C) offsite. When you rotate the drives, you bring your oldest one (C) back onsite and make it active, while taking what has now become the oldest drive (B) offsite—and so on.

The safest way to keep multiple backup drives is to set them up separately. Configure one drive with partitions for duplicate and versioned backups. Set up Time Machine (or another versioned backup app) and let it run; also create a bootable duplicate. Then disconnect the drive and repeat the entire procedure with a second drive. If you use Time Machine, you can configure multiple destination drives, and Time Machine switches between them automatically (see [Choose a Destination](#)).

If you use a Time Capsule, you can't just swap out its internal drive whenever you feel like it (it's a pain to do, and it voids the warranty). You can, however, keep your backups on an external USB drive connected to your Time Capsule and then swap *that* drive from time to time—perhaps reserving the internal drive for media sharing.

You may be wondering where exactly “offsite” could be in your case. Here are some suggestions:

- Your place of work
- A neighbor's or relative's home
- A storage unit
- A safe deposit box

Don't keep an offsite backup in your car (or your garage!), which is, if anything, more susceptible to damage and theft than your home. Heat and cold extremes in your car can also hasten data corruption. If you want as much security as possible with a trade-off of less convenience, keep the drive in a safe deposit box at your local bank.

Taking care of your media is just as important as making proper backups in the first place. If your backup disk is lost or damaged, it does you no good. So whatever else you do, be sure to store your backup media in a cool, dry place away from significant sources of light, static electricity, vibration, and other hazards (such as inquisitive pets or children). This may seem obvious, but it pays to remember that you're doing backups in the first place because your data is valuable—perhaps even irreplaceable.

Tip: For extra safety, when your media isn't actively in use, store it in a container that's rated fireproof for media.

iTunes Match, Apple Music, and Music Backups

If you want extra backup insurance for your music—or if you want to save space on your backup drives—Apple has a deal (or two) for you. As long as you're an iCloud member, you can pay \$24.99 per year for a subscription to iTunes Match. This service ensures that Apple's servers have a copy of every track in your iTunes library, and that you can download or stream those tracks at will, from any of your devices. (Although this works even with music you didn't purchase from the iTunes Store—including music you recorded yourself—Apple will store only 100,000 such tracks for you.) As a bonus, if the version of any matching track in Apple's library has a higher quality than what you already had, you can download the better version. Or, if you subscribe to Apple Music, you get all the features of iTunes Match at no extra cost, along with all the other Apple Music benefits.

Using iTunes Match or Apple Music in place of another online backup service means you'll save lots of time (and possibly money too), because in all likelihood Apple will already have copies of most of your music on its servers. Using it in place of local backups is riskier (in that you're relying solely on Apple's copy) but could save considerable storage space on your external hard drives.

The only real downside (if you can call it that) is that you must keep paying for one service or the other to maintain those copies of your music in the cloud. That seems to me like a pretty great deal, especially considering that iTunes Match and Apple Music are valuable for much more than backups of your music.

Use a Cloud Backup Service

A second (or third) drive can be expensive, and all that swapping and relocating drives can be a hassle. A different approach is to store your secondary backup online, using any of numerous cloud backup services that offer encrypted backups of large amounts of data at reasonable prices. The idea behind cloud backup services is simple: using either a

conventional backup app or proprietary software, perform backups as usual, but use secure internet file servers—rather than local or network volumes—as the destination.

To oversimplify matters, I think of cloud backup services as falling into two main categories: self-contained (meaning they supply their own software) and BYOS (bring your own software). These are my own, rather arbitrary labels, but I think they provide a useful way of slicing up the landscape.

HIPAA and Cloud Backups

In the United States, the Health Insurance Portability and Accountability Act (HIPAA) contains provisions governing the security and privacy of medical data. Similar regulations cover other professions in which the confidentiality of client data is crucial. I've heard it said that HIPAA rules out any sort of internet backup, but that is not the case. You just have to carefully follow the rules (for which, peruse [this handy 117-page PDF guide](#)).

One of the main stipulations is that all data must be encrypted at the source (that is, on your computer) in such a way that no unauthorized person can decrypt it. Some cloud providers use such an arrangement by default, some offer it as an option, and others don't do it at all. To take IDrive as an example, its default password setting would not be HIPAA-compliant, but you have the option to use a private encryption key, and doing so [appears to meet the HIPAA security standard](#). (Backblaze, sadly, is not currently HIPAA-compliant, even though it offers a private password or custom key.)

You must also observe requirements about longevity of data storage, traceability of changes, disaster recovery planning, and a number of other issues. Ensuring HIPAA compliance with cloud backups is not trivial, but it's absolutely possible. If you're bound by HIPAA or similar rules, be sure to check with your backup provider to confirm that it offers the necessary features and that your account has been configured in a HIPAA-compliant manner.

Self-Contained Cloud Backup Services

Oodles of online services offer backups for Mac users; see the [online appendixes](#) and my Wirecutter article [The Best Online Cloud Backup Service](#). Some of the most popular services are:

- **Acronis True Image:** [Acronis True Image](#) has a respectable set of features for storing versioned backups either on local drives or to the company's proprietary cloud storage. You can pay \$49.99 for a one-time purchase that includes no cloud storage; \$49.99 per year for a plan that includes 250 GB of storage; or \$99.99 per year for a plan that includes 1 TB of storage. (Multi-user licenses and additional storage are also available and are quite reasonably priced.) Among many other features, Acronis can back up your Facebook posts, store a copy of your *entire* disk in the cloud, and even restore an entire disk to a bootable state from a cloud backup. The catch is that this requires transferring more data than most home broadband connections can handle in any reasonable period of time. (And in any case, you can't boot from your duplicate in the cloud; you must first restore it to a local disk.)
- **Backblaze:** This service is my top pick, now that CrashPlan is off the table, and it's what I use for my own family. [Backblaze](#) charges \$5 per month or \$50 per year (per computer) for unlimited data storage. Setup is almost trivially easy, and I've found it to be speedy and reliable. By default, Backblaze backs up all your important files without requiring configuration other than entering your email address. It excludes system files and items in your `/Applications` folder, among others. You can adjust what's in and what's out in System Preferences > Backblaze. To restore files, you can download them (individually or as a ZIP archive) from the web or have Backblaze mail you the files overnight on an external hard drive. (In fact, the restore-by-mail option is effectively free; if you send back the drive after restoring your data, Backblaze refunds the cost of the service.)

Either way, a downside to Backblaze is that when restoring files, you must manually move them to where they belong; it won't put them

back in place automatically. Another potential downside for some users is that Backblaze's backups (and restores) mingle files from all the different user accounts on your Mac; if it's important to keep each user's data strictly private, that might be an issue. In addition, Backblaze stores old versions and deleted files for only 30 days, which is shorter than I prefer. And it fails to back up or restore some Mac metadata (such as ownership and permissions, creation dates, and Finder tags). But it's still, in my opinion, superior to the competition—and if ease of setup is your main consideration, Backblaze is the one to beat.

Tip: To learn about Backblaze's approach to security, see their page [How Backblaze uses Encryption to Protect your Data](#).

- **DollyDrive:** [DollyDrive](#), which I've also mentioned elsewhere in this book (see, for example, [DollyDrive](#) and [DollyDrive Tips](#)) is another app that includes options for both local and online storage; it also lets you sync files across devices and share files with other people. Monthly costs for unlimited Macs range from \$5 for 500 GB of data to \$25 for 2 TB, but there's also a plan for unlimited storage from a single Mac for \$6 per month, and discounts apply for one- and two-year subscriptions. Free seeding is also available.
- **IDrive:** [IDrive](#), the runner-up in my Wirecutter roundup, offers a maximum of only 2 TB of storage for backups (plus 2 TB more for file syncing), compared to Backblaze's unlimited storage. It also costs a bit more (\$69.50 per year, though with a discount for the first year). On the plus side, IDrive offers indefinite retention of deleted files (versus Backblaze's 30 days) and up to 10 old versions of each file, supports network volumes as source or destination, and lets you seed your initial backup (by mailing in a hard drive) for free. It even has an app that runs on some NAS models, enabling you to back up their data to cloud storage. I offer considerably more detail about the service in my [Wirecutter](#) article.

Note: All these services offer compression, encryption, and delta encoding for efficient uploads and secure storage. They also offer iOS apps with which you can view and download backed-up files while away from your Mac.

What About Cloud Storage and Syncing Services?

In earlier incarnations of this book, I included several other online services in this list, such as [Dropbox](#), [SpiderOak](#), and [SugarSync](#). Although these services have much to recommend them—including versioning, syncing files across multiple devices, and sharing files with others—I think it’s generally unwise to rely on them as *backup* services. You can read about my reasoning in the sidebar [Dropbox, the Almost-Backup Service](#), earlier. I do list many such services in the [online appendixes](#) for the sake of completeness, but I distinguish them from true online backup services like Backblaze.

If you decide to use one of these services for backups anyway, examine its features carefully; not all are alike. For example, as of early 2019, the popular Carbonite service offers versioned backups only for Windows users. Therefore, as far as Mac users are concerned, Carbonite is a nonstarter when it comes to backups.

BYOS (Bring Your Own Software) Internet Backups

The other category of internet backup services isn’t explicitly designed for backup at all; it’s just storage space that you can use in whatever way you want. To use it for backups, you must supply your own backup software, and in some cases additional software that enables your backup app to mount or otherwise interact with the storage space.

Although there are numerous services like this, I’ve chosen just a handful as examples:

- **Amazon Drive:** Amazon’s [consumer-oriented cloud storage service](#) costs \$59.99 per year for 1 TB of storage (a significant reduction from the *unlimited* storage it offered until mid-2017). Its performance doesn’t match some of the other options listed here, and given the reduced quota, the price is only average.

- **Amazon S3 and Glacier:** Amazon.com's [S3, or Simple Storage Service](#), provides virtually limitless—yet modestly priced—online storage, complete with encrypted transfer. S3 charges separately for data storage (rates start at \$0.023 per gigabyte per month for standard storage or \$0.0125 per gigabyte per month for “infrequent access” storage, and vary depending on where the data is stored), data transfer (\$0.09 per gigabyte downloaded after the first one), and requests, meaning operations that affect the data (prices vary depending on the request type; delete requests are free). Prices go down as volume goes up, and prices in Europe are slightly higher.

In any case, given Amazon's pricing structure for S3 storage, if you keep more than about 218 GB of data online, other services are more economical. As it turns out, even Amazon now offers a cheaper service, called [Glacier](#), with prices as low as \$0.004 per gigabyte per month—but the catch is that because Glacier is intended for long-term storage, it can take several hours to access files when you want to restore them.

Regardless of whether you use S3 or Glacier, getting at Amazon's online storage space requires both nontrivial setup and third-party software. The most popular tool to access your S3 or Glacier storage space from a Mac is [Arq](#); see [Arq](#) (including the note there about similar apps) and [Arq Tips](#).

- **Backblaze B2 Cloud Storage:** [B2](#) from Backblaze is storage only, without the backup app and service. The cost is a mere \$0.005 per gigabyte per month (in other words, 1 TB for \$5 per month), with the first 10 GB free. Because B2 is fairly new, only a few consumer-friendly Mac backups apps (such as Arq and Retrospect) support it so far, but more are surely on their way (and there are also command-line clients that work on the Mac).
- **Google Drive:** [Google Drive](#) costs the same as Dropbox for 1 TB of storage (\$9.99 per month), but you can also choose from among more tiers, with as little as 15 GB (free) to as much as 30 TB (\$299.99 per month). Although you can use many tools to back up

your data to Google Drive, Google offers its own [Backup and Sync](#) app that does exactly what its name suggests.

- **Google Storage Nearline and Coldline:** Google's answer to Amazon Glacier, [Nearline](#) costs slightly more at \$0.01 per gigabyte per month but doesn't make you wait hours to access your data. [Coldline](#), meanwhile, costs only \$0.007 per gigabyte per month but is designed for storage you don't need to access frequently or quickly. Like Glacier, Nearline and Coldline require third-party software—and once again, [Arq](#) is the natural choice if you want to use this online storage space to back up your Mac (see [Choose Another Versioned Backup App](#) and [Arq Tips](#)).
- **Strongspace:** This [online storage provider](#) offers several plans, starting with 15 GB for \$3.99 per month, up to 200 GB for \$18.99 per month. The service offers access via SFTP (supported by many Mac backup apps, although not by any of my favorites) or [rsync](#) (accessible via Terminal); the company now provides its own [free desktop software](#) for Mac, too.
- **Wasabi:** A relative newcomer, [Wasabi](#) costs as little as \$0.0039 per gigabyte per month (which translates to \$3.99 per month for 1 TB), making it the least-expensive option currently available—just a hair less than Amazon Glacier—but with considerably better performance than even the standard S3 service. Because it uses the same API as S3, it's compatible with any backup app that can use S3.

Before you settle on one of these providers (and especially before you start uploading terabytes of data), be sure to read the fine print of its terms of service carefully. Some of these services limit your upload rate (typically after you've uploaded a certain amount of data or a certain number of files), meaning it could take a surprisingly long time to back up and restore your data. Although price does not strictly correlate to performance, some of the less-expensive services yield slow effective transfer speeds that may significantly reduce their perceived value.

Cloud Backup Services: Pros and Cons

On the plus side, cloud backup services keep your files safely offsite with absolutely no effort on your part—and they do so for every backup you perform with your cloud backup software, not merely on a weekly (or “whenever I remember”) basis. They also encrypt your files and usually make their own redundant, offsite copies of your data. If you’re unable to conveniently store a set of backup media outside your home or office, an internet backup service can make that process painless. Even if you do maintain diligent offsite backups, an internet backup service can provide extra insurance for particularly important files.

Turning to the cons, these services are no substitute for duplicates; you’ll still have to maintain those locally yourself. And with cloud backups, the biggest issue is usually speed: even with a fast broadband connection, you could easily spend weeks doing an initial full upload of a moderately large disk, and of course restoring files may also be quite slow. So you may want to limit the files you back up online—perhaps only the contents of your home folder, or even just your `~/Documents` folder. (Alternatively, choose a service such as DollyDrive or IDrive that lets you seed your initial backup by sending them an external hard drive.) Finally, you may need to think about monthly data caps and other restrictions your ISP may have on how you transfer data. Check with your ISP to confirm that using an online backup service won’t run afoul of their policies.

For all these reasons, most people should consider internet backup services as a supplement to conventional backup methods—a convenient way to get offsite storage—not as a replacement for local backup media.

As I said earlier, I use Backblaze for my family’s backups. It’s not perfect, and I do miss some features I formerly had in CrashPlan for Home, but all things considered I think Backblaze is the best choice for most people right now.

What If Your Data Is Already in the Cloud?

In this chapter I've discussed backing up data from a Mac to storage in the cloud. But increasingly, the data we care about is never stored locally in the first place. Services such as Google Apps, Microsoft Office 365, and web-based email services enable you to create and store information in the cloud using nothing more than a web browser. But you may still want to back up that data—to local storage, a different cloud provider, or both. I discuss this further a bit later, in [Back Up Data from the Cloud](#).

What to Do When Disaster Strikes

You've diligently performed the backups recommended in this book, and then, one fateful day, disaster strikes. It might be a small disaster (one important file is missing) or a large one (your whole computer is missing). In any case, the very first thing you should do is take a deep breath and remind yourself that everything is going to be fine. Once you're finished not panicking, proceed with the instructions here, depending on the nature of your disaster.

Restore Individual Files

The easiest problem to recover from is a small number of files that are missing, or for which you need an older version. Follow these steps:

1. If you backed up the files using Time Machine, try restoring them using the steps in [Restore Data with Time Machine](#); or, if you used another versioned backup app, follow the developer's instructions (check the Help menu) for restoring your files.
2. If the files are missing from your backup, check your bootable duplicate. Connect the drive (if it's not already attached) and navigate to the location on the disk where the file should be. If it's there, copy it to your main disk.
3. If steps 1 and 2 don't work—for example, if your entire backup drive is missing—move on to your secondary backup. That may mean fetching an extra backup drive from another location and following steps 1 and 2 again, or using your internet backup app to find the file in your online backup.

Warning! If you need to restore data from a photo management app (such as Photos), virtualization software, or any app that uses a database-like structure, restore the *entire* data unit (photo library, virtual machine, or whatever) rather than individual files within it, or data corruption may result. You might prefer to restore these from a duplicate; see [Duplicates of Non-Boot Volumes](#).

Restore the Data, Not the App

I can't tell you how many times I've heard someone say, "I've lost my data from App X, so I want to restore the *app* from my backups. How do I do that?" I always reply that restoring the app is the wrong thing to do.

Nearly all apps—even those, like Contacts, Calendar, and Photos, that aren't based on documents—store their *data* separately from the *app*. If information is missing or crashes occur, chances are virtually nil that the app itself is broken, and restoring it won't bring back your data.

Instead, figure out where the app stores its data (a quick Google search can often help) and restore those files. If that doesn't work, try restoring the app's preference file(s) too.

Use Your Bootable Duplicate

In some situations it's clear that your problem is worse than a few missing files. If your Mac won't start up—it gets stuck at a blue or gray screen or displays a flashing question mark icon—turn next to your bootable duplicate. Also use your duplicate if many files seem to be missing or damaged, apps won't launch, you're unable to start the Mac using macOS Recovery, or it exhibits other similar system-wide misbehavior. Follow these steps:

1. Attach the drive containing your bootable duplicate. (Remember, it must be directly attached to your Mac; you can't boot from a duplicate over a network.)

Note: As a reminder, if you have a newer Mac with a T2 chip ([see full list here](#)), before you perform step 2 you must [follow these instructions](#) to reboot in macOS Recovery, choose Utilities > Startup Security Utility, and select “Allow booting from external media” under External Boot. Then restart your Mac. (You should *not* change the Secure Boot setting, however.)

2. If your Mac is already running, restart it; if not, turn it on. Immediately (or as soon as it begins restarting) press and hold the Option key.
3. When your screen shows the volumes available for booting your Mac, release the Option key, use the arrow keys to select your duplicate, and press Return. Your Mac should boot from the duplicate—but be aware that this may take considerably longer than booting from your regular internal startup disk. (And if your backup drive uses a slow interface, such as USB 2.0, it will take longer still.)

Once your Mac finishes booting, you can continue working from your duplicate if you want to. But if possible, you should check your internal drive and repair it.

4. Run Disk Utility (in [/Applications/Utilities](#) on your duplicate). Select your internal disk in the list on the left. In the First Aid view, click Repair Disk. Disk Utility attempts to fix the disk. If it succeeds, you can restart your Mac right away, and you’ll automatically go back to using your internal disk. If Disk Utility is unable to repair the disk, you have three options:
 - ▶ Try a third-party disk repair utility, such as Alsoft’s [DiskWarrior](#). (Note that as of publication time, DiskWarrior is not yet capable of rebuilding APFS volumes, which are used for all boot volumes under Mojave and for SSD boot volumes under High Sierra, but the developer is working on adding full APFS support.)
 - ▶ Erase the internal disk and then reverse the duplication process.
 - ▶ Restore your entire disk using Time Machine (or another backup app, if you made a versioned backup of the entire disk).

If you decide to take the second route—restoring your disk from a bootable duplicate—read on for instructions. For help restoring an entire disk from a Time Machine backup, refer back to [Restore a Disk Using Time Machine](#).

Restore a Disk from a Bootable Duplicate

If your internal hard drive has become so badly damaged that it can't be repaired by disk utilities—or if your hard drive, or your entire Mac, had to be replaced—your best bet is to erase the damaged drive and then restore its entire contents. Although you can restore your disk from a Time Machine backup, the process usually takes a very long time—and of course it won't include any files you excluded from Time Machine. A better tactic, assuming you have a functioning and up-to-date bootable duplicate, is to restore your disk from the duplicate.

To restore the contents of your bootable duplicate to your internal disk, follow these steps:

1. Follow steps 1–3 under [Use Your Bootable Duplicate](#) (just previously) to start up from the duplicate.
2. Open Disk Utility (in [/Applications/Utilities](#)).
3. Select your computer's internal disk in the list on the left.
4. In the Erase view, click Erase, and confirm that you really want to do that. Disk Utility erases the disk.
5. Follow the steps in [Create and Use a Bootable Duplicate](#) to copy the contents of your duplicate back onto your internal disk—but in this case, choose the external disk containing your duplicate as the source and your internal disk as the destination.
6. When the restoration is complete, restart from your internal disk.
7. Allow data (particularly files you added or modified since you last updated your duplicate) to sync from the cloud using services such

as iCloud Drive, iCloud Photo Library, and Dropbox; this reduces the number of items you'll need to find in your backups. (See [Can Cloud Sync Simplify Backups?](#))

8. If you have further files to restore that weren't synced from the cloud, and your versioned backup software (Time Machine or otherwise) ran after the most recent update of your bootable duplicate, you may want to use that software now to copy any new or changed files back to your main disk. Unfortunately, most backup apps (including Time Machine) have no way to select only files that changed *after* a specified date and time—namely, those that changed and were backed up after you last updated your bootable duplicate. See the sidebar [Finding Recently Backed-Up Files](#), ahead.

After you restore a bootable duplicate in this manner, Time Machine may conclude that all the files on your disk have changed and try to create an additional copy of all of them. Read the sidebar [Restarting Time Machine Backups After a Restore](#), earlier, for more details and a possible solution.

Recovering from the Loss of a Backup Drive

What if you had just one drive with a bootable duplicate and versioned backups—relying on a cloud backup service for a secondary backup—and you lose both your internal drive and your external backup drive? Restoration is harder, but still possible.

On a new or freshly erased drive, (re)install macOS, setting it up with the same username and password you used previously. Next, install your key apps from the Mac App Store, discs, or downloads—and be sure one of those apps is your internet backup utility! Use that utility to restore the files from your online backup. This can take quite a while, but as long as you stored the entire contents of your home folder online, the end result should be a restoration of your system to nearly the state it was in previously.

Finding Recently Backed-Up Files

Most backup apps let you easily find and select the most recent version of any file—or the last version backed up *before* an arbitrary time—for restoration. But what if you want to restore only the files that were backed up *since* an arbitrary time? If you’ve restored your disk from a bootable duplicate and want to put back all the files that your versioned backup copied after that duplicate was last updated, that’s surprisingly challenging to do. Here are some tips:

- ✦ If your backup app lets you search your backups by modification date, you might be able to use that as a substitute. Look for all files *modified* since your last duplicate; even though that’s not the same as when they were backed up, it stands to reason that if files with a later modification date are stored in your backup, they were backed up after they were modified!
- ✦ If your backup app stores files in a Finder-readable format, use Spotlight’s advanced search features to specify that “Last modified date is after” is the date when your duplicate was last updated. (See [Using Finder’s Advanced Search to Find Recently Modified Files](#) by Jim Tanous of the Mac Observer for instructions.)
- ✦ If all else fails, you’ll have to search manually through your backups for files you might have changed recently. The most likely locations are your [~/Desktop](#), [~/Documents](#), and [~/Downloads](#) folders, but you may have to look around elsewhere.

Manage Your Media

For many people, a backup drive may sit on a desk for years, quietly doing its thing without any intervention. For others, two or more drives may be shuttled between locations to provide offsite storage. But in either case, your backup drive (or other media) won't last forever. So, in this brief chapter, I look at [What to Do When Your Disks Fill Up](#) and explain why you should [Consider Long-Term Archive Storage](#).

What to Do When Your Disks Fill Up

Your bootable duplicates and versioned backups should continue updating themselves happily for some time. But sooner or later, the drives you use for backups will fill up. (Whether this takes a few months or a few years depends on the rate at which you accumulate new data and the size of your backup disks.) When this happens, you have two options: buy new drives and start over, or recycle. By “recycle” I don't mean throw your drives in a blue bin; I mean erase them and reuse them for a new set of backups.

One argument for starting fresh is that new drives are virtually always more reliable than old ones. Another is that you can save your old drives as a long-term archive, in case you need to see what you backed up a few years ago (assuming the drive continues to work after all that time). On the other hand, recycling media saves money, not to mention physical storage space. And most people have little need for backups stretching back more than a couple of years.

The choice is entirely yours, but I can give you some tips either way.

If You Recycle Old Backups

For versioned backups, you may want to recycle your drives on a regular basis, *before* they fill up. By periodically erasing them and starting over with a full backup—instead of relying indefinitely on

incremental additions since a single full backup long ago—you reduce the risk of data loss due to file corruption or misbehaving backup software. How often you recycle your media is up to you, but in general I'd suggest recycling every one to two years.

Do, however, be aware that when you recycle media, you lose all the versioned backups stored since you started that particular cycle. In addition, if you recycle more than one set of media (for example, two or three hard drives), stagger them: do one, wait a week or two, then do the next one, and so on. That way, if you suddenly discover that you've erased the media containing an old file you need, you'll still have a chance to recover it easily from another set of backup media.

For bootable duplicates, as long as there's enough free space on your destination disk, you can simply erase the disk and start over from scratch. But if you're running out of space on the disk or partition you use for duplicates, then your only options are to repartition the drive—either expanding the partition for duplicates if there's enough room or repurposing a multi-partition drive as a single-partition drive—or to erase the disk, use it for something else, and buy a new, larger drive to use for bootable duplicates from now on.

Tip: If you're erasing a disk anyway, this is a good time to reassess partition sizes (see [Decide on Capacity](#)). If your disk or home folder is significantly larger than before, consider changing the partition sizes to better accommodate your current needs.

If You Archive Old Backups

When you see that your backup media is close to being full—or when your drive's warranty has run out and you start losing faith in it—you can set it aside, buy new drives, and start new sets of backups.

Unfortunately, as I discuss just ahead in [Consider Long-Term Archive Storage](#), hard drives make a poor choice for long-term storage (though an older hard drive that you wouldn't trust for backups may be fine for casual, noncritical uses). In other words: yes, do buy new drives, but

don't put too much faith in being able to retrieve backups from your old drives years from now.

If, when it comes time to erase your drives, you still want to maintain a copy of the old data, use your backup software to duplicate your versioned backups and bootable duplicates onto your new (and presumably larger) disks, effectively keeping a single backup lineage intact.

Securely Deleting Old Backups

When it's time to replace a hard drive completely, you may consider giving away or selling your old drive. Before doing so, be sure to *securely* erase it so that its new owner cannot use a file recovery app to retrieve all your data! Merely dragging files to the Trash and emptying it will not erase the data in such a way that it cannot be recovered.

In Yosemite and earlier versions of OS X, Disk Utility had a feature that let you overwrite a disk one, three, or seven times to be sure its data is completely unrecoverable. That feature disappeared in El Capitan and is unlikely to return, because the design of certain SSDs makes this feature unreliable; even if you think you've securely erased everything, some of your files might be recoverable. A number of third-party utilities can still securely erase individual files or folders, overwrite the contents of an entire disk, or both. However, I'd consider them safe only for hard drives, not for SSDs. [ShredIt X](#) is one example of a versatile (if slightly pricey) tool that can securely erase both files and the empty space on a disk.

Consider Long-Term Archive Storage

Whether you keep a single backup drive in service for many years or periodically move your data to new drives (see [If You Archive Old Backups](#), ahead), you should give some thought to the longevity of your storage medium. Over a period of years, the data on a hard disk can degrade even if the drive hasn't been used at all, as the particles on the platters lose their magnetic charge.

In fact, all digital media degenerates over time; although the physical process and expected lifespan vary, optical discs (such as CD-ROMs and DVDs), digital tape, and even flash memory can lose data over a period of years. To be sure, “archival quality” media exists, with claims that it will preserve data for a century or more. (For example, the makers of [M-Disc](#) media claim it will last for 1,000 years.) But no one knows for sure, because it hasn’t been around that long yet. And besides, any optical technology you use today might be incompatible with the Macs you have in the future.

As long as you periodically move your active backup data to new media (or restart your backups on fresh media) every few years or so, you shouldn’t have to worry about media degradation. But if you want to keep archives of data that’s no longer on your computer (and no longer being backed up actively)—and especially if you want that data to be readable decades in the future—you should take special care with it. Here are some suggestions:

- If you store your archives locally, then whatever media you use for them, store it in a cool, dry, dark place. At least once every five years, copy the archives onto new media.
- Alternatively, consider using a cloud service for long-term storage. Cloud services such as Backblaze make redundant copies of your data, monitor data integrity and drive health, and routinely upgrade hardware as necessary. Of course, you’ll pay for this service, but it’s a more reliable way than local storage to ensure that your data continues to be readable for a long time to come. You can save money by using an *archival* cloud storage service such as Amazon Glacier; see [BYOS \(Bring Your Own Software\) Internet Backups](#).
- Regardless of how you store your archives, verify them (by restoring a few random files) at least once a year.
- If you intend for your data to outlive you, make sure your loved ones know where your archives are stored, how to access them, and how to maintain them. For much more on this topic (including what data to preserve for posterity and how to go about it), see my book [Take Control of Your Digital Legacy](#).

Ultra-Long-Term Archival Storage

Because hard drives, CDs, DVDs, and other conventional media can degrade over time, they're not good choices for truly long-term archives (as in, data you want to be accessible decades or centuries from now). If you're looking for a way to make sure your great-great-grandkids can still access your data, you may be in the target audience for a storage medium called a *nanoform* from [Fahrenheit 2451](#).

A nanoform is a sapphire disc (two inches or four inches in diameter) capable of holding up to 2,500 documents or photos. They aren't stored as ones and zeroes, though; they're laser-engraved. So you (or future generations) can read the contents of the disc with a microscope or a strong magnifying glass. The nanoform is nearly indestructible—fireproof, waterproof, and impervious to magnetic fields. And since magnifying glasses will always exist, they're future-proof, too!

The only catch is the cost: about \$2,400 for the four-inch nanoform, or \$2,100 for the two-inch model. But then, you may consider that a small price to pay to guarantee your data's immortality!

Consider Special Backup Needs

Although duplicates, versioned backups, and offsite storage cover most situations the typical user will encounter, some people have special backup needs that don't quite fit the mold.

I'm thinking, for example, of users with vast numbers of digital photos and those who [Deal with Huge Volumes of Data](#) because they work extensively with the gigantic files required for digital video or pro audio apps. In other special cases, you may need to [Back Up While on the Road](#) (especially photos) or [Back Up Windows Files and Volumes](#).

Each of these situations may require additional steps beyond conventional duplicates and versioned backups.

Back Up Digital Photos

If you have no more than a few gigabytes of photos on your Mac, you can back them up along with the rest of your data and not take any special steps. But the ease of snapping photos and videos with an iPhone or iPad—and the increasing resolution of files from iOS devices and DSLRs alike—has increased the likelihood that a Mac user's photo library will extend to tens or even hundreds of gigabytes (my own is over 150 GB—yikes!). With the growing number and size of your images, you may find that duplicates and versioned backups alone don't meet all your backup needs.

Luckily, numerous tools, services, and strategies exist for the express purpose of making photo backups as painless and secure as possible. Consider these options in addition to (or, if you prefer, instead of) duplicates and versioned backups.

iCloud Photo Library

If you manage your photos with Apple's Photos app, you can take advantage of iCloud Photo Library to store copies of your photos offsite. It's not *exactly* a backup, but it provides at least some protection for your photos. (If you don't use Photos, there's nothing to see here; move along to [Photo Sharing Services](#).)

The basic idea of iCloud Photo Library is that *all* your photos and videos from Photos sync to Apple's servers, and from there to *all* your other Macs and iOS devices. Although that sounds both simple and wonderful in theory, in practice it's an odd and confusing process. I spell out all the details in my TidBITS article [iCloud Photo Library: The Missing FAQ](#).

You'll have to pay for storage above 5 GB of data, though prices are roughly in line with most online storage and backup services. It's probably worth it for the convenience of having the same photos on all your devices, not to mention easier sharing.

But even though iCloud Photo Library stores copies of all your photos in the cloud, it's not quite the same thing as an online backup. The difference is that if you delete or modify a photo on one device using iCloud Photo Library, that change propagates to all your other devices. (In this sense, it's a bit like IMAP email: the server holds the master copy of each item, until the client says to delete it; then it's deleted from all clients.) You do get 30 days to recover anything you accidentally deleted, but that's not much of a safety net. If you realize on day 31 that you deleted a photo you need, you're out of luck. With conventional backups, by contrast, you can usually decide how long backups are kept (which can be indefinitely).

Even so, if you can afford the storage (and the bandwidth—iCloud Photo Library transfers an enormous amount of data), it's not a bad idea to use it as a *partial* solution to photo backups.

Photo Sharing Services

If iCloud Photo Library isn't for you (or if you want to supplement it with a service that makes it harder to lose your photos), there are many alternatives. Numerous services provide *unlimited* storage for your digital photos, along with complete control over which ones are shared and with whom, sometimes for as little as zero dollars! Beyond the basics of photo storage and sharing, such services differ in the selection of features they offer. Most offer prints of your digital photos for a fee; some will send you CDs or DVDs with backups of your photos, too.

Because the choices (and details such as prices and storage space) change so frequently, I've put information on photo sharing services in the [online appendixes](#), where I can more easily keep it up to date.

The main catch with these services is that you'll give up integration with Photos (assuming Photos is your preferred photo cataloging app). Some of them work together with iPhoto or Aperture; some don't. Another catch (as with iCloud Photo Library): you'll need a robust broadband connection with plenty of bandwidth and a generous monthly data allowance.

If you can pass those hurdles, then considering that you can back up *all* your photos at little or no cost using sites of this sort, it's almost a no-brainer. Although you may already include your photos in your duplicates and versioned backups, another offsite backup never hurts—and you'll get easy photo sharing as a bonus.

Cataloging Software

Apple intended for Photos to replace iPhoto and Aperture, although at the moment there's no compelling reason to switch if you're happy with iPhoto or Aperture. In any case, both Photos and iPhoto are consumer-level apps that weren't designed for professionals—or for amateurs who have tons of photos and take their images seriously—and Aperture, for all its virtues, has no future. When your photo management needs outgrow Photos or iPhoto, you'll need to look elsewhere for serious image-cataloging software.

For macOS, you have two main choices (apart from high-end client-server packages):

- [Adobe Photoshop Lightroom CC](#)
- [Phase One Media Capture One](#)

Note: Lightroom CC comes in two versions: a new, cloud-centric version and Lightroom Classic CC. Both are included in Adobe's Photography Plan subscription. To learn more about the new Lightroom CC, read Jeff Carlson's [Take Control of Lightroom CC](#).

Although these apps aren't free like Photos, they offer flexible searching, contact sheet creation, and much more. Crucially for our purposes, they maintain thumbnail catalogs of all your images even if you move the original files to a different volume (and even if that volume happens to be sitting at the bottom of a pile of junk in your closet).

By using one of these apps to back up your photos—whether or not you delete the originals—you gain the ability to search a visual index for your images. When you find the one you want, the software will tell you which hard drive, DVD, or CD it's stored on. (With the new Lightroom CC, cloud storage is also an option; in fact, it's the preferred destination for your photos.)

If you choose one of these tools, you could potentially exclude photos from your regular versioned backups and use the cataloging software's built-in backup tools for your photos instead—though extra backups, especially of your photos, can never hurt. If you use cataloging software to back up your photos (instead of, or in addition to, other software), it will dramatically increase the ease with which you can find and restore them. You can also, optionally, delete older photos from your disk after you've backed them up, saving room on your startup volume while still maintaining a handy catalog of thumbnails.

Deal with Huge Volumes of Data

Some kinds of data are inherently quite voluminous, and therefore have special implications when it comes to backup. I'm thinking primarily of video, audio, and high-resolution photo data, which are often stored on external hard drives or RAIDs with more capacity than a Mac's internal storage. (If you store this data on a NAS, also see the next topic, [Back Up a NAS](#).)

Video files consume an enormous amount of disk space, and when you're editing a large video project, the file sizes can become truly staggering, especially with 4K, 6K, and 8K video. Because of the sheer quantity of data you may generate, conventional duplicates and versioned backups may not make the most sense. You're also likely to create numerous intermediate files between the raw footage and the final product, and deciding whether or how to back up that data can be challenging.

All this is equally true if you're working in audio production, especially if your Mac functions as a multitrack recorder. It also holds for photographers working with gigantic, ultra-high-resolution images and for several other categories of user.

So, if you frequently generate more than a few gigabytes of new or modified files in a single day, read on for my recommendations.

Video Backup Strategy

If you regularly edit video on your Mac, you may need to adjust your backup strategy to account for these jumbo-sized files.

Video Data Types

Think about the different forms video data may take:

- The raw files you copied from your camera, camcorder, or iOS device onto your Mac.
- A project (in, say, Final Cut Pro or iMovie) containing a selection of video files plus the information about how they fit together—not to

mention music, narration, special effects, and so on. In the case of Final Cut Pro, this also includes video and audio cache files, which could be on a separate, connected disk.

- A final, rendered movie, in one or more sizes and formats (DVD-ready, web-ready, and so on). Needless to say, a given project may be “final” and still undergo changes later!

Which of these should you include in your backup plan—and how?

- **Raw files on your disk:** Your original footage (or, rather, the original footage you’ve moved from your camera, camcorder, or iOS device to your Mac) is especially valuable. You can always re-edit video if necessary, but having to reshoot something from scratch may be inconvenient, if not impossible. So, I suggest archiving it—at least until your project is finished—by copying it to extra hard drives and then putting those drives in a safe place away from your Mac. If you expect to come back to it much later, using a cloud archiving service such as Amazon Glacier (see [BYOS \(Bring Your Own Software\) Internet Backups](#)) might be smart.

Assuming you create such archives, you should exclude these files from your normal versioned backups and bootable duplicates, to save time and storage space.

Tip: If your camera or camcorder stores its data on inexpensive, removable media such as tape or DVD, *always* keep the original media. Don’t overwrite it for your next project; instead, treat that media as though it were a film negative and store it in a safe place. You’ll use up more media this way, but you’ll have an automatic backup of all your footage.

- **Project files:** The project files are perhaps the most challenging component, because you may modify them many different times. If you include these files as part of a standard versioned backup, you may find (depending on which video editing and backup software you use, and several other variables) that even a tiny change to a 20 GB video project results in the *entire* 20 GB file being *added* to each day’s backup.

So I suggest storing backups of your in-progress project files independently of your other backups. If the storage requirements are ridiculous (as they may be), consider saving only a week's worth of versions and then deleting older ones to free up space. Once you've completed your feature film (or this year's holiday DVD) and sent it off to the distributor (or your family), you're unlikely to need all the intermediate versions of the project files again—though you may still want the *final* project files later.

Tip: Choose backup software that offers compression and/or delta encoding to make the most of limited storage space, and use physical media for offsite copies. Use fireproof, waterproof, theft-resistant storage devices for your local backups. (See my TidBITS article [Do Bulletproof Backups Require a Disaster-proof Drive?](#).)

Warning! When restoring projects from a backup, all components—including the raw video clips, the project settings, and any additional graphics or audio—must be returned to their original locations. In addition, it's best to restore an entire project at once, not just individual files, lest your video editing software get confused and turn your project into a work of abstract art (and not in a good way).

- **Final, rendered movies:** When you've finished a project and know you won't be editing it again in the near future, copy all your project files to inexpensive, archival cloud storage or archive them onto a spare hard drive—preferably using two or more drives that you'll store in separate places. Then delete the project files from your regular disk and recycle your video backup disk by erasing and starting over again with a full backup of your next project.

In other words, treat your video data with the same care you give all your other files, but don't get hung up on long-term storage of every single edit you make of every movie. The most important things to back up are your original footage, versioned backups of projects currently in progress, and your final project files.

Strategy for Other Large Files

Although video files tend to be the largest, and therefore the most challenging to back up, large audio and photo files (and perhaps others) have similar issues. Rather than lay out details for every sort of data as managed by each of the many audio and photo processing apps out there, allow me to offer some general guidance.

Set Cost and Storage Expectations Appropriately

Although you can reduce storage requirements for your backups somewhat using apps that offer file compression and/or delta encoding, you can't escape the fact that larger amounts of data require larger amounts of backup media. That's going to cost money, and, especially in the case of network backups, it's going to take significantly longer for each backup run. (For truly huge files, cloud backups are often a nonstarter unless you have bandwidth to burn.)

Keep Copies of Your Original Files

Raw audio recordings, your unedited photos as they came off your camera's memory card, and other original files are especially important. Everything else you do (editing, mixing, applying adding effects) *could* be done again, however time-consuming it may be, but original audio performances or photographs can never be recreated in exactly the same form.

Of course, you don't have to (and shouldn't) keep these forever *on your disk*, but at the same time it doesn't make sense to overwhelm your regular versioned backups. Instead:

- Exclude these files from the versioned backups you update daily (in Time Machine or another versioned backup app).
- Invest in an extra hard drive or two just to hold these archived files. Alternatively, if you have an optical drive, you could copy these files onto DVD or Blu-ray discs (this is a rare exception to my advice to avoid optical media), store multiple copies in a safe place, and refresh your copies from time to time (see [Consider Long-Term Archive Storage](#)). In either case, delete the copies on your disk when you're done actively working on them.

Back Up Active Projects

For projects that are in an intermediate stage between raw media and final product, be sure you have regular backups:

- Include all these files in the regular duplicates of your disk(s), because the amount of space required for your duplicates isn't cumulative as it is for versioned backups.
- As with video, choose versioned backup software that offers compression and/or delta encoding, both of which can help you make the most of limited storage space.
- Do create versioned backups of the files, too, but consider keeping these backups on a drive separate from your other data to prevent your regular versioned backups from ballooning out of control. In other words, in your ordinary versioned backups to Drive A, exclude the folders with your audio or photo data, and in a separate set of versioned backups stored on Drive B, include *only* your audio or photo data. It may help to write a checklist for yourself to keep track of what's where!
- When you're finished with a project, delete most or all its intermediate stages from your "big-files-only" backup, leaving just the final stage.

Unfortunately, I know of no magic bullet to make backups of large files completely painless and affordable, but these tips can help you minimize the aggravation.

Back Up a NAS

So far I've talked about NAS devices (see [Network Storage Devices](#)) only as a potential *destination* for your backups. However, if you also use a NAS as primary storage (that is, as the main or only location for certain kinds of data), you also need to think about backing up the NAS itself. Some people, for example, like to use a NAS (instead of a computer) to store photos, music, and videos for the entire family. If the

data on the NAS isn't a copy of something already stored somewhere else, it's every bit as vulnerable to data loss as anything on your Mac.

The wide variety of NAS devices makes it impossible for me to offer specific advice here—what works on one model won't work on another, and what's reasonable for a small NAS with a single drive might seem absurd for a multi-drive NAS holding tens of terabytes. However, I would like to offer some general guidance.

First, to state the obvious, you'll need a storage destination with at least as much capacity as your NAS currently uses (and more is better, to allow room for growth). So, if your NAS has 4 TB of data, you'll need at least 4 TB of additional storage to back it up. That could be, for example:

- **An external hard drive or RAID connected to your NAS:** Most NAS devices have ports (typically USB 3 ports) that support external storage.
- **A second NAS:** In some cases, you can set up a NAS-to-NAS backup that takes place without involving any of your computers.
- **Your Mac:** Although you *can* back up a NAS to your Mac's internal or external drive, that strikes me as an odd thing to do, in that the main reason for using a NAS in the first place is to have a large, independent storage space for your data that doesn't rely on your Mac.
- **A cloud destination:** You may be able to back up your NAS to a cloud storage or cloud backup service, just as you can do for your Mac. Although this will be time-consuming and bandwidth-intensive, it provides an offsite copy of your data, whereas a NAS-to-drive or NAS-to-NAS backup won't help you if your house burns down or if someone steals all your equipment.

Note: Some NAS devices that support multiple internal drives can be configured such that one drive backs up to another, but I think that's an unsafe option, for exactly the same reasons that I recommend against backing up your Mac's startup volume to a different drive inside the same Mac—you're putting all your digital eggs in one basket.

All of the above options assume that the NAS includes, or permits you to install, software that runs on the device itself. This is true more often than not—most NAS devices are essentially headless computers, running their own simplified operating system. However, it isn't *always* true; for example, Apple's AirPort Time Capsule can be considered a NAS but it offers no way to install or run software on the device itself. As long as your NAS can be mounted as a network drive on your Mac, any Mac backup software that supports network drives as sources should be able to back it up.

Assuming, however, that you want backups to run directly from your NAS, how can you know if your NAS supports backup software, which destinations you can use, and how to set it up? Look at the documentation that came with your NAS or consult the manufacturer's website. Here are a few examples of instructions for backing up popular NAS models:

- [NETGEAR ReadyNAS](#)
- [QNAP Turbo NAS](#)
- [Synology NAS](#)

Back Up Data from the Cloud

In this book, I've assumed that the data you want to back up is stored locally on your Mac (or a nearby device) and that the backups will go onto local media, into the cloud, or both. But what about all your data that starts out in the cloud? If you use a web browser to access your email, Google Docs for creating office documents, or any of numerous other web-based apps for creating and storing data, you're relying

entirely on that one service to maintain its own backups of your data. That process may be invisible to you and out of your control, leaving you with no recourse if your data should ever disappear.

In some cases, you may already have local copies of your online data without realizing it. For example, if your email account uses IMAP or Exchange and you access it using an app such as Mail, Thunderbird, or Outlook, you can have a complete local copy of all your server-based email messages as long as you have your settings configured properly (in most cases, your email client's default settings are exactly what you want). The same goes for cloud-based contact and calendar data accessed using apps such as Contacts and Calendar. But these sorts of services are the exception. Any data you create or edit in a web browser most likely has no local copy.

A number of cloud providers can back up data from any of several cloud-based services (such as Google's various offerings, Office 365, and Dropbox) to a completely different cloud service (cloud-to-cloud backups), to local storage (cloud-to-local backups), or both. Here are a few examples, which mostly (except as noted) require monthly or annual subscription fees:

- [Backupify](#) is mainly geared toward business users of Google Apps. It backs up Gmail and Google Drive, plus Google Calendar, Contacts, and Sites, to proprietary cloud storage. It also backs up data from Salesforce and certain types of Office 365 accounts.
- [CloudAlly](#) has backup plans for Office 365, Google G Suite, Box, and IMAP, plus other, more business-oriented cloud services such as SharePoint and Salesforce.
- [cloudHQ](#) takes a somewhat different approach by syncing data between cloud services such as Google Apps, Amazon S3, Dropbox, Office 365, and Evernote in any combination you choose. If you sync to a service such as Dropbox that already mirrors your data locally, you get both cloud-to-cloud and cloud-to-local backup automatically. A free tier works with a limited set of services.

- [CloudPull](#) backs up your Google data, including Google Drive and Gmail, to your Mac. Although you'll pay for the software, since you're using your own Mac for storage, you won't pay a monthly fee. For more information, read [Back Up Your Google Data with CloudPull](#) by Adam Engst.
- [Mover](#) can connect any of more than a dozen cloud services with each other for backup and sync. Among those services are Box, Dropbox, and Google Drive. Pricing starts at \$20 for a one-time migration of up to 20 GB of data.
- [MultCloud](#) is designed primarily to aggregate and sync the data from various cloud providers (such as Dropbox, Google Drive, and Amazon Drive—but *not* iCloud Drive). This is an approach to cloud storage that I consider fundamentally flawed. However, MultCloud does include a genuinely useful feature: the capability to back up data from one cloud provider directly to another, without having to use your Mac as an intermediary. A free version has limited functionality; the paid Premium plan adds unlimited data traffic and the option to schedule transfers.
- [Spanning Backup](#), another business-oriented service, backs up G Suite, Office 365, or Salesforce data to cloud storage.
- [Unclouder](#) is a one-trick pony: it creates an extra backup, on your Mac's disk, of the data stored in iCloud Drive. Because these backups are manual and don't sync with the cloud, they protect you against loss of data from iCloud Drive on all your devices due to user error or problems on Apple's end.

Do you need one of these services? I wouldn't subscribe just for Gmail or Office 365 mail, because it's easy and free to use IMAP to store a copy of all your email on your Mac and then back your email up with the rest of your data. As for other cloud-based data, it depends on how heavily you use the services and how important your data is. I use Google Docs and similar web apps only occasionally, and the data I store there isn't important enough to me to pay for an extra backup. However, if you store crucial data only in the cloud, a cloud-to-cloud or cloud-to-local backup service may be a smart investment.

Warning! Whatever you do, don't use the same company's services for both primary storage and backups. For example, if you rely heavily on Google Docs, Google Drive is not where you should back up that data; spread out your risk by using an entirely different cloud provider.

Back Up While on the Road

It's relatively easy to back up when you're at home or at the office: you can set up a system that copies data from one or more computers to local or network drives and that stores it automatically. But when you're away from your usual equipment, backups become more difficult.

When traveling with a laptop, you face two main questions:

- Do you back up to local media (a flash drive, say, or an external hard drive) or use the internet to back up to a remote location?
- If you do choose to back up remotely, what's the best way to do so safely and efficiently?

Backing up your laptop directly to a hard drive or flash drive is invariably quicker than backing up over the internet. You also avoid any worries about sensitive data being intercepted in transit, and you have a handy copy of your data available for instant restoration if you need it. On the other hand, if your laptop and its accessories are stolen, left in a taxi, or otherwise lost, you're likely to lose all your backups too. So a word to the wise: if you choose to keep your backups with you, at least keep them separate from your computer—and make sure they're encrypted.

Local backups are best for people who generate large volumes of data—videos, for example. If you create several gigabytes of new files every day while away, backing up remotely might be too time-consuming. A local backup is also the only good option if you're traveling somewhere without high-speed internet access.

On the other hand, if you generate only a modest amount of data on the road and fast internet access is available (especially if it's *free* fast internet access!), backing up remotely is an excellent option, as all your data is safely offsite. Again, be sure to use an encrypted connection or backup software that encrypts the files before they're sent over the internet, because otherwise you run a slight risk that a hacker could intercept your private data while it's in transit.

Tip: Regardless of which method you use, I strongly suggest making a full backup just before you leave for your trip. That will minimize the amount of data you have to back up during your trip and will give you a safety net in case your laptop is stolen.

Local Backups on the Road

When your concern is to maintain backups of just the files you're actively working on (as might be the case if you'll do full backups when you return home or to the office), you have more flexibility in choosing storage media, since massive capacity is unnecessary.

USB flash drives are ubiquitous, tiny, and inexpensive at modest capacities, so they make a good choice for backups on the road. Ditto for SD cards, if you have a Mac laptop with a built-in SD card reader. Because flash storage of either sort can get pricey at high capacities, it's less well suited for backing up an entire disk—see [Hardware You Should Probably Avoid](#)—but if you have only a few gigabytes to back up, flash drives and SD cards are quite handy.

If you use a flash drive or SD card, keep these tips in mind:

- Even if you normally back up every file on your Mac, save time and media while traveling by backing up only your most important files—specifically, those you've worked on during your trip. (When in doubt, you can do a Spotlight search in the Finder for just those files modified in, say, the last day.)
- If your backup app supports encryption, use it. You wouldn't want someone who stumbles upon your flash drive to get easy access to any personal information stored in your files.

Yet another option—and my personal preference—is an external hard drive, which lets you back up (and, if necessary, restore) your entire disk. For ease of transportation, I suggest a bus-powered (no AC adapter required), pocket-sized model. See the [online appendixes](#) for suggestions.

Remote Backups on the Road

You can back up your files remotely in any of several different ways, depending on your circumstances and preferences. As I mentioned earlier, though, all these methods presuppose that you have a relatively small amount of data to back up—you’ll likely be constrained by the upstream bandwidth of your internet connection and may also have time constraints that limit how much data you can comfortably back up. Here are some remote backup options:

- **Internet backup services:** For backing up a relatively small amount of data, consider an online backup service. For example, Backblaze or IDrive can back up your laptop’s files to proprietary cloud storage, while Acronis True Image, Arq, and several other apps can use cloud storage, local hard drives, or both. For more options, see [Use a Cloud Backup Service](#).
- **Push or pull backups with home server:** If you run third-party backup software on a server at home or the office (see [Network Backup Approaches](#)), you may be able to connect to that server remotely, but that’s not as easy as it may sound. “Push” backups work only if you can mount your backup server’s volumes remotely; “pull” backups work only if your server can mount your laptop’s volume remotely. Sometimes this remote mounting is possible, but often not; your firewall at home must enable access to the necessary ports, and the ISP providing your remote access must permit file-sharing access over their network. You also run a risk that your files may be intercepted in transit by a hacker, unless you take extra steps to encrypt the network link between your laptop and your server.

- **Client-server backups with home server:** Client-server backup software, such as Retrospect, normally polls only the local network for available clients. In some cases, you can manually enter an IP address for a computer outside your local network. However, if you're traveling and don't know what IP address you'll have at any given time, this method is problematic. A possible solution is to use a dynamic DNS service, such as the one provided by [easyDNS](#), to assign your laptop a domain name whose IP address changes as needed, and then enter that domain name in your backup software. Although various other techniques (and third-party networking tools) sometimes allow remote file sharing, they're less likely to work with client-server setups.

Tip: Whether using push, pull, or client-server backups, you can get around most difficulties in contacting your backup server remotely—as well as ensure private, encrypted communications—with a VPN (virtual private network) connection to your home network, but the details of setting up such a system go beyond what I can cover in this book.

Back Up an iOS Device

This book is about backing up your Mac, but many Mac users are also iOS users, and I've had requests to say a few words here about backing up iOS devices.

Even though iOS devices contain data that's every bit as valuable as what's on your Mac, they follow a much different model for both data storage and backups. Here are the key points you should be aware of:

- **Most iOS data is also stored in the cloud.** Even if you never explicitly back up your iOS device in any way, the majority of iOS apps store their data in the cloud (in one form or another), meaning that even if your device were stolen or destroyed, it would be possible to retrieve your data (for example, using a new iOS device). This is true, of course, for data such as calendars, contacts, email, and reminders: when you connect to an online account such as iCloud,

Google, or Exchange, your iOS device stores a copy of this personal data—but the original is in the cloud.

Many other apps, both from Apple and from third parties, also use cloud storage or syncing of one sort or another, at least optionally. Some of them use iCloud Drive; others use Dropbox, another cloud storage provider, or a proprietary service run by the app's developer. In any case, apps that store data locally *only* on your iOS device are relatively rare. Although the copy of the data in the cloud isn't exactly a backup as I define it in this book, it can serve much the same purpose, at least to the extent that it protects you against the loss of your device.

- **Restoring from iOS backups is all or nothing.** The previous point notwithstanding, if you want to back up all the data on your device, including anything you've opted to store locally plus all your apps and settings, you can do so. But you won't find third-party backup apps for iOS that work the same way macOS backup apps do, and although you can disable backups of individual apps or delete the entire backup of a single device (in Settings > *Your Name* > iCloud > Manage Storage > Backup > *Device Name*), that's the extent of control Apple gives you. More significantly, if you lose data and need to restore a backup, you must normally restore *everything*—that is, wipe everything off your device, reinstall iOS, and restore *all* your data from an iCloud or iTunes backup (see the next bullet). Apple provides no way to restore individual files from a backup.

Note: A third-party Mac app called [iMazing](#) does enable you to extract individual items from an iTunes backup of your iOS device. However, although you can access these on your Mac, iMazing offers no direct way to restore them onto your iOS device.

- **You have two backup options.** Apple offers two approaches to the all-or-nothing backup. One way is to use iCloud, which takes just a few taps to set up. With iCloud backups enabled, once a day (as long as your iOS device is locked, connected to Wi-Fi, and attached to a power source), iOS backs up all your data to iCloud.

The other option, if you prefer to avoid iCloud, is to back up the data from your iOS device(s) to your Mac using iTunes. You can use either a Wi-Fi connection or a USB cable for iTunes backups; the former is more convenient but the latter is faster. If you do choose an iTunes backup, be aware that all the data you're backing up from your iOS device will take up space on your Mac, and thus it will also take up space in your Mac's backups.

Apple provides complete instructions for setting up iOS backups via either iCloud or iTunes in [How to back up your iPhone, iPad, and iPod touch](#), and for restoring backups in [Restore your iPhone, iPad, or iPod touch from a backup](#).

As a reminder (see [Back Up Data from the Cloud](#)), storing data in the cloud and backing up to the same cloud service isn't really smart! So, if you rely on iCloud storage for all the documents on your iOS device and also use iCloud backups exclusively, you're entirely at the mercy of iCloud. So I recommend thinking carefully about where your data is stored and choosing a backup destination that's different from your storage destination.

Back Up Windows Files and Volumes

You can run Windows alongside macOS, using either Apple's Boot Camp software (which puts the entire Windows installation on a separate partition) or virtualization software such as Parallels Desktop or VMware Fusion (which stores the Windows environment in a special disk image file). Either way, the presence of a second operating system increases the complexity of your backup needs.

If you use Windows only occasionally and don't store much data on your Windows volume, you might consider forgoing Windows backups altogether. Reinstalling Windows and a few apps (as you might have to do in the case of a disk problem) is annoying but not the end of the world. (And, if you use a cloud sync service such as Dropbox for most of your personal files, you can install the corresponding app and let it sync, eliminating the need to fetch those files from a backup.) Howev-

er, if your use of Windows is more extensive, read on for instructions on keeping your data safe.

The way you back up your Windows files depends partly on the way in which you're running Windows and partly on your specific needs. The main consideration is whether you're using Boot Camp or a virtualization environment.

Boot Camp

As far as macOS is concerned, the Windows partition Boot Camp creates is just another volume, so most Mac backup software can read its files easily. That may lead you to conclude you can simply back up your Windows partition along with your Mac partition using your favorite Mac backup app; however, a few issues arise:

- If you've formatted your Windows volume as NTFS (the only option for Windows Vista and later), macOS can read from, but not write to, that volume. This means you can back up your files but not restore them from within macOS—a potentially significant problem.

One way around this problem is to use [Microsoft NTFS for Mac by Paragon Software](#), which transparently allows macOS to read and write NTFS volumes. There's also the open-source [NTFS-3G](#) and its commercial variant, [Microsoft NTFS for Mac by Tuxera](#), both of which are based on MacFUSE from Google Code.

- Some backup software, including SuperDuper!, cannot read from Windows partitions at all.
- If you rely on Mac software to back up your Windows volume, then backups can take place only when you're running macOS. So if you run Windows under Boot Camp for extended periods of time, your risk of data loss increases.
- Even in cases where you can back up the entire contents of your Windows partition while running macOS, a complicated procedure is usually necessary when restoring files to make sure the restored Windows volume is bootable. So as with duplicating a macOS

volume, it's a job better left to specialized software, in this case software running under Windows.

Therefore, if you've decided to back up your Boot Camp volume, you'll need to develop separate strategies for creating duplicates, versioned backups, or both.

Duplicate a Boot Camp Volume

The easiest way by far to duplicate (and restore) a Boot Camp volume without leaving macOS is to use [Winclone](#), a Mac backup utility specifically designed for that purpose. Winclone is a simple, straightforward app: you choose a source (your Boot Camp volume), click the Image button, and follow the prompts to create a disk image with a copy of all your Boot Camp files; you can store that image anywhere you like, including on your internal disk. You can also restore a Boot Camp volume without rebooting from another drive. Prices range from \$19.99 to \$249.99, depending on which features you need.

Alternatively, you can make a bootable duplicate of your Windows volume from within Windows. Very few Windows backup apps offer this capability; one that does is called [Casper](#).

A more common way to back up a Windows installation is called *imaging*. In Mac terms, creating a Windows system image would be comparable to duplicating one's entire disk onto a disk image stored on another volume; the disk image itself wouldn't be bootable, but you could restore it onto a hard drive that then would be. Sometimes, Windows imaging utilities can create incrementally versioned images, such that you can restore your entire disk (although not necessarily individual files) to various past states without requiring multiple complete copies of the whole disk. Imaging software may let you store a single backup on another disk in such a way that you can boot from that disk if you connect it to the same computer, but unlike in macOS, a disk that can boot up one PC can't necessarily boot another; some imaging utilities can make this happen, but some can't.

Examples of Windows imaging software include:

- [Casper](#) (which, as mentioned above, also creates bootable duplicates)
- [DriveImage XML](#)
- Windows Backup (built into Windows 7 and later, but has far fewer features than the others)

I no longer use Boot Camp on a regular basis (virtualization meets my needs better), and even if I did, my usage would be so light and infrequent that imaging my disk wouldn't be worth the time and bother. So, I haven't used any of these apps extensively enough to have much of an opinion other than to say I'd start with a free choice and go from there. However, I do think some variety of versioned backups is a good idea, and I turn to that topic next.

Create Versioned Backups of a Boot Camp Volume

If you want to make versioned backups of some or all your Windows files, you can do so either from macOS—after a reboot, naturally—or from within Windows.

Versioned Boot Camp Backups Under macOS

It may be possible to use Mac backup software to make versioned backups of your Boot Camp volume. Assuming it's formatted as NTFS (used in Windows Vista and later), your Mac backup software should be able to see and to back up Windows files, but you'll be unable to *restore* them from within macOS unless you've also installed NTFS for Mac (as described just previously) or similar software.

In any case, remember that because these methods depend on macOS software, which can't run until you reboot into macOS, your files won't be backed up while you're using Windows.

Yet another option exists, and although it might involve changes to your workflow, I think it's the simplest approach. If you install [Mac-Drive](#) under Windows, you can mount your Mac (HFS Plus or APFS) volume and read and write files on it directly, just as though it were a regular Windows volume. So, if you do this and then ensure that you

always save the Windows files that you want to back up on your Mac volume, they'll always be backed up with the rest of your Mac files when your Mac backup software runs.

Versioned Boot Camp Backups Under Windows

If you run Windows under Boot Camp frequently, and create or modify lots of files there, then making versioned backups of your Windows files is important for the same reason as doing so for your Mac files.

You can do this in many ways, but I suggest choosing one of three main approaches (listed here in the order I think you should consider them):

- **Use a cloud-based sync service with versioning support.** If the files you're creating in Windows are mostly on the small side, you could store them in a folder that you sync with a service like Dropbox or SugarSync (see the sidebar [What About Cloud Storage and Syncing Services?](#)). They would be automatically synced to the cloud, with multiple versions stored there, and you would avoid having to do any extra work to keep the files backed up. On the minus side, this would work only for a limited set of files—not for every file on your Windows volume.
- **Run cross-platform, network backup software.** If I were setting up versioned backups for my own Boot Camp volume, I'd use Backblaze. The Windows version is almost identical to the Mac version, and I can use my existing account (although I'd have to pay for an additional subscription). If you're already doing network backups with Retrospect, that's another good choice—but keep in mind that the computer functioning as your backup server can't be the same Mac that's running Boot Camp. Other apps could work, too, but all things being equal I like the idea of using the same software and storage media for backups on all my computers.
- **Run Windows-only backup software.** There are oodles of Windows-only backup apps—more even than on the Mac (and that's saying something). I have no personal experience with backup software that runs only on Windows, but I've read good things about StorageCraft's [ShadowProtect Desktop](#), which goes beyond

mere imaging to offer the sort of detailed control over versioned backups that my favorite Mac backup apps do.

Virtualization Software

If you use virtualization software such as Parallels Desktop or VMware Fusion, your Windows files live on a special disk image that appears as a regular volume in Windows. Your existing Mac backup software can copy that disk image, making what amounts to a bootable duplicate of your virtual machine—but read on to learn about some potential pitfalls of doing so. You can also use any of several techniques to make versioned backups of individual files and folders inside your virtual machine, either in macOS or from within Windows.

Duplicate a Virtual Machine

Since a virtual machine disk image is, as far as macOS is concerned, merely a file (or, in some cases, a series of files), the easiest way to back them up is simply to ensure that your Mac backup software copies them along with the rest of your documents. In other words, whether you create a duplicate or a versioned backup of your Mac data, you still end up with a bootable duplicate of your Windows virtual machine.

But there's a catch. The disk image is usually quite large—often in the tens of gigabytes—and simply running Windows modifies the image. That creates a problem for any backup software that does file-by-file incremental updates (as Time Machine does, for example), because it will consider the whole file to have changed each time. Adding these disk images to versioned backups will rapidly chew up disk space and make backups take much longer.

You can solve this problem in any of several ways:

- **Create snapshots.** Both Parallels and Fusion let you take snapshots of your virtual machine's current state, so you can roll back to that state at a future time if the need arises. Taking a snapshot saves the largest portion of your virtual disk in a read-only state, so that as you continue to use the virtual machine in the future, the changes are stored in smaller chunks that are quicker to back up. In Parallels, you can enable a comparable feature called

SmartGuard: with a virtual machine running, choose Actions > Configure > Backup and select SmartGuard; then click Details and specify a schedule and other settings. In Fusion, you should also turn on AutoProtect to create new snapshots automatically on a schedule: choose Virtual Machine > Snapshots, click AutoProtect Settings, set AutoProtect to On, and click Done.

- **Use backup software that supports delta encoding.** If your backup software copies only the changed *portions* of files, rather than entire files (refer to [Delta Encoding](#)), you needn't worry that you'll have to copy 20 GB of data for every hour that you use Windows.
- **Back up virtual machines separately.** You can exclude your virtual machines from your regular versioned backups and then set up a separate backup, just for the virtual machines, that you run manually as needed—perhaps configuring your software to keep only a limited number of backed-up versions in order to save space.

Warning! Before backing up a virtual machine using any Mac backup software, make sure you pause, suspend, or shut down the virtual machine. Otherwise, the disk image may change during the backup process, leading to a corrupted and unusable backup.

If your Mac backup software creates versioned backups (whether they're file-based or use delta encoding), an interesting consequence of backing up a virtual machine is that the distinction between a bootable duplicate and a versioned backup blurs. You have, in effect, a versioned bootable duplicate: you can return your entire virtual machine to its state at any previous time when a backup ran, although you can't restore individual files or folders within your virtual machine to earlier states independently. If that's important to you—as it well may be—read on for how to create versioned backups of files and folders from your Windows virtual machine.

Create Versioned Virtual Machine Backups

Whatever the benefits of backing up an entire virtual machine, one downside is that Mac backup software can't normally see into your

Windows volume to back up and restore individual files and folders. If you spend a lot of time creating and modifying files in Windows, it may be important to have frequent versioned backups of your Windows data rather than wait until you can pause your virtual machine to perform a full backup.

You can create versioned backups of your Windows data in any of several different ways, but I suggest trying one of the first two suggestions that follow if feasible, because they'll make your life easier:

- **Use a shared macOS folder.** Both Parallels Desktop and VMware Fusion let you set up folders from your Mac (or even your entire Mac drive) so that you can access them from within Windows. So you could use a shared macOS folder to save the Windows files you create and modify, and simply have your Mac backup software include that folder in your backups.
- **Use a shared Windows folder.** This is the flip side of the previous item. Virtualization software can share folders (such as My Documents) from Windows so that they're available in macOS—as long as your virtual machine is running. Do that, and your existing Mac backup software can access your Windows data directly.
- **Back up from within Windows.** Use any of the options noted earlier in [Versioned Boot Camp Backups Under Windows](#): sync your data to the cloud with a service that supports versioning (such as Dropbox or SugarSync); use cross-platform, network-based backup software such as Backblaze or Retrospect; or run your favorite conventional Windows backup app. Of these, my first inclination would be to install Backblaze.

About This Book

Thank you for purchasing this Take Control book. We hope you find it both useful and enjoyable to read. We welcome your [comments](#).

Ebook Extras

You can [access extras related to this ebook](#) on the web. Once you're on the ebook's Take Control Extras page, you can:

- Download any available new version of the ebook for free, or buy a subsequent edition at a discount.
- Download various formats, including PDF, EPUB, and Mobipocket. (Learn about reading on mobile devices on our [Device Advice](#) page.)
- Read the ebook's blog. You may find new tips or information, as well as a link to an author interview.
- Find out if we have any update plans for the ebook.

If you bought this ebook from the Take Control website, it has been automatically added to your account, where you can download it in other formats and access any future updates. However, if you bought this ebook elsewhere, you can add it to your account manually:

- If you already have a Take Control account, log in to your account, and then click the “access extras...” link above.
- If you don't have a Take Control account, first make one by following the directions that appear when you click the “access extras...” link above. Then, once you are logged in to your new account, add your ebook by clicking the “access extras...” link a second time.

Note: If you try these directions and find that your device is incompatible with the Take Control website, [contact us](#).

About the Author and Publisher



Joe Kissell is the author of more than 60 books about technology. As of May 2017, he also became the publisher of Take Control Books, when alt concepts inc.—the company he runs along with his wife, [Morgen Jahnke](#)—acquired the Take Control series from TidBITS Publishing Inc.’s owners, Adam and Tonya Engst.

Joe is also a contributing editor to TidBITS and a senior contributor to Macworld. Before he began writing full-time in 2003, Joe spent nearly eight years managing software development. He holds a bachelor’s degree in Philosophy and a master’s degree in Linguistics.

In his rare non-work hours, Joe likes to travel, walk, cook, eat, and practice t’ai chi. He and Morgen live in San Diego with their sons, Soren and Devin, and their cat, Zora. To contact Joe about this book, [send him email](#) and *please* include [Take Control of Backing Up Your Mac](#) in the subject. You can also follow him on Twitter ([@joekissell](#)) or visit his personal website, [JoeKissell.com](#).

Credits

- Publisher: Joe Kissell
- Editor: Caroline Rose
- Cover design: Sam Schick of [Neversink](#)
- Logo design: Geoff Allen of [FUN is OK](#)

Also by Joe Kissell

Click any book title below or [visit our web catalog](#) to add more ebooks to your Take Control collection!

[*Take Control of Apple Mail*](#): Learn the ins and outs of Apple's email app in macOS and iOS.

[*Take Control of Maintaining Your Mac*](#): Learn preventive maintenance steps to keep your Mac running smoothly.

[*Take Control of Speeding Up Your Mac*](#): Turn a slow Mac into a high-performance machine.

[*Take Control of the Cloud*](#): Wrap your head around the wide variety of cloud services and apps, and make smart purchasing decisions.

[*Take Control of the Mac Command Line with Terminal*](#): Master your Mac's command-line interface and learn basic Unix skills.

[*Take Control of Troubleshooting Your Mac*](#): Solve most everyday Mac problems without a trip to the Genius Bar.

[*Take Control of Upgrading to Mojave*](#): Experience a trouble-free upgrade to the latest version of macOS with this comprehensive guide.

[*Take Control of Your Digital Legacy*](#): Make sure your important digital information is preserved for future generations.

[*Take Control of Your Online Privacy*](#): Learn what's private online (not much)—and what to do about it.

[*Take Control of Your Paperless Office*](#): With your Mac, scanner, and this ebook in hand, you'll finally clear the chaos of an office overflowing with paper.

[*Take Control of Your Passwords*](#): Overcome password overload without losing your cool.

Copyright and Fine Print

Take Control of Backing Up Your Mac, Third Edition

ISBN: 978-1-947282-14-8

Copyright © 2019, alt concepts inc. All rights reserved.

[alt concepts inc.](#) 4142 Adams Ave. #103-619, San Diego CA 92116, USA

Why Take Control? We designed Take Control electronic books to help readers regain a measure of control in an oftentimes out-of-control universe. With Take Control, we also work to streamline the publication process so that information about quickly changing technical topics can be published while it's still relevant and accurate.

Our books are DRM-free: This ebook doesn't use digital rights management in any way because DRM makes life harder for everyone. So we ask a favor of our readers. If you want to share your copy of this ebook with a friend, please do so as you would a physical book, meaning that if your friend uses it regularly, they should buy a copy. Your support makes it possible for future Take Control ebooks to hit the internet long before you'd find the same information in a printed book. Plus, if you buy the ebook, you're entitled to any free updates that become available.

Remember the trees! You have our permission to make a single print copy of this ebook for personal use, if you must. Please reference this page if a print service refuses to print the ebook for copyright reasons.

Caveat lector: Although the author and alt concepts inc. have made a reasonable effort to ensure the accuracy of the information herein, they assume no responsibility for errors or omissions. The information in this book is distributed "As Is," without warranty of any kind. Neither alt concepts inc. nor the author shall be liable to any person or entity for any special, indirect, incidental, or consequential damages, including without limitation lost revenues or lost profits, that may result (or that are alleged to result) from the use of these materials. In other words, use this information at your own risk.

It's just a name: Many of the designations in this ebook used to distinguish products and services are claimed as trademarks or service marks. Any trademarks, service marks, product names, or named features that appear in this title are assumed to be the property of their respective owners. All product names and services are used in an editorial fashion only, with no intention of infringement. No such use, or the use of any trade name, is meant to convey endorsement or other affiliation with this title.

We aren't Apple: This title is an independent publication and has not been authorized, sponsored, or otherwise approved by Apple Inc. Because of the nature of this title, it uses terms that are registered trademarks or service marks of Apple Inc. If you're into that sort of thing, you can view a [complete list](#) of Apple Inc.'s registered trademarks and service marks.