Die neue Passwörter-App in macOS Sequoia

Howard Oakley, eclecticlight.co • Übersetzung KJM

Nachdem ich die neue Passwörter-App in Sequoia unter die Lupe genommen habe, bin ich von ihr begeistert. Wenn Sie nicht davon überzeugt sind, dass Sie Ihre Geheimnisse durch ein anderes Passwort schützen müssen, sollten Sie sich die App genau ansehen, denn sie könnte Ihnen das Abonnement für ein Passwortmanager-Programm eines Drittanbieters ersparen. In diesem Artikel wird erklärt, auf welche Geheimnisse sie Zugriff gibt, denn das kann verwirrend werden.

Macs und Apple-Geräte haben einen gemeinsamen Schlüsselbund, den Datenschutz- oder iCloud-Schlüsselbund. Auf diesen Schlüsselbund konnte man früher über die Passwörter-Einstellungen in Safari und den Systemeinstellungen zugreifen, die durch die Passwörter-App ersetzt wurden. Macs haben noch weitere Schlüsselbunde, darunter einen ebenso wichtigen, den Schlüsselbund für die Anmeldung des Benutzers. Die Kennwörter-App hat nichts mit diesem oder anderen dateibasierten Schlüsselbüchern zu tun, also komme ich erst am Ende auf diese zurück.

Schlüsselbund Datenschutz

Seit OS X 10.9 gibt es auf Macs für jeden Benutzer nur einen einzigen Schlüsselbund für den Datenschutz. Wenn Sie Ihren Schlüsselbund in iCloud freigeben, ist dies die lokale Kopie des freigegebenen Schlüsselbundes und wird als iCloud-Schlüsselbund bezeichnet; wenn Sie ihn nicht in iCloud freigeben, wird er stattdessen als „Lokale Objekte“ bezeichnet. Die lokale Kopie davon wird normalerweise in ~/Library/Keychains/[UUID]/keychain-2.db gespeichert, wobei die UUID diejenige ist, die diesem Mac zugewiesen wurde.

Der Datenschutz-Schlüsselbund kann fast alle Standardtypen von Geheimnissen speichern, einschließlich Internet- und andere Passwörter, Zertifikate, Schlüssel und Passkeys, aber keine sicheren Notizen. Vor macOS 11 wurden nur Internet-Passwörter mit iCloud synchronisiert, aber ab Big Sur werden alle Inhalte synchronisiert, einschließlich der Passkeys, die nun endlich als Bürger erster Klasse gelten. Im Gegensatz zu dateibasierten Schlüsselbunden können die Geheimnisse im Datenschutz-Schlüsselbund durch die Secure Enclave geschützt werden und können daher durch biometrische Merkmale wie Touch ID und Face ID auf iOS und iPadOS geschützt werden. Daher werden sie für Passkeys benötigt, die von traditionellen dateibasierten Schlüsselbunden nicht unterstützt werden.

Bitte um weitere Unterstützung

Das Herausgeben des Newsletters für den MACtreff Köln ist mit Kosten verbunden: Der Internet-Zugang, das Hosting der Homepage und die Software zur Webseitenerstellung kosten mich jährlich rund 670 €.

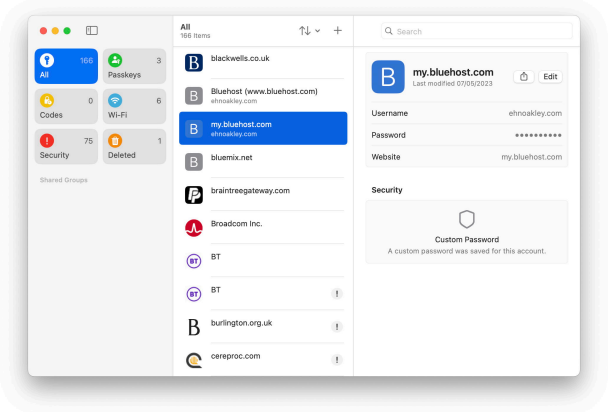
Gestiegene Krankenversicherungsbeiträge haben meinen Spielraum eingeengt, den seit 1989 betriebenen Aufwand weiterhin zu finanzieren.

Daher meine Bitte: Unterstützt meine Arbeit bitte durch eine Spende auf mein Paypal-Konto, indem Ihr auf den folgenden Link klickt paypal.me/KJM54 und dort einen Betrag eingebt.

Mein Dank gilt allen Lesern, die schon gespendet haben!

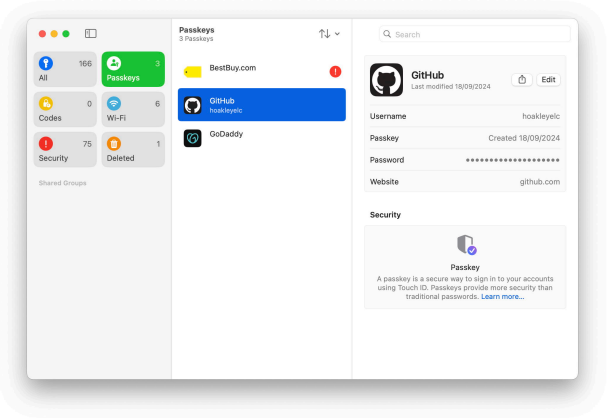
Kurt J. Meyer

Passwörter



Die einfachste Kategorie von Geheimnissen, auf die die Passwörter-App zugreift, sind Internet- und Website-Passwörter, die in der Kategorie „Alle“ aufgeführt sind und für die Kategorie „Sicherheit“ in Frage kommen, wenn sie kompromittiert wurden, wiederverwendet werden oder schwach sind. Für diese Passwörter ist Passwörter der einzige Ort, an dem sie bearbeitet und verwaltet werden können, da die von der Schlüsselbundverwaltung bereitgestellte Auflistung fast nicht vorhanden ist. Andere Kategorien, wie z. B. Anwendungskennwörter, erscheinen hier nicht und sind nur in der Schlüsselbundverwaltung zugänglich. Aber für die meisten üblichen Zwecke bietet die Passwörter-App Zugang zu denjenigen, die Sie am häufigsten benötigen.

Passkeys

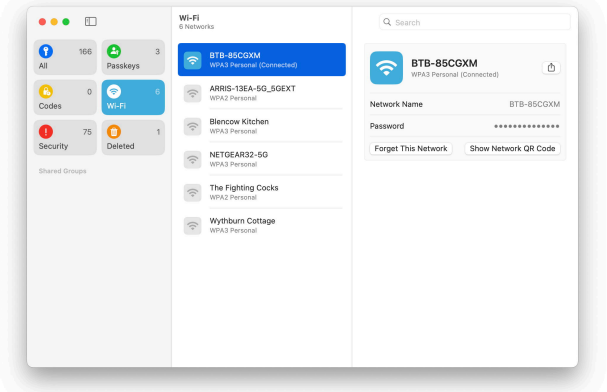


Obwohl sie noch nicht so weit verbreitet sind, wie sie es verdienen, fordern immer mehr Websites dazu auf, sich mit einem Passkey („Hauptschlüssel“) zu authentifizieren, und das sollten Sie auch tun, wenn Sie können. Die Passwörter-App ist die einzige Möglichkeit, auf sie zuzugreifen, da sie in den Listen der Schlüsselbundverwaltung nicht enthalten sind.

Das Erstellen und Verwenden eines Passkeys erfordert eine Form der biometrischen ID. Wenn Ihr Mac über eine Tastatur mit Touch ID verfügt, ist das kein Problem, aber es gibt einen einfachen Workaround, wenn Sie einen Hauptschlüssel auf einem Mac ohne Touch ID verwenden möchten, vorausgesetzt, Sie haben ein Apple-Gerät mit Touch ID oder Face ID.

Wenn Sie versuchen, sich bei einer Passkey-Website anzumelden und zur biometrischen Authentifizierung aufgefordert werden, wählen Sie die Option im Popup-Menü unten, um einen Passkey von einem Gerät in der Nähe zu verwenden. Öffnen Sie die Kamera auf Ihrem iPhone oder iPad und rahmen Sie den QR-Code ein, der auf Ihrem Mac angezeigt wird. Sie sollten dann eingeladen werden, sich auf dem Gerät anzumelden. Das mag anfangs etwas umständlich erscheinen, geht aber schnell von der Hand.

Wi-Fi-Passwörter



Diese werden zwar auch im Schlüsselbund des Datenschutzes gespeichert, aber was Sie auf jedem Mac und Gerät sehen, hängt auch davon ab, welche Netzwerke in den individuellen Wi-Fi-Einstellungen als „Bekannte Netzwerke“ aufgeführt sind. Um diese zu überprüfen, öffnen Sie Wi-Fi in den Systemeinstellungen und klicken Sie auf die Schaltfläche Erweitert... am Fußende der Einstellungen.

Dies kann verwirrend sein, da Sie auf verschiedenen Macs und Geräten sehr unterschiedliche Listen bekannter Netzwerke vorfinden können. Auf jedem Gerät sollten die Netzwerke, die in der Wi-Fi-Gruppe der Password-App angezeigt werden, mit denjenigen in der Liste der bekannten Netzwerke übereinstimmen.

Die übrigen Schlüsselbunde auf einem Mac sind dateibasiert und können von der Kennwörter-App nicht eingesehen werden.

Anmelde-Schlüsselbund

Für jeden Mac-Benutzer ist sein persönlicher dateibasierter Schlüsselbund standardmäßig der Anmelde-Schlüsselbund, der sich in ~/Library/Keychains/login.keychain-db befindet. Dieser wird automatisch entsperrt, wenn sich der Benutzer anmeldet, da er dasselbe Passwort wie der Benutzer-Account hat. Hier sollte jeder Benutzer seine Zertifikate, sicheren Notizen usw. für die allgemeine Verwendung auf dem Mac speichern.

Auch wenn das Verzeichnis nicht gesperrt ist und gelesen und beschrieben werden kann, solange der Benutzer angemeldet ist, ist der Zugriff auf seinen Inhalt nicht garantiert. Wenn eine Anwendung das macOS-Sicherheitssystem aufruft, um ein gespeichertes Kennwort für ihre Verwendung abzurufen, bestimmt dieses System, ob der Anwendung der Zugriff auf diese Informationen vertraut wird und ob der Schlüsselbund gesperrt ist. Angenommen, das Kennwort ist dort gespeichert, die App ist vertrauenswürdig und der Schlüsselbund ist entsperrt, dann wird das Kennwort abgerufen und an die App zurückgegeben. Wenn die App nicht vertrauenswürdig ist oder der Schlüsselbund gesperrt ist, zeigt das Sicherheitssystem, nicht die App, ein unverwechselbares Standarddialogfeld an, in dem das Kennwort für den Schlüsselbund zur Authentifizierung abgefragt wird, bevor es das Kennwort an die App weitergibt.

Der Benutzer kann nicht bestimmen, welche Apps für das Sicherheitssystem vertrauenswürdig sind. Diese werden vom Sicherheitssystem, dem spezifischen Zugriff, den es einer App gewährt, und den einzelnen Elementen im Schlüsselbund des Benutzers bestimmt. In seiner restriktivsten Form kann das System allen anderen Anwendungen den Zugriff auf ein bestimmtes Geheimnis im Schlüsselbund verwehren, aber bestimmte Geheimnisse können auch von mehreren verschiedenen Anwendungen gemeinsam genutzt werden.

System-Schlüsselbunde

Es gibt zwei wesentliche Gruppen von Schlüsselbunden für macOS:

- in /System/Library/Keychains im Sealed System Volume befinden sich SystemRootCertificates und andere, die den Satz von Root-Sicherheitszertifikaten für diese Version von macOS bereitstellen;
- in /Library/Keychains befinden sich der System-Schlüsselbund und andere mit Zertifikaten und Passwörtern, die für alle Benutzer erforderlich sind, einschließlich derer, die für den Zugriff auf die Wi-Fi-Verbindungen des Macs benötigt werden.

Benutzerdefinierte Schlüsselbunde

Apps und Benutzer können auch ihre eigenen Schlüsselbunde erstellen. Zu den Schlüsselbunden, die ich auf meinen Macs habe, gehören gemeinsame Schlüsselbunde mit virtuellen Maschinen von Parallels, mehrere für Microsoft-Anwendungen und einige für Adobe-Produkte. Ich neige auch dazu, eine Kopie des Anmelde-Schlüsselbundes von meinem letzten Mac zu erstellen und sie unter einem anderen Namen nach ~/Library/Keychains zu kopieren, damit ich, falls ich bei der Migration auf einen neuen Mac wichtige Zertifikate oder Passwörter vergessen habe, diese dort finden kann.

Obwohl diese zusätzlichen Schlüsselbunde in den Suchpfad für den Schlüsselbund aufgenommen werden können, werden sie, wenn macOS nach einem Geheimnis in einem Schlüsselbund sucht, im Gegensatz zum Anmeldeschlüsselbund normalerweise gesperrt gehalten. Wenn ich oder eine Anwendung auf sie zugreifen möchte, werde ich nach dem Kennwort des Schlüsselbundes gefragt. Bei alten Anmeldeschlüsselbunden ist das natürlich nur mein altes Anmeldekennwort für jenen Mac.

Eines der größten Sicherheitsprobleme bei dateibasierten Schlüsselbunden ist, dass sie für Malware relativ leicht zu exfiltrieren sind und bei entsprechend leistungsfähiger Hardware ein Brute-Force-Zugriff auf ihre Inhalte möglich ist.

Schlüsselbundverwaltung

Das mitgelieferte Tool für die Arbeit mit dateibasierten Schlüsselbunden ist die Anwendung Schlüsselbundverwaltung, die nun in den Hintergrund gerückt wurde und unter /System/Library/CoreServices/Applications zu finden ist. Auch wenn Apple diese Anwendung und dateibasierte Schlüsselbunde im Allgemeinen gerne abschaffen würde, können sie noch nicht verschwinden, egal wie gut die Passwords-Anwendung sein mag.

CSV-Import/-Export

Für diejenigen, die CSV-Dateien in Passwords importieren möchten, sind die Felder, die exportiert werden: Titel,URL,Benutzername,Passwort,Notizen,OTPAuth. Ich gehe davon aus, dass der Import einer CSV-Datei, die von einem anderen Passwortmanager exportiert wurde, erfolgreicher sein wird, wenn man sie so formatiert, dass sie mit dieser ersten Zeile übereinstimmt. Eine Tabellenkalkulation wie Numbers ist ein guter Ort, um CSV-Dateien zu bearbeiten.

Referenzen

Apple TN3137:
Mac-Schlüsselbund-APIs und -Implementierungen

Apple-Schlüsselbunddienste

6 Funktionen in macOS Sequoia, die Sie tatsächlich nutzen werden

Quelle: osxdaily.com • Übersetzung: KJM

Jetzt, wo MacOS Sequoia für alle Mac-Benutzer zum Aktualisieren und Installieren zur Verfügung steht, fragen Sie sich vielleicht, welche der vielen neuen Funktionen und Änderungen besonders verlockend sind und welche Sie tatsächlich nutzen könnten. Anstatt Sie mit einer Liste von siebenundzwanzig Billionen Neuerungen zu überhäufen, die Sie schnell wieder vergessen werden, konzentrieren wir uns hier auf sechs der wichtigsten neuen Funktionen in macOS Sequoia, die Sie ausprobieren sollten und die Sie wahrscheinlich regelmäßig nutzen werden.

1: iPhone-Spiegelung

Anmerkung: Leider steht diese Funktion in „unserer Region" (Deutschland oder EU?) noch (?) nicht zur Verfügung.

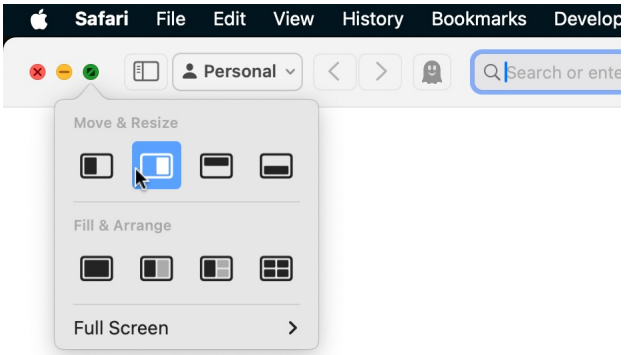
Die iPhone-Spiegelung ist wohl die größte und nützlichste Funktion in MacOS Sequoia. Sie ermöglicht es Ihnen, Ihr iPhone von Ihrem Mac aus mit Ihrem Cursor und Ihrer Tastatur zu steuern.

Starten Sie einfach die App „iPhone Mirroring" (auf Deutsch: „iPhone-Synchronisierung"), die sich standardmäßig im Ordner „Programme" befindet, und schon können Sie loslegen.

Beachten Sie, dass Sie zur Verwendung von iPhone Mirroring auch das iPhone auf iOS 18 oder neuer aktualisieren müssen.

2: Einfaches Anordnen von Fenstern

Multitasking mit mehreren geöffneten Apps und Fenstern ist in macOS Sequoia dank der stark verbesserten Fensterkachelfunktionen einfacher denn je.



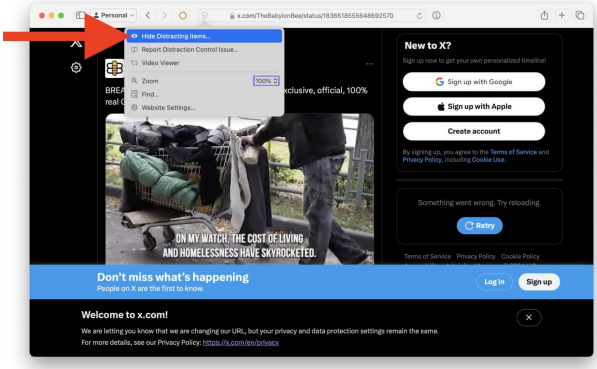
Sie können auf die neuen Fensterkachelfunktionen auf verschiedene Weise zugreifen. Am einfachsten ist es, wenn Sie den Mauszeiger über die grüne Schaltfläche in der Titelleiste eines Fensters halten.

Sie können auch die Optionstaste gedrückt halten, während Sie ein Fenster verschieben, damit die Optionen für die Fensteranordnung auf dem Bildschirm angezeigt werden, wenn Sie den Mauszeiger über das Fenster bewegen.

Sie können auch über das Menü „Fenster" auf die Optionen zum Anordnen von Fenstern zugreifen, indem Sie auf „Verschieben und Größe ändern" gehen und auswählen, an welcher Stelle Sie das Fenster einrasten oder anordnen möchten.

3: Störende Elemente in Safari ausblenden

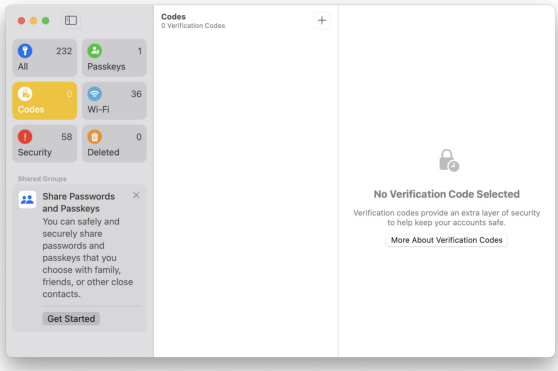
Heutzutage gibt es auf fast jeder Website jede Menge lästige Elemente, die den Bildschirm verstopfen, seien es die riesigen Cookie-Hinweise, automatisch abspielende Videos, „Anmelden mit Google/Microsoft/Facebook"-Pop-ups, Anmeldeaufforderungen, Newsletter-Pop-ups, unangenehme Werbung oder andere lästige oder ablenkende Elemente auf der Seite. Hier kommt die neue Funktion „Ablenkungssteuerung" von Safari ins Spiel, mit der Sie diese störenden Elemente auswählen und verschwinden lassen können.



Sie können die Ablenkungssteuerung in Safari auf jeder Webseite aufrufen, indem Sie in der URL-Statusleiste auf die Schaltfläche „Lesezeichen/Optionen“ klicken, dann „Störende Elemente ausblenden“ wählen und anschließend die störenden Elemente auf dem Bildschirm auswählen, die Sie ausblenden möchten.

4: Passwörter-App

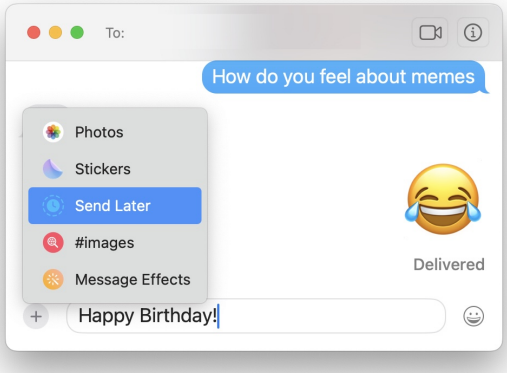
MacOS verfügt jetzt über ein eigenes Programm „Passwörter“, mit dem es einfacher ist, den Überblick über Ihre unzähligen Logins, Wi-Fi-Passwörter, Passkeys und Authentifizierungsdaten zu behalten.



Die Passwörter-App wird auch mit iCloud synchronisiert, wenn du den iCloud-Schlüsselbund verwendest. Das macht sie zu einer echten plattformübergreifenden App und Erfahrung, da die Passwörter-App auch auf iOS 18 und iPadOS 18 läuft.

5: Geplante Nachrichten

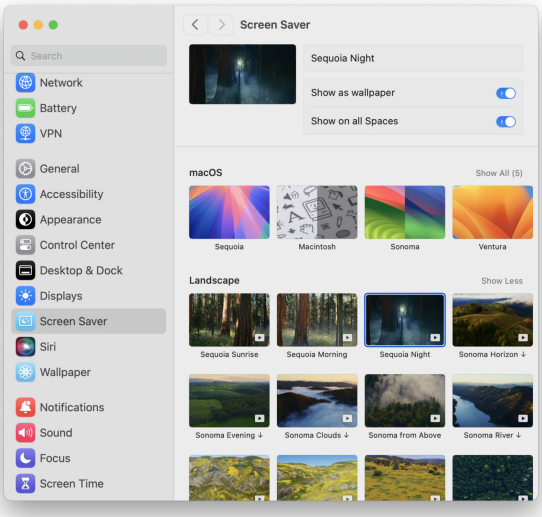
Die Möglichkeit, den Versand von Nachrichten zu planen, wurde schon lange gewünscht und ist nun als Teil von Sequoia verfügbar. Dies ist ideal für das Senden von Nachrichten zu Feiertagen, Geburtstagen, Jahrestagen und vielem mehr.



Um eine Nachricht zu planen, geben Sie einfach die gewünschte Nachricht ein, klicken Sie auf das Pluszeichen (+), wählen Sie „Später senden“ und wählen Sie das Datum und die Uhrzeit, zu der Sie die Nachricht senden möchten.

6: Neue Bildschirmschoner und Hintergrundbilder

Wer liebt nicht schöne neue Hintergrundbilder und Bildschirmschoner? macOS Sequoia ist nach dem berühmten riesigen Sequoia-Baum im Sequoia-Nationalpark benannt, und es gibt einige wunderschöne neue Bildschirmschoner und Hintergrundbilder, die diese Naturschönheiten zeigen.

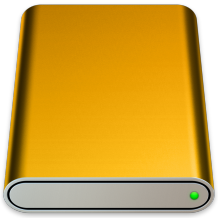


Außerdem gibt es einige lustige neue Optionen für Bildschirmschoner und Hintergrundbilder im Retro-Stil, die Sie sich ebenfalls nicht entgehen lassen sollten.

*Schlussbemerkung: Das Bugfix-Update **Sequoia 15.01** hat einige der Probleme, die in 15.0 existierten, gelöst, so z.B. das Firewall-Problem, durch das Programme plötzlich keinen Zugriff aufs Internet mehr bekamen.*

Welches Festplattenformat?

Howard Oakley, eclecticlight.co • Übersetzung KJM



macOS unterstützt mehrere verschiedene Festplattenformate, von denen jedes seinen Zweck hat. In diesem Artikel wird erklärt, welches der Formate Sie wählen können, wenn Sie eine Festplatte in Sequoia formatieren. macOS unterstützt auch einige andere Formate wie NTFS, die nur zum Lesen verwendet werden können, auf die ich hier aber nicht eingehen werde.

Struktur des Datenträgers

Bevor ein Dateisystem auf einer Festplatte formatiert werden kann, muss der Speicher der Festplatte nach einem der drei Standardschemata partitioniert werden:

- **GUID Partition Map (GPT)**, Standard für die meisten Festplatten und Dateisysteme in macOS;
- **Master Boot Record (MBR)**, früher für MS-DOS und Windows verwendet;
- **Apple Partition Map**, ein altes, von Macs ver-wendetes Format, das Sie vermeiden sollten, wenn Sie nicht wissen, dass es erforderlich ist.

Selbst wenn die gesamte Festplatte nur ein Dateisystem oder ein Volume haben soll, ist eines davon erforderlich, da es Informationen darüber speichert, wie der Speicherplatz auf der Festplatte zugewiesen ist.

Volumes und Container

Abgesehen von APFS benötigen die meisten Dateisysteme, die Sie wahrscheinlich verwenden werden, eine ganze Partition auf der Festplatte für jedes Volume. Eine HFS+-Platte mit zwei Volumes ist beispielsweise in zwei Partitionen unterteilt, die jeweils ein HFS+-Volume enthalten. Da die Partitionierung statisch sein soll, bedeutet dies, dass diese beiden Volumes eine feste Größe haben und keinen freien Speicherplatz zwischen ihnen teilen. Nach der Erstellung ist es möglich, die Partitionierung zu ändern, und das Festplattendienstprogramm wird versuchen, dies zerstörungsfrei zu tun, ohne dass Daten in den Volumes verloren gehen, aber das ist nicht immer möglich.

APFS-Volumes sind anders und teilen sich freien Speicherplatz innerhalb einer Partition, die in der APFS-Terminologie als Container bezeichnet wird. APFS-Container ähneln im Wesentlichen den HFS+-Volumes, da es sich um statische Partitionen handelt, aber APFS-Volumes werden innerhalb ihres statischen Containers dynamisch dimensioniert. Wenn Sie also eine Festplatte mit zwei HFS+-Volumes und zwei APFS-Volumes haben, wird diese Festplatte mindestens drei Partitionen haben:

- eine für jedes der beiden HFS+-Volumes,
- eine als Container für die beiden APFS-Volumes, obwohl sie stattdessen auch jeweils einen eigenen Container erhalten könnten.

Es wird behauptet, dass APFS-Volumes eher wie Verzeichnisse oder Ordner in HFS+ sind, aber das ist verwirrend und sollte ignoriert werden. Jedes APFS-Volume hat sein eigenes Dateisystem, und das Ziehen einer Datei von einem Volume auf ein anderes führt zu zwei völlig getrennten Kopien dieser Datei, die doppelt so viel Speicherplatz benötigen wie eine — so verhalten sich Ordner nicht!

Verfügbare Formate

Das Festplattendienstprogramm Version 22.7 in macOS Sequoia 15.0 kann die folgenden Dateisysteme mit einer GUID Partition Map formatieren:

- APFS, unverschlüsselt und Groß-/Kleinschreibung nicht beachtend
- APFS, verschlüsselt und case-insensitive
- APFS, unverschlüsselt und Groß-/Kleinschreibung beachtend
- APFS, verschlüsselt und Groß-/Kleinschreibung beachtend
- HFS+ gelagert und Groß-/Kleinschreibung nicht berücksichtigend (JHFS+)
- HFS+ protokolliert und Groß-/Kleinschreibung beachtend
- ExFAT
- MS-DOS (FAT32).

Bei Verwendung eines Master Boot Record oder einer Apple Partition Map sind die folgenden Formate verfügbar:

- HFS+ journalled und Groß-/Kleinschreibung nicht berücksichtigend (JHFS+)
- HFS+ journalled und Groß-/Kleinschreibung beachtet
- ExFAT
- MS-DOS (FAT32).

APFS ist nicht kompatibel mit Master Boot Record oder Apple Partition Map.

Das Kommando-Tool `diskutil` bietet zusätzlich noch FAT, FAT12, FAT16, Free Space und HFS+ ohne Journalling, obwohl diese in Disk Utility nicht verfügbar sind.

Beachten Sie, dass verschlüsselte HFS+-Formate im Gegensatz zur Hilfe von Disk Utility nicht mehr in Disk Utility verfügbar sind. Angesichts der Verfügbarkeit verschlüsselter APFS-Formate kann ich mir allerdings nicht vorstellen, warum jemand verschlüsseltes HFS+ verwenden sollte. Das liegt daran, dass die Unterstützung für Verschlüsselung erst später zu HFS+ hinzugefügt wurde, während sie bei APFS von Anfang an vorgesehen war und daher weit überlegen ist.

Welches Format für Macs?

Das Standardformat für Festplatten, auf die von Macs zugegriffen wird, ist jetzt APFS, nicht verschlüsselt und ohne Unterscheidung von Groß- und Kleinschreibung, und sollte mit allen Macs verwendet werden, auf denen Mojave und höher läuft.

Die Unterscheidung zwischen Groß- und Kleinschreibung kann unter bestimmten Umständen wichtig sein. Die beiden Situationen, in denen dies wahrscheinlich erforderlich ist, sind die Speicherung von Time Machine-Backups und Volumes, in denen native Dateien von iOS oder iPadOS gespeichert werden müssen, die APFS mit Groß- und Kleinschreibung verwenden.

Verschlüsseltes APFS unterscheidet sich von FileVault, das auf internen SSDs verwendet wird. Wenn Sie jedoch FileVault auf einer macOS-Installation auf externem Speicher aktivieren, wird dies als verschlüsseltes APFS implementiert. Auf den internen SSDs von Macs mit T2- oder Apple-Silizium-Chips bietet FileVault zusätzlichen Schutz für die Schlüssel, die für die in der Secure Enclave durchgeführte Hardwareverschlüsselung verwendet werden, und sollte daher immer aktiviert sein. Verschlüsseltes APFS wird dringend für Volumes auf externen Festplatten empfohlen, die private oder sensible Daten enthalten, wie z. B. Time Machine-Backups.

Daher sollten Time Machine-Sicherungen auf verschlüsseltem oder unverschlüsseltem APFS mit Groß- und Kleinschreibung erstellt werden.

APFS oder HFS+?

APFS wurde in erster Linie für die Verwendung auf SSDs und nicht auf Festplatten entwickelt und verfügt nicht über Funktionen, die die Leistung bei der Verwendung auf Festplatten erhalten. Sofern ein Volume auf einer Festplatte nicht für die Speicherung von Time Machine-Sicherungen vorgesehen ist, kann es daher immer noch besser sein, eines der unterstützten HFS+-Formate zu verwenden. Die Entscheidung, welches Format besser ist, hängt davon ab, wie das Volume verwendet werden soll.

Da SSDs von der Fragmentierung von genutztem oder freiem Speicherplatz weitgehend unbeeinflusst sind, ist APFS nicht darauf ausgelegt, die Fragmentierung zu minimieren, vielmehr erhöhen einige seiner besten Funktionen zwangsläufig die Fragmentierung. Insbesondere die Dateisystem-Metadaten in APFS-Volumes können stark fragmentiert werden, was zu einer schlechten Leistung auf Festplatten führt. Zwei extreme Beispiele sind Boot-Festplatten und solche, die zum Speichern weitgehend statischer Medienbibliotheken verwendet werden.

Aktuelle Versionen von macOS booten problemlos von externen Festplatten und sind trotz ihrer relativ schlechten Übertragungsraten alles andere als unbrauchbar. Probleme treten auf, wenn Sie diese Festplatte verwenden und Dateivorgänge in Ihrem Home-Ordner durchführen. Im Laufe einiger Wochen oder Monate nimmt die Fragmentierung zu, insbesondere in den Metadaten des Dateisystems, und die Leistung sinkt.

Medienbibliotheken, von denen am häufigsten gelesen wird und deren Dateien relativ wenig geändert werden, weisen weniger Änderungen in ihren Dateisystem-Metadaten auf und leiden möglicherweise nie unter einer spürbaren Leistungsbeeinträchtigung. Dies gilt auch für Time Machine-Backups, auch wenn einige Benutzer nach vielen Monaten oder ein oder zwei Jahren von Leistungseinbußen berichten.

Time Machine in Sequoia startet keine neuen Sicherungsserien mehr auf HFS+; wenn Sie versuchen, eine Festplatte mit einem einzelnen HFS+-Volume als Sicherungsspeicher hinzuzufügen, wird die Festplatte automatisch in einen APFS-Container mit einem einzelnen APFS-Volume konvertiert, das die Groß-/Kleinschreibung beachtet, und dieses wird zum Speichern der Sicherungen verwendet. Sie können jedoch immer noch Sicherungsprogramme von Drittanbietern wie Carbon Copy Cloner verwenden, um Sicherungen auf HFS+-Volumes zu erstellen, obwohl jetzt APFS empfohlen wird. Dies kann mehrere erhebliche Nachteile haben, unter anderem:

- Es können keine Schnappschüsse vom Sicherungsspeicher erstellt werden.
- APFS spezielle Dateitypen werden nicht unterstützt. Bei spärlichen Dateien kann dies dazu führen, dass die Sicherungen wesentlich größer sind als die Quelldateien. Schlimmer noch: Wenn Sie eine gesicherte Sparse-Datei wiederherstellen, wird sie nicht automatisch in das Sparse-Dateiformat von APFS zurückkonvertiert.
- Das Kopieren von Blöcken wird in der Regel nicht unterstützt, was wiederum dazu führt, dass die Sicherungen größer werden und mehr Zeit für die Sicherung benötigt wird.
- Sofern verfügbar, können inkrementelle Sicherungen aufgrund der Anzahl von Dateien und Ordnern unhandlich werden.

Grundsätzlich können sowohl APFS als auch HFS+ auf APFS-Sicherungsspeicher gesichert werden, während HFS+-Speicher nur für Sicherungen von HFS+ geeignet sind.

Welches Format für Windows-Kompatibilität?

Obwohl andere Computer HFS+ und manchmal sogar APFS-Datenträger lesen können, wissen nur wenige ihrer Benutzer, wie sie auf die nativen Dateisysteme des Mac zugreifen können. Wenn Sie von anderen Computern aus auf Ihren Speicher zugreifen wollen, ist eines der beiden unterstützten MS-DOS/Windows-Formate am besten geeignet.

Die Informationen in der Hilfe des Festplattendienstprogramms sind etwas irreführend, wenn es um die Wahl zwischen FAT32 und ExFAT geht. FAT32 bietet eine maximale Datenträgergröße von 2 TB mit Dateien von bis zu fast 4 GB pro Stück, ist aber in erster Linie für magnetische Datenträger gedacht.

Sofern das System, das den Datenträger lesen soll, nicht auf FAT32 beschränkt ist, ist es im Allgemeinen vorzuziehen, stattdessen ExFAT zu verwenden. Dieses Format unterstützt große Volumina und Dateigrößen und wurde für die Verwendung in Flash-Speichern optimiert. ExFAT ist daher das am häufigsten anzutreffende Format für USB-Flash-Laufwerke (Thumb Drives, Memory Sticks) und SD-Karten, wobei es das Standardformat für SDXC- und SDUC-Karten mit mehr als 32 GB ist.

FAT32 und ExFAT werden sowohl mit GUID Partition Map als auch mit Master Boot Record Schemata unterstützt. Sofern der andere Computer oder das andere System nicht sehr alt ist, sollten Sie GUID Partition Map bevorzugen. Keines der beiden Datenträgerformate unterstützt Verschlüsselung. Wenn Sie also Dateien schützen wollen, sollten Sie sie separat verschlüsseln oder in einem zugänglichen verschlüsselten Archivformat speichern.

Zusammenfassung

- Für allgemeine Zwecke sollte das Standard-Datenträgerformat eine GUID Partition Map mit entweder einfachem oder verschlüsseltem APFS verwenden.
- Verschlüsseltes APFS sollte für Volumes auf externen Festplatten verwendet werden, die private oder sensible Daten enthalten. File Vault sollte auf internen SSDs aktiviert werden.
- Neue Time Machine-Backups können jetzt nur noch auf APFS mit Groß-/Kleinschreibung, entweder einfach oder verschlüsselt, erstellt werden.
- Festplatten mit aktiven Dateisystemen können mit APFS eine schlechte Leistung aufweisen, und HFS+ mit Journalling kann immer noch vorzuziehen sein, hat aber erhebliche Einschränkungen und Nachteile.
- Festplatten, die eher statisch genutzt werden, z. B. für Medienbibliotheken und Backups, sollten mit APFS sicher sein, können aber unter Umständen eine schlechte Leistung aufweisen.
- Wenn es keine guten Gründe für die Verwendung von FAT32 gibt, formatieren Sie USB-Flash-Laufwerke, SDXC- und SDUC-Karten, die mit Nicht-Mac-Systemen verwendet werden müssen, mit ExFAT in einem GUID-Partitionierungsschema.