TRIM für SSD Drives - eine Zusammenfassung

Ein macintouch.com-Leser fragte kürzlich:

Nachdem ich das Web abgesucht und viele Artikel [über SSDs] gelesen habe, bin ich immer noch definitiv verunsichert über das „ob", bei welcher Marke, „warum/warum nicht" bezüglich des Aktivierens von TRIM (im Gegensatz zur eingebauten Garbage Collection) und des Optimierens der Lebensdauer.

Viele definitive Aussagen, die ich kürzlich erst gelesen habe, sind tatsächlich drei (oder mehr) Jahre alt. Viele andere definitive Aussagen sind markenspezifisch und nicht zu verallgemeinern. Da ich kurz davor stehe, mein MacBook Pro mit einer SSD aufzurüsten, wäre es wirklich nett, den aktuellsten „definitiven" Ratschlag zu bekommen.

Herausgeber Ric Ford antwortete darauf:

Dieses Thema ist bei uns im Laufe der Zeit fast zu Tode diskutiert worden, und man kann all die Details, Links und Referenzen in unseren archivierten Reader-Reports nachlesen, aber ich werde versuchen, ein Fazit zu ziehen, da ich das Thema aufmerksam verfolgt habe… -Ric Ford

- TRIM bietet einzigartige Vorteile (bessere Langlebigkeit/Abnutzungs- und Leistungswerte), die von nichts anderem geboten werden (das beinhaltet "garbage collection" und "overprovisioning"). Es is besonders wertvoll, wenn ein SSD sich allmählich füllt und/oder für sehr große Dateien genutzt wird.
- TRIM's Vorteile mögen weniger bemerkbar sein für Leute, die viel freien Platz auf ihrem SSD haben und eher alltägliche Dinge tun wie z.B. Textbearbeitung, Surfen im Web usw.
- TRIM fügt eine Ebene an Komplexität hinzu, auf der auch die Gefahr besteht, dass Bugs schlimme Auswirkungen wie Datenzerstörung haben können, aber die weit verbreitete, erfolgreiche Anwendung von TRIM legt die Vermutung nahe, dass dies mit guten, modernen Mainstream-SSDs und -Computern wohl kein Problem ist.
- TRIM arbeitet nur mit internen Laufwerken; es wird weder von FireWire- noch von USB-Geräten unterstützt (so weit ich es feststellen kann). Es mag vielleicht mit Thunderbolt und/oder eSATA Laufwerken funktionieren.
- Apple benutzt TRIM für seine eigenen SSD (die sogenannten „Flash"-Speichersysteme), z.B. im MacBook Air und in Retina MacBook Pro Modellen (ebenso wie in Benutzer-konfigurierten Modellen mit Flash Drives). Apple hat einige defekte SSDs verkauft, die zurückgerufen werden mussten, aber keine Details über den Defekt veröffentlicht.
- Angelbird SSD wrk ist das einzige SSD eines Fremdherstellers, das von vornherein in Apple's OS X Software mit TRIM unterstützt wird. Dies sind nicht die billigsten SSDs, aber ich habe noch von keinerlei Problemen damit gehört, und es scheint eine gute Wahl für jemand zu sein, der einfache TRIM-Unterstützung sucht.
- Cindori Software's **Disk Sensei** scheint für SSDs von anderen Herstellern eine gute Wahl zu sein, obwohl Apple in OS X 10.10 endlich eine gut versteckte Einstellmöglichkeit hinzugefügt hat, mit der man TRIM auf Laufwerken anderer Hersteller mit einem Unix-Befehlszeilenprogramm (**trimforce**) im Terminal aktivieren kann.
- Ob TRIM aktiv ist oder nicht, findet man hier: `About This Mac > More Info > Serial-ATA > your SSD > TRIM Support [Yes/No]`

Ein Leser kommentierte:

Ric's Zusammenfassung über TRIM ist excellent. Wenn ich riskieren darf, einen Punkt über das Einbauen eines SSDs in ein System hinzuzufügen, würde ich sagen: Wenn Du überlegst, eine Festplatte mit einem SSD zu ersetzen, besonders, wenn es um die Boot Disk des Rechners geht, dann lass Dich nicht von Fragen oder Bedenken über TRIM davon abhalten – nicht einmal eine Sekunde. Die Vorteile eines SSDs sind enorm, und selbst, wenn Du der ziemlich seltene Fall bist, der TRIM nicht aktivieren kann oder möchte, wirst Du immer noch eine große Verbesserung sehen.

Es mag Ausnahmen oder Grenzfälle geben; die meisten anderen aber werden eine gewaltige Leistungssteigerung durch das SSD erleben, mit oder ohne TRIM.

Das ist nur meine Meinung, und ich würde immer noch sagen, TRIM sollte aktiviert sein, aber ich wollte betonen, dass TRIM weniger wichtig ist als überhaupt ein SSD zu nutzen. Ich habe vielleicht ein halbes Dutzend Festplatten durch SSDs ersetzt in relativ alten MacBooks, und jeder Anwender hat gesagt, es sei wie ein neuer Computer.

Antwort von Ric Ford:

Ich stimme völlig überein bezüglich der Leistung von SSDs, die überwältigend ist, und TRIM beeinflusst dies tatsächlich eher unmerklich. Ich vergaß auch, zu erwähnen, dass aktuelle Mainstream SSDs eine bemerkenswerte Langlebigkeit haben und möglicherweise länger halten als rotierende Festplatten. Es fällt schwer, einen Grund zu finden, ein Arbeitssystem nicht mit einem SSD upzugraden, obwohl ich Festplatten immer noch als Speichermedien für Backups und Archive mag.

Übersetzung: KJM

Soll man seine Daten in der Cloud speichern?

von Wendy Zamora, blog.malwarebytes.org
Übersetzung: KJM

Es ist ziemlich einfach, zu verstehen, wohin eine Datei geht, wenn man sie auf seinem PC speichert. Sie liegt auf Deiner Festplatte, vielleicht beherbergt in einer Reihe von Ordnern, die Du selbst angelegt und angeordnet hast. Diese Datei ist nur auf Deinem Rechner gespeichert, es sei denn, Du entscheidest, sie an Dich selbst zu mailen oder sie auf einer externen Festplatte oder einem USB-Stick zu speichern.

Wie ist das in der Cloud?

Ganz einfach gesagt, ist „die Cloud" nur ein modischer Ausdruck für ein Netzwerk von miteinander verbundenen Servern (ein Server ist einfach ein Computer, der Daten oder Dienste anderen Computern zur verfügung stellt). Wenn Du Dateien in die Cloud speicherst, können sie von einem Computer aus genutzt werden, der mit dem Netzwerk dieser Cloud verbunden ist. Nun nimm diese Idee und multipliziere sie, um zu verstehen, wie die Cloud für Dich funktioniert. Die Cloud besteht nicht nur aus ein paar Servern, sondern aus einem Netzwerk vieler Server, die typischerweise in einem Raumschiff-artigen Lagerhaus aufgebaut sind – oder in mehreren hundert Raumschiff-großen Lagerhäusern. Diese Lagerhäuser werden bewacht und verwaltet von Firmen wie Google (Google Docs), Apple (iCloud) oder Dropbox.

Es ist also kein irgendwie nebulöses Konzept. Es ist physisch, anfassbar, real.

Wenn Du Dateien in die Cloud speicherst, kannst Du auf sie von jedem Computer aus zugreifen, vorausgesetzt, er ist mit dem Internet verbunden und Du hast Dich in die Plattform Deines Dienstes eingeloggt. Nehmen wir z.B. Google Drive. Wenn Du Gmail benutzt, kannst Du überall auf den Drive zugreifen, wo Du auch Deine Mail abrufen kannst. Melde Dich bei dem Dienst an, und Du findest Deine ganze Bibliothek an Dokumenten und Fotos beieinander.

Warum machen sich Leute Sorgen über die Sicherheit in der Cloud?

Es ist physisch nicht mehr in Deiner Hand. Du speicherst nicht auf eine Festplatte bei Dir zuhause. Du sendest Deine Daten zu einer anderen Firma, die Deine Daten vielleicht tausende Kilometer entfernt aufbewahrt; daher hängt es von ihnen ab, diese Informationen sicher zu speichern. „Ob Daten automatisch gesendet werden (man denke an Apps, die Daten automatisch mit der Cloud synchronisieren) oder manuell von Anwendern, die Fotos auf soziale Medien hochladen, das Endresultat ist, dass all das irgendwo notiert und gespeichert wird", sagt Jérôme Segura, Senior Security Researcher bei Malwarebytes.

Und dieses Irgendwo ist ein Platz, der nicht unter Deiner direkten Kontrolle ist.

Risiken der Speicherung in der Cloud

Die Sicherheit der Cloud ist gut, aber nicht unverletzbar. Cyber-Kriminelle können an diese Dateien kommen, entweder indem sie Sicherheitsfragen erraten oder Passworte umgehen. Das ist, was beim großen iCloud Hack von 2014 passierte, wo Nacktbilder von Prominenten erbeutet und online publiziert wurden.

Aber das größere Risiko der Datenspeicherung in der Cloud ist die Privatsphäre. Selbst wenn keine Daten gestohlen oder publiziert werden, können sie noch gesehen werden. Regierungen können gesetzmäßig Informationen anfordern, die in der Cloud gespeichert sind, und es liegt an den Cloud-Service-Providern, ob sie den Zugriff verweigern. Zehntausende Anfragen nach Benutzerdaten werden von Regierungsagenturen jedes Jahr an Google, Microsoft und andere Firmen geschickt. Meistens händigen die Firmen zumindest einen Teil der Daten aus, selbst wenn es nicht der komplette Inhalt ist.

„Manche Leute argumentieren, dass sie nichts zu verbergen haben, dass sie nichts Falsches tun, und dass es sie nicht kümmert, ob irgendwer auf ihre private Information zugreift, besonders, wenn das bei der Verfolgung von Terroristen helfe", sagt Segura. „Es gibt zwar keinen Zweifel daran, wie wertvoll der Zugang zu Daten für die Geheimdienste ist, aber es ist wichtig, daran zu erinnern, dass jedes Individuum ein grundsätzliches Recht auf Privatsphäre hat."

Vorteile der Datenspeicherung in der Cloud

Andererseits sind die Daten, die man in der Cloud speichert, weit besser gesichert als auf der eigenen Festplatte. Cloud-Server stehen in Lagerhäusern, weit weg von den meisten Angestellten, und sie werden schwer bewacht. Zusätzlich sind die Daten auf den Servern verschlüsselt, was es Angriffe darauf zu einer mühsamen, wenn nicht sogar furchterregenden Aufgabe für Hacker macht, während eine Malware-Infektion des Computers zuhause alle persönlichen Daten Cyber-Gangstern zugänglich und die Daten sogar verletzlich machen kann gegenüber Ransomware-Bedrohungen. Tatsächlich empfehlen wir, zum Schutz gegen Ransomware die Daten lieber bei einem Cloud-Service zu speichern.

Weitere Vorteil der Datenspeicherung in der Cloud sind die Kosteneffektivität und der einfache Zugang. Man kann Tonnen an Daten oft kostenlos speichern, wenn man die Cloud benutzt. Vergleich das einmal mit der Anzahl an externen Festplatten und USB-Sticks, die Du kaufen musst, und auch die Schwierigkeit, auf die Daten zuzugreifen, wenn Du sie auf mehrere Geräte verteilt hast, und Du siehst, weshalb Datenspeicherung in der Cloud für Firmen und für Konsumenten gleichermaßen eine populäre Option geworden ist.

Das Fazit

Ja, Deine Daten sind relativ sicher in der Cloud – vermutlich viel sicherer als auf Deiner eigenen Festplatte. Zusätzlich kannst Du einfach auf Deine Daten zugreifen und sie pflegen. Dennoch legen Cloud-Dienste letzten Endes Deine Daten in fremde Hände. Wenn Du Dir keine besonderen Sorgen über die Privatsphäre machst, dann ist das kein Grund zur Aufregung. Aber wenn Du sensible Daten hast, die Du vor neugierigen Augen schützen möchtest, speicherst Du sie vielleicht am besten auf einer externen Festplatte, die dann von Deinem Computer zuhause abgekoppelt bleibt.

Wenn Du bereit bist, Daten in der Cloud zu speichern, schlagen wir vor, Du suchst Dir einen Cloud Service mit Multi-Faktor-Authentifizierung und Verschlüsselung aus. Befolge außerdem die folgenden Ratschläge, um Deine Daten in der Cloud sicher zu halten:

- Benutze **„hardcore" Passworte**: Für die Datenspeicherung in der Cloud sollte man lange und zufällige Passworte benutzen. Nutze nie dasselbe Passwort zweimal!
- Sichere Deine Daten auf mehreren **verschiedenen Cloud-Konten**: Leg nicht all Deine wichtigen Daten an einen Platz!
- Praktiziere **Smart Browsing**: Wenn Du an einem öffentlichen Computer auf die Cloud zugreifst, denk daran, Dich wieder auszuloggen, und speichere nie Deine Passwort-Informationen.