

FAST LTA
Wir sichern Terabytes.

COLD STORAGE

Tape, Disk oder Cloud?

ÜBERDENKEN SIE IHRE BACKUP-STRATEGIE



Hallo,

wir sind die **FAST LTA AG**.

Unser Firmensitz ist in der Rüdeshheimer Str. 11 in 80686 München, Deutschland. Sie erreichen uns telefonisch unter +49 (89) 890 47 - 0, per Fax unter +49 (89) 890 47 - 890 und via E-Mail über info@fast-lta.de. Beim Amtsgericht München sind wir unter der HRB 127 484 eingetragen, unsere USt-ID ist DE204232266. Die Kontodaten bei der Kreissparkasse München Starnberg sind IBAN DE76 7025 0150 0022 2363 19 und BIC BYLA DE M1 KMS. Im Vorstand sitzen Matthias Zahn, Jörg Adelstein und Reiner Bielmeier, der Vorsitzende des AR ist Jens Gloede. Im Internet finden Sie uns unter www.fast-lta.de.

DISCLAIMER

Das Dokument erhebt keinen Anspruch auf Vollständigkeit. Änderungen jederzeit vorbehalten. Alle Bilder und Marken sind Eigentum ihrer jeweiligen Rechteinhaber. Veröffentlichung - auch auszugsweise - nur nach ausdrücklicher Genehmigung von FAST LTA.

Raus aus dem Backup-Dilemma

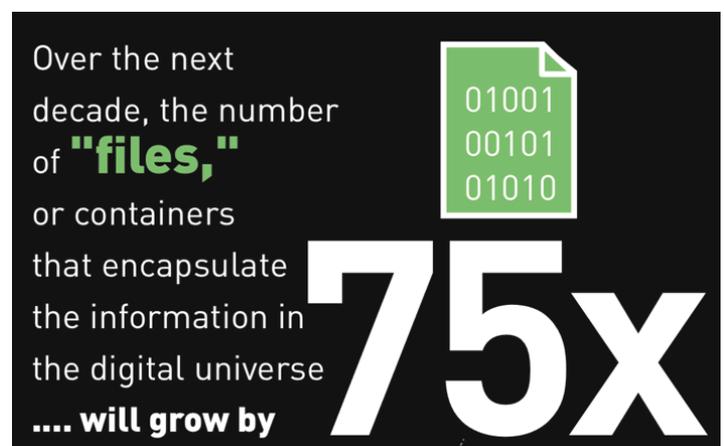
Derzeit wird wieder an allen Ecken und Enden über Backup-Strategien diskutiert. Während von der einen Seite Cloud Backups als Allheilmittel gepriesen werden, konzentrieren sich andere darauf, bestehende Technologien marginal zu verbessern.

Dass Backups ein notwendiges Übel sind, weiß inzwischen jeder IT-Verantwortliche. Dass aber die ständig wachsenden Datenmengen nicht nur gespeichert, sondern auch gesichert werden müssen, stellt bisherige Backup-Strategien und –Technologien zunehmend vor Herausforderungen. Ein großer Teil der gespeicherten Daten ändert sich jedoch so gut wie nie mehr und ist zudem selten im Zugriff – ist aber mangels Anfangssicherheit im Speichersystem weiter Teil des Backup-Prozesses und verstopft diesen damit. Die Folgen: Immer länger werdende Backup-Fenster, zerstückelte Backup-Strategien, komplexe Multi-Tier-Setups mit jeweils eigenen Backup-Prozessen – und haufenweise Probleme beim Restore, sollten doch einmal Daten verloren gehen.

Der einzige Ausweg, der auch langfristig Entlastung bringt, ist, die Datenmenge im Backup zu reduzieren. Das gelingt nur, wenn das Speichersystem, auf dem der Großteil der anfallenden Daten gespeichert ist, bereits so sicher ist, dass kein zusätzliches Backup notwendig ist.

Die Explosion der statischen Daten

Schon 2011 hat das Marktforschungsinstitut IDC vorhergesagt, dass die zu speichernden Daten in 10 Jahren um das 75fache steigen werden¹.

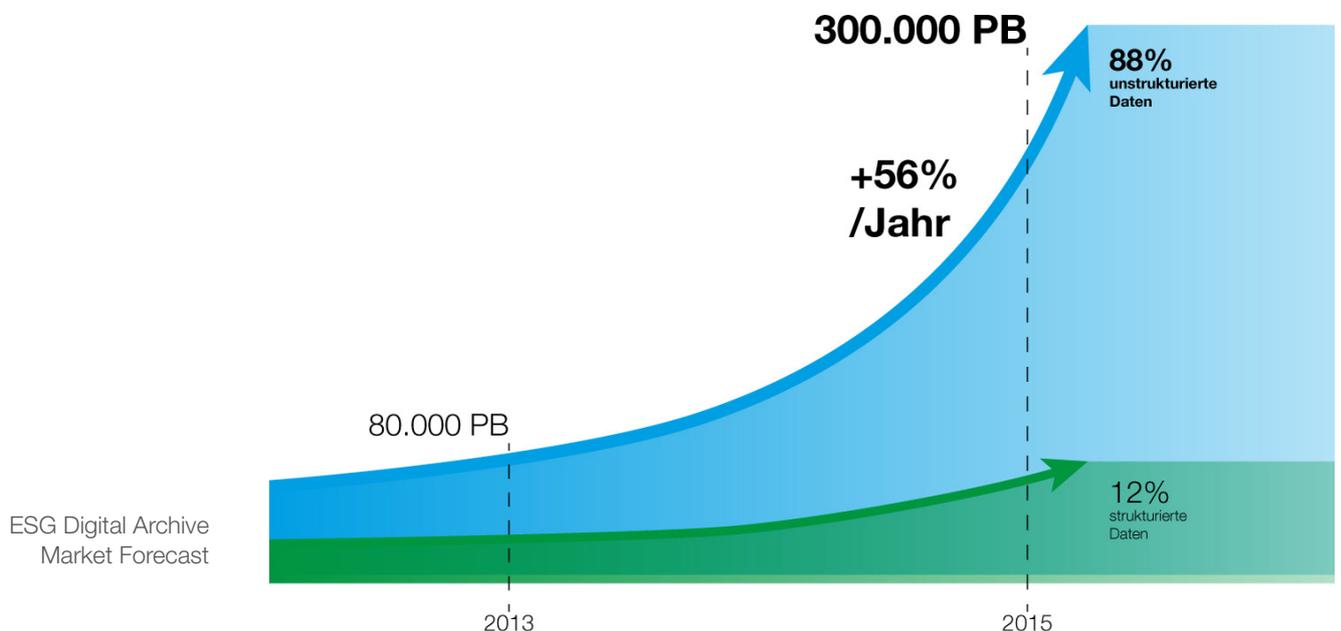


IDC Digital Univers
Infographic

¹ IDC „Digital Universe 2011 Infographic“, <http://germany.emc.com/collateral/about/news/idc-emc-digital-universe-2011-infographic.pdf>

Diese Explosion an Informationen hat Auswirkungen auf alle Unternehmen: Der Bedarf an Speicher wächst rasant, gleichzeitig sollen alle Daten verfügbar, abgesichert gegen unbefugten Zugriff und jederzeit reproduzierbar sein. Dem gegenüber stehen allerdings IT-Budgets, die das Datenwachstum nicht widerspiegeln. Tatsächlich sanken 2013 die geplanten Ausgaben für Storage bei Konzernen um 19 Prozent und bei größeren Mittelständlern um 22 Prozent, ermittelte das Marktforschungsunternehmen 451 Research².

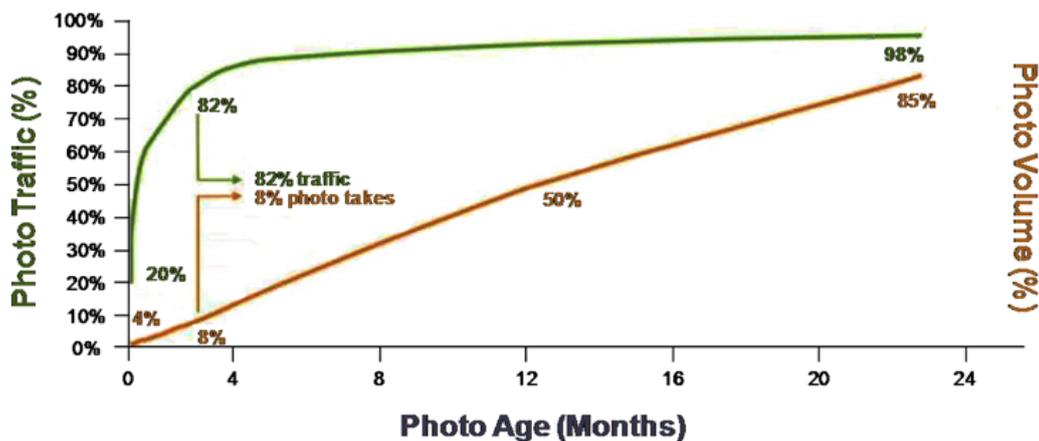
Ganz besonders stark steigen inzwischen die so genannten statischen Daten - also die Daten, die nach der Speicherung kaum mehr abgerufen und so gut wie nie verändert werden. Schnellere Netzwerke, überall verfügbares Internet, und hochauflösende Bilder und Videos im privaten wie im professionellen Bereich tragen ebenso dazu bei wie die Sammelwut, die durch Trends wie Big Data und Soziale Netzwerke hervorgerufen wird.



² Simon Robinson, "Survey: Storage Budgets shrink while Capacity balloons", Computer Weekly, 3. Juli 2014, <http://bit.ly/1Bvi0Es>

Alle Daten müssen ständig verfügbar sein

Dabei müssen diese Daten, obwohl selten benötigt, jederzeit verfügbar sein. Beispiel Facebook: Der Löwenanteil von 82% des durch Fotos generierten Traffics wird bereits nach 3 Monaten von nur 8% der Fotos erreicht³. Durch die „Search & Browse“-Mentalität müssen jedoch alle Fotos stets verfügbar sein, da niemand vorhersagen kann, nach welchen Kriterien morgen gesucht wird.



Quelle: Facebook

Noch wichtiger ist natürlich, dass keine Daten verloren gehen.

³ IDC, „Cold Storage is Hot Again“, Studie 2013, <http://www.storiant.com/resources/Cold-Storage-Is-Hot-Again.pdf>

Backup & Restore – ungeliebte Geschwister

Deshalb stellt sich überall, wo Daten erfasst und gespeichert werden, auch die Frage nach dem Absichern gegen Datenverlust. Wie bei gedrucktem Papier ist dabei die einfachste Methode, eine Kopie anzulegen - ein „Backup“. Der Sinn dieses Backups ist seit jeher klar: Falls das Original beschädigt oder verloren geht, springt die exakte Kopie in die Bresche. Im Digitalen muss dabei die Kopie nicht physikalisch bewegt werden, das Original wird vielmehr daraus wieder hergestellt - der „Restore“.

Backup auf Tape

Da aufgrund der ständig steigenden Anforderungen an Kapazität und Geschwindigkeit die Speichersysteme auch immer teurer wurden, ging man dazu über, die Backup-Kosten stark zu optimieren. Für Backups werden die günstigsten Medien verwendet (Tapes), vollständige Kopien werden nur in bestimmten Abständen angelegt. Dazwischen werden nur die veränderten und neu hinzugekommen Daten gesichert. Durch die so erlangte Komplexität ist ein Restore einzelner Dateien meist aufwändig und zeitraubend. Soll ein kompletter Datenbestand wieder hergestellt werden, müssen unter Umständen neben dem letzten Full Backup noch diverse inkrementelle und differenzielle Backups wieder eingespielt werden. Da Tapes einer gewissen Alterung unterliegen und zur Überprüfung aufwändig eingelegt und komplett gelesen werden müssten, wird ein Datenverlust auf den Backup-Medien meist auch erst im Ernstfall festgestellt. Dass Daten in einem Tape Backup & Restore nicht wieder hergestellt werden können, ist gar nicht so selten. Hauptgrund dafür ist fehlerhafte Hardware und Medien, was dazu führt, dass bis zu 50% aller Restores von Tape Backups mit Datenverlust verbunden sind⁴.

⁴ SOURCEIT Technologies, <http://www.sourcit.net/services/cloud-backup-recovery/compared-to-tape-backup/>

Im Grunde beruhen viele Tape-Backup-Strategien also auf dem Prinzip Hoffnung: Da niemand genau weiß, ob die Backups vollständig intakt sind, hofft man einfach, dass man sie nie brauchen wird. Dazu passt auch, dass laut einer Studie nur 34% aller Anwender ihre Backups-Tapes nach dem Schreiben überprüfen. Noch schlimmer: erschütternde 77% davon stellen dabei Fehler fest⁵.

Backup auf Disk

Ebenfalls schon 2011 wurde in einer Studie festgestellt, dass 80% der europäischen IT-Manager weg vom Tape und Disk-Arrays als Backup nutzen wollen. Der Hauptgrund dafür ist die Geschwindigkeit, was in verkürzten Backup-Fenstern und schnellerem Restore resultiert⁶.

Grundsätzlich eine gute Idee, die zudem mehrere Vorteile mit sich bringt. Daten lassen sich auf Festplattenspeichern mittels diverser Redundanzmechanismen besser gegen Verlust absichern. RAID-6 verkraftet beispielsweise in der Theorie den Ausfall von 2 Festplatten eines Verbundes – beim Tape müsste man dafür 2 Kopien ziehen. In der Praxis gibt es diverse Faktoren, die diese Ausfallsicherheit jedoch drastisch reduzieren, so dass auch das Backup wiederum nicht als sicher gilt, wenn nicht mindestens eine Kopie davon existiert.

Oft wird deshalb ein komplexes Disk-to-Disk-to-Tape-Backup aufgesetzt, um einerseits schnellen Restore zu ermöglichen, andererseits im Extremfall noch auf eine Tape-Kopie zurückgreifen zu können. Dass diese Strategie die Komplexität enorm vergrößert, liegt auf der Hand.

5 Storage Magazine, storagemagazine.techtarget.com

6 EMC, „European Disaster Recovery Survey“, Studie 2011, <http://germany.emc.com/microsites/2011/emc-brs-survey/index.htm>

Backup in die Cloud

Inzwischen etabliert sich ein dritter Weg, Daten abzusichern: die Cloud. Dabei werden Daten ganz einfach nicht mehr lokal auf eigenen sondern verteilt auf von Dienstleistern bereitgestellten Medien gespeichert. Das komplizierte Hantieren mit Tapes entfällt, die Anbieter versprechen hohe Ausfallsicherheiten. Eine aktuelle Studie zeigt jedoch: fast ein Drittel aller Cloud-Anwender haben in der Cloud bereits Daten verloren⁷.

Was für die Zusammenarbeit und das Verteilen von Daten durchaus Sinn macht – nämlich der weltweite Zugriff auf die Daten in der Cloud – ruft allerdings für unternehmenskritische Daten zunehmend Sicherheitsbedenken hervor. Vor allem weltweit operierende Anbieter kämpfen mit den unterschiedlichen rechtlichen Vorgaben und Anforderungen, die oft im Gegensatz zum Anspruch der Unternehmen stehen: dass niemand außer Berechtigte auf die Daten Zugriff haben.

Cloud-Backups haben noch einen entscheidenden Nachteil: Je nach Anbindung und Ausstattung des Dienstleisters dauert es durchaus lange, bis Daten für ein Restore zur Verfügung stehen. Datenmengen von mehreren Terabyte aus der Cloud wieder herzustellen ist eigentlich nicht vorgesehen. Cloud-Backups lösen also wenn überhaupt dann nur das Tape als letzten Tier ab, die Empfehlung lautet: Disk-to-Disk-to-Cloud, was weder die Komplexität verringert noch die Kosten entscheidend reduziert.

⁷ Aberdeen Group, „SaaS Data Loss: The Problem You Didn't Know You Had“, <http://v1.aberdeen.com/launch/report/perspective/8323-AI-cloud-data-loss.asp>

Der Weg aus dem Backup-Dilemma

Wie oben beschrieben war ja schon vor 4 Jahren klar, dass die Datenmengen explodieren würden. Der Ersatz des Backup-Mediums ist deshalb nur eine kurzfristige Lösung, oder besser ein Hinauszögern des eigentlichen Problems: Es werden einfach zu viele Daten produziert. Und aktuelle Backup-Strategien sind zu komplex und zu unsicher. Wie die aktuelle Gartner-Studie „The Broken State of Backup“⁸ belegt, sind überhaupt nur 75-85% aller Backups erfolgreich, ermöglichen also eine vollständige Wiederherstellung korrupter Daten.

Der einzige Weg aus dem Backup-Dilemma ist die Menge der Daten nachhaltig zu reduzieren. Nur durch das Weglassen von Backups für Daten, die sich sowieso nie wieder ändern und höchst selten im Zugriff sind, kann die Business Continuity bei unternehmenskritischen, sich oft ändernden Daten, die im ständigen Zugriff sind und deshalb weiterhin regelmäßig gesichert werden müssen, gewährleistet werden.

Wohin mit den statischen Daten?

Die Schwierigkeit dabei ist die Identifikation dieser Daten. Manche Bereiche können leicht klassifiziert werden: Datenbanken, virtuelle Maschinen, aktuelle Projekte - alles kritische Daten, die im ständigen Backup-Prozess bleiben müssen. Aber der Großteil der anderen, statischen Daten ist schwer zu klassifizieren - vor allem, wenn unklar ist, von wo aus auf diese Daten zugegriffen werden soll. Online-Archive unterliegen Trends, die plötzlich die Verfügbarkeit von bestimmten Inhalten erfordern. Aktuelle Ereignisse führen dazu, dass Medien, die Monate und Jahre lang nicht benötigt wurden, plötzlich massenhaft angefragt werden. Big Data Analysen müssen auf jeden Datensatz Zugriff haben, der jemals gespeichert wurde.

Meist gibt es deswegen eine Multi Tier Strategie: Geschwindigkeit und Verfügbarkeit werden durch deutlich höhere Kosten pro TB erkaufte. SSD-Arrays werden dabei für agile Daten die

⁸ Gartner, „The Broken State of Backup“, http://cdn2.hubspot.net/hub/30865/file-25654811-pdf/docs/gartner_-_the_broken_state_of_backup_%286-09%29_%281%29.pdf

heute üblichen Festplatten-Arrays ablösen, unter anderem weil durch fehlende Mechanik weniger Probleme durch Fragmentierung auftreten. Tapes werden zunehmend nurmehr als „Datenfriedhof“ genutzt - also als letzte Instanz für Daten, die ohne Zugriffsmöglichkeit archiviert werden sollen.

Disk Libraries

Dazwischen machen sich Disk Libraries breit, die große Datenmengen verfügbar speichern können. Herkömmliche Disk Libraries bringen jedoch eine Reihe von Nachteilen mit sich. Durch die enorme Fragmentierung müssen z.B. stets alle Festplatten der Library in Betrieb sein, was Energie kostet und die mechanischen Festplatten belastet und somit schneller altern lässt⁹. Wie oben beschrieben sind herkömmliche Disk Libraries auch einfach nicht sicher genug, um auf eine zusätzliche Sicherung für ein mögliches Disaster Recovery zu verzichten.

⁹ FAST LTA, „White Paper: Linear Disk Storage“, 2015 , <http://www.silentbricks.de/de/linear-disk-storage/>

Linear Disk Storage mit Erasure Coding

Eine Kombination neuer Technologien bietet sich an, diese Probleme zu lösen und damit tatsächlich dafür zu sorgen, dass Backups um die statischen Daten reduziert werden können, ohne dass die Kosten explodieren.

Linear Disk Storage

Linear Disk Storage sorgt dafür, dass zusammen gehörende Daten auch zusammenhängend gespeichert werden. Nur so ist ein effizientes Energiemanagement möglich, das langfristig die Verbrauchskosten minimiert. Die unfragmentierte Speicherung bringt weitere Vorteile mit sich: So lassen sich Daten wie bei der Speicherung auf Tape leicht transportieren, aber auch aus dem System entfernen¹⁰.

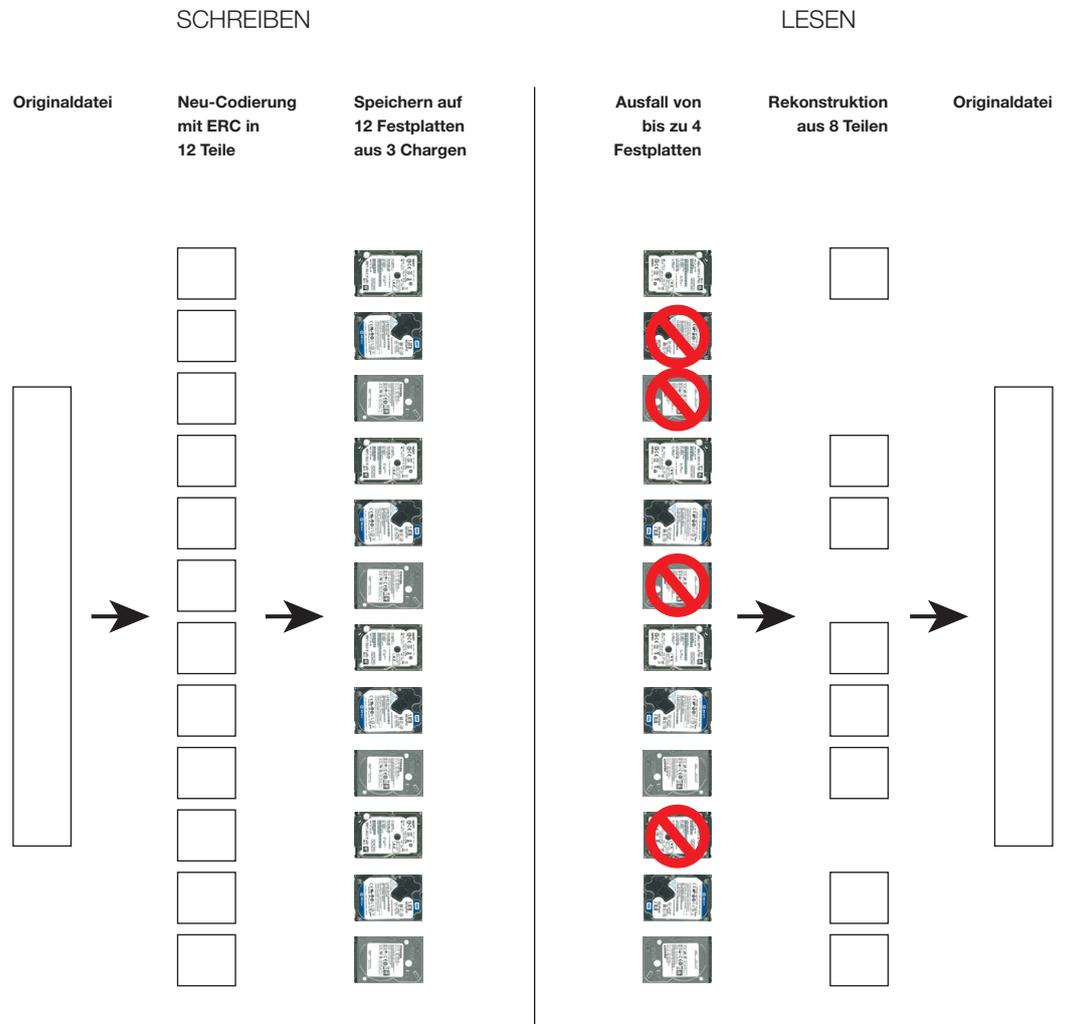
Erasure Coding

Der zweite Baustein ist die Erhöhung der Sicherheit. Da RAID-Speicher auf Dauer einfach nicht sicher genug sind¹¹, schickt sich Erasure Resilient Coding (ERC, auch kurz: Erasure Coding) an, der neue Standard für die Absicherung von Daten durch Redundanzkodierung zu werden.

Erasure Coding bezeichnet ein mathematisches Verfahren zum Datenschutz, das Daten in Fragmente aufteilt, erweitert und neu mit redundanten Teilen codiert, die dann auf physikalisch getrennten Orten (z.B. Standorten oder Medien) gespeichert werden. Das Ziel von Erasure Coding ist die zuverlässige Wiederherstellung von verlorenen Teilen aus den Informationen von anderen Datenteilen aus dem Verbund. Erasure Coding wird zunehmend statt

¹⁰ FAST LTA, „White Paper: Linear Disk Storage“, 2015 , <http://www.silentbricks.de/de/linear-disk-storage/>

¹¹ Robin Harris, „Why RAID-6 stops working in 2019“, ZDnet 2010 , <http://www.zdnet.com/article/why-raid-6-stops-working-in-2019/>



Beim Erasure Coding im ERC 8/12-Schema können bis zu 4 beliebige Festplatten ausfallen, ohne dass Daten verloren gehen

RAID verwendet, da die Komplexität zur Wiederherstellung und der Überschuss an benötigtem Bruttospeicherplatz bei höherer Sicherheit wesentlich geringer sind. Erasure Coding ist dabei allerdings rechenintensiver als RAID.

Erasure Coding wird überall dort eingesetzt, wo große Mengen an Daten gegen Verlust durch Ausfall einzelner Komponenten, z.B. Festplatten oder ganzer Standorte, gesichert werden sollen. Dabei ist das Brutto-/Netto-Verhältnis konfigurierbar. Vereinfacht gesagt wird beim Erasure Coding ein Datensatz in m Fragmente aufgeteilt und mit k weiteren Fragmenten neu codiert, so dass gesamt $n=m+k$ Fragmente entstehen. Für die Wiederherstellung der Daten genügen beliebige m Fragmente, es können also k Fragmente verloren gehen.

Wird zum Beispiel eine „8 aus 12“-Konfiguration (ERC 8/12) eingesetzt, sind die Fragmente auf 12 Festplatten verteilt, von denen beliebige 8 zur Wiederherstellung der Daten ausreichen. Es können also innerhalb eines Festplatten-Sets bis zu 4 Festplatten gleichzeitig ausfallen, ohne dass Datenverlust droht. Damit bietet ERC 8/12 höhere Sicherheit als eine gespiegelte RAID-6 Konfiguration.

Die Mathematik hinter Erasure Coding ist mehr als 50 Jahre alt und wurde z.B. dazu verwendet, Daten von Satelliten zur Erde zu funken. Bei der Übertragung treten garantiert viele Fehler auf, der Algorithmus stellt jedoch sicher, dass auch bei vergleichsweise wenigen empfangenen Fragmenten die Daten im Original wiederherstellbar waren.

Die Silent Brick Library

FAST LTA bietet mit der Silent Brick Library eine enorm flexible Disk Library an, die ideal zur sicheren Speicherung statischer Daten geeignet ist. Daten sind dabei linear auf transportierbaren Silent Brick Datencontainern gespeichert, die in sich durch 4 Redundanzreserven gesichert sind. Von den 12 Festplatten je Silent Brick können bis zu 4 gleichzeitig ausfallen, ohne dass Daten verloren gehen. Ergänzt wird das eingesetzte 8/12 Erasure Coding durch Digital Audit und die Mischbestückung mit Festplatten aus 3 Chargen, so dass eine dreifache Absicherung gegen Datenverlust entsteht. Nur durch die Kombination dieser Sicherheitsmerkmale speichert die Silent Brick Library Daten so sicher, dass kein weiteres Backup erforderlich ist – sofern der Standort insgesamt als sicher gilt. Eine Replikation einzelner Silent Bricks an einen zweiten Standort zur zusätzlichen Absicherung gegen Katastrophen wie Feuer oder Überflutung ist dabei aufgrund der linearen Speicherstruktur besonders unkompliziert.

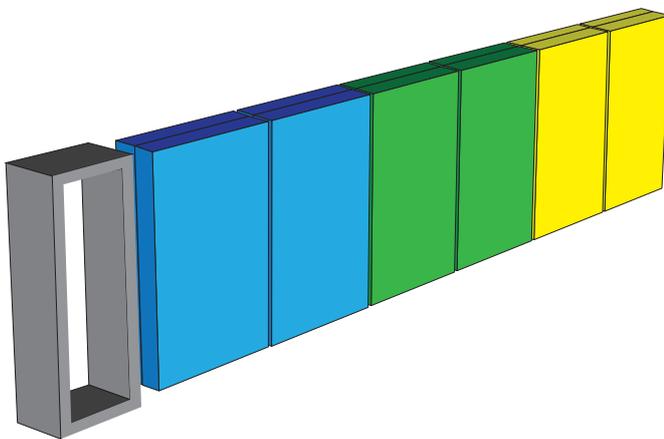
Überlegene Redundanzkodierung mit Erasure Coding

Bei der Silent Brick Library von FAST LTA wird ein ERC 8/12 eingesetzt, das Verhältnis von Brutto- zu Nettokapazität beträgt also 2:1 – und das, obwohl 4 Redundanzreserven zur Verfügung stehen. Um einen Festplattenverbund mit Replikation so abzusichern wären $5 \times 8 =$

30 Festplatten notwendig. Bei einer gespiegelten RAID-6-Konfiguration, bei der ebenfalls bis zu 4 Festplatten ausfallen können, sind immer noch $2 \times (8+2) = 20$ Festplatten notwendig.

Erasur Coding ist also bei gleicher Sicherheit wesentlich effizienter und damit auch kosten- und energiesparender als jede andere Speichertechnologie.

Mischbestückung zur Vermeidung von Chargenfehlern



Dennoch gibt es Fälle, in denen auf Festplatten gespeicherte Daten ohne äußere Einflüsse verloren gehen können. Das eine Problem sind so genannte Chargenfehler (englisch: Epidemic Failure), bei denen innerhalb statistisch ungewöhnlich kurzer Zeit gleiche Festplattenmodelle Defekte aufweisen. Dies kann z.B. durch fehlerhafte Chargen in der Produktion entstehen (bedingt durch veränderte Produktionsbedingungen aber auch Fehler in Teilen der Firmware), oder einfach durch den Alterungsprozess von mechanischen Teilen auftreten. In Festplattensystemen mit

Jeder Silent Brick Storage-Container enthält je 4 Festplatten aus 3 unterschiedlichen Chargen

lauter Festplatten aus dergleichen Charge – was durchaus üblich und z.T. sogar durch den Festplatten-Controller notwendig ist – bedeutet ein Festplattenausfall deswegen oft Gefahr für das Gesamtsystem.

FAST LTA setzt deswegen in allen seinen Festplattenspeichern immer Festplatten aus mindestens 3 unterschiedlichen Chargen von möglichst vielen unterschiedlichen Herstellern ein. Beim oben beschriebenen ERC 8/12 können so alle 4 Festplatten einer Charge ausfallen, ohne dass Datenverlust droht.

Schutz vor URE durch Digital Audit

Und noch ein weiteres Problem befällt die Festplatten: Der so genannte Unrecoverable Read Error, kurz: URE. Festplattenhersteller geben an, dass etwa eines von 10 hoch 14 Bits

einfach und ohne besonderen Grund nicht richtig gelesen werden kann. Das klingt nach einem zu vernachlässigbarem Problem, schließlich ist das eine enorme Zahl mit 14 Nullen. Allerdings sind die Datenmengen heutzutage dermaßen hoch, dass dieses Problem sehr real wird: Alle 12 Terabytes gibt es statistisch garantiert einen Lesefehler. Bei codierten Daten bedeutet das, dass die Datei schlicht nicht wiederhergestellt werden kann. Mit den heutigen Festplattengrößen (Stand Anfang 2015: bis zu 12 TB pro Festplatte) ist Datenverlust also fast schon sicher. Die Gemeinheit dabei ist, dass der Fehler erst beim Lesen der Daten erkannt werden kann. Eine Speicherung, die auf Parity-Vergleich beruht (RAID), erkennt diesen Fehler also nicht – bis genau die eine betroffene Datei wiederhergestellt werden soll.

Die eigens entwickelten Festplatten-Controller von FAST LTA weisen deshalb eine wichtige Funktion auf: Den Digital Audit. Im Controller verankert und vom Host-System unabhängig liest diese Funktion eigenständig und regelmäßig jedes einzelne Bit der gespeicherten Daten und vergleicht die Hashes, die sich aus den Inhalten der Dateien ergeben und somit von jedem Bit abhängen, mit den bei der ursprünglichen Speicherung gesicherten Hashes. Tritt nun so ein Bitfehler auf, wird er von Digital Audit zuverlässig erkannt. Durch die hohen Redundanzreserven kann die betroffene Festplatte im Hintergrund repariert oder sogar abgeschaltet werden, ohne dass Datenverlust droht.

Silent Brick Library: So sicher, dass kein weiteres Backup notwendig ist

Die Kombination aus Linear Disk Storage und den drei beschriebenen Faktoren zur Sicherstellung der Datenintegrität sorgt dafür, dass Daten, die auf der Silent Brick Library gespeichert sind, nicht noch zusätzlich abgesichert werden müssen.

Zusammen mit der Flexibilität und der einfachen Ordnung durch physikalisch trennbare Medien ergibt sich so vor allem eine erhebliche Reduzierung der Komplexität. Neben der stark vereinfachten Administration spart dies auch erheblich Kosten und erhöht die Planungssicherheit bei sinkenden IT-Budgets. Und wo kein Backup, da kein Restore – auf die Daten in der Silent Brick Library kann einfach jederzeit zugegriffen werden.

Erleben Sie die Silent Brick Library auf der CeBIT in Halle 2, Stand A37. Mehr Informationen unter www.silentbricks.de

Silent Brick Library:
Disk Library für Cold
Storage Anwendungen



FAST LTA
Wir sichern Terabytes.

COLD STORAGE

Hallo,

wir sind die **FAST LTA AG**.

Unser Firmensitz ist in der Rüdeshheimer Str. 11 in 80686 München, Deutschland. Sie erreichen uns telefonisch unter +49 (89) 890 47 - 0, per Fax unter +49 (89) 890 47 - 890 und via E-Mail über info@fast-lta.de. Beim Amtsgericht München sind wir unter der HRB 127 484 eingetragen, unsere USt-ID ist DE204232266. Die Kontodaten bei der Kreissparkasse München Starnberg sind IBAN DE76 7025 0150 0022 2363 19 und BIC BYLA DE M1 KMS. Im Vorstand sitzen Matthias Zahn, Jörg Adelstein und Reiner Bielmeier, der Vorsitzende des AR ist Jens Gloede. Im Internet finden Sie uns unter **www.fast-lta.de**.