De 4 pijlers van secundaire storage

Waar op te letten bij de keuze van een secundair storage systeem

Het is zoals in real life: de sexy primaire storage systemen krijgen 80% van de aandacht (en van het budget) en de saaie secundaire storage krijgt 80% van het werk (datavolume). Terwijl de primaire storage vanwege snelle technologische veranderingen gemiddeld om de drie jaar vervangen wordt moet opslag voor back-up en archief veel langer mee gaan. Niemand vind het prettig om de 3 jaar tera- of zelfs petabytes aan data te verhuizen. De keuze voor een (of meerdere?) secundaire opslagsysteem moet weloverwogen zijn. Hierbij spelen de volgende vier criteria een rol.

#1: DATAVEILIGHEID

Op zich wel logisch: als een storage systeem voor back-up en archivering ingezet wordt zou het zelf geen additioneel back-up nodig moeten hebben. Het thema veiligheid kan hier in drie niveaus onderverdeeld worden:

Beveiliging op toegangsniveau om beveiligd te zijn tegen dataverlies of datamanipulatie door aanvallers of gebruikersfouten. Afhankelijk van de toepassing zijn regelmatige of zelfs automatische snapshots en de bescherming door hardware-WORM de juiste keuze. Toenemend waargenomen aanvallen door bijv. ransomware maar ook bewuste of abusieve pogingen om data te wissen wordt zo effectief een grendel voorgeschoven.

Beveiliging op hardwareniveau om tegen dataverlies door uitval van gegevensdragers beschermd te zijn. Dit wordt bereikt door kopieën of redundantie zodat een gedefinieerd aantal van de gebruikte gegevensdragers uit kan vallen zonder dat dataverlies optreedt. De meest bekende is hier RAID wat echter niet als veilig genoeg wordt aangezien om zonder aanvullende maatregelen te kunnen voldoen. RAIDz als onderdeel van ZFS, met name in de variant triple parity, is hier al beduidend veiliger omdat sluipende fouten en daarmee een falen van een rebuild meestal voorkomen kan worden. Als bijzonder veilig wordt erasure coding, de aangewezen opvolger van RAID, beschouwd. Erasure coding vergt beduidend minder systeemresources bij het rebuild en is aanvullend zeer flexibel te configureren, bijv. ook met viervoudige redundantie.

Beveiliging op systeemniveau om tegen dataverlies door totale uitval beveiligd te zijn. Als een systeem door brand, waterschade of diefstal niet meer bruikbaar of toegankelijk is helpt ook de beste technologie niet meer. Deze calamiteiten kunnen alleen door een replicatie naar een tweede locatie opgevangen worden. Meestal moet hiervoor het gehele systeem identiek gespiegeld worden, sommige systemen staan ook het repliceren naar een tweede locatie op dataniveau toe. Het voordeel van de replicatie op dataniveau is duidelijk: beide systemen kunnen op hun locatie als productiesysteem gebruikt worden en telkens naar de andere locatie repliceren.

#2: FLEXIBILITEIT

Gebruikelijk bedraagt de investeringscyclus in de IT sector 3 jaar. Secundaire storage moet echter zijn werk veel langer verrichten. Daarom is het essentieel dat dit storage systeem maximale flexibiliteit biedt om voor de toekomst gewapend te zijn.

De **schaalbaarheid** is hier het eerste aspect dat in het oog valt. De behoefte aan opslagcapaciteit groeit rap, nagenoeg niemand kan voorspellen hoeveel data in 3, 5 of 10 jaar opgeslagen worden. Als een storagesysteem reeds bij de aanschaf zo gedimensioneerd moet zijn dat alle mogelijkheden afgedekt zijn is meestal een hoge investering nodig. Meer geschikt zijn daarom systemen die elastisch met de behoefte schaalbaar zijn. Een belangrijk punt hierbij is dat de schaalbaarheid ook dan nog gegarandeerd moet zijn als de oorspronkelijk gebruikte soort gegevensdragers niet meer beschikbaar is.

Bij de flexibiliteit hoort ook dat de **configuratie** van het systeem niet al te vastgelegd is. Welke bestandssystemen, softwaretoepassingen en applicaties worden ondersteund? Is een aanvulling met SSDs mogelijk als het prijsniveau in de buurt van de harde schijven komt? Kunnen storagegedeeltes flexibel aan verschillende toepassingen toegewezen worden – en kunnen deze ook onafhankelijk van elkaar groeien of krimpen?

Niet te vergeten is ook de **connectiviteit** van het gekozen systeem. Afhankelijk van de gewenste toepassing kan het nodig of wenselijk zijn dat de fysieke verbinding met de toenemende behoeftes groeit. Waar vandaag 1 GBit ethernet gebruikelijk is zijn morgen al 10, 40 of 100 GBit vereist. Als de storage vast met de servercomponenten verbonden is betekend een upgrade meestal een vervanging van het gehele systeem.

#3: OFFLINE-MOGELIJKHEDEN

Alle data zijn permanent online, in de cloud en overall en altijd beschikbaar. Dit bergt echter een aantal nadelen en risico's die voor secundaire storage systemen problematisch kunnen worden. Permanent toegankelijke dataopslag is ook permanent aan hackers en ransomware blootgesteld. Massief gedistribueerde opslagstructuren (cloud) leiden tot onzekerheden betreffende het omgaan met gevoelige data en zijn vaak niet in overeenstemming met wettelijke regels en voorschriften zoals de AVG. Daarom ervaren offline-geschikte opslagmedia in de laatste tijd opnieuw toenemende aandacht. Het buzzword hierbij is "**air gap**". Wat niet verbonden is maar door een fysiek gat – een air gap – gescheiden is, kan niet geïnfecteerd worden omdat geen toegang mogelijk is. Wenselijk is hierbij natuurlijk dat men niet aanvullende offline-kopieën moet maken die dan beveiligd in een kluis bewaard kunnen worden. Het handling van dit soort offline-media is zo omslachtig dat de hoop overweegt, deze media nooit nodig te hebben. Natief offline-geschikte niet-lineaire media geven wél de mogelijkheid data snel en zonder ingewikkeld kopiëren weer beschikbaar te stellen.

#4: WEINIG COMPLEXITEIT

Het laatste kriterium is de **reducering van de storagecomplexiteit**. De reducering van de complexiteit is in de IT sector een van de grote thema's van de komende jaren, bijna geen instelling of onderneming kan specialisten voor elk component in huis hebben. Duidelijk: de primaire storage heeft bijzondere aandacht en moet individueel op de performancebehoeftes afgestemd zijn. Voor de langdurige opslag geldt echter: minder is meer. De meer systemen betrokken zijn, de meer contactpersonen, configuraties, user interfaces en service contracten zijn er. Omdat secundaire storage systemen voor langdurige bewaring gemaakt zijn, spelen ook de duur van de servicecontracten en de mogelijkheid tot verlenging bij gelijkblijvende voorwaarden een rol.

Conclusie

Veiligheid en schaalbaarheid zijn voor de hand liggende eisen aan een opslagsysteem voor back-up en archief, echter zijn hier al behoorlijke verschillen te zien. Aanvullend komen de nieuwe (oude) eisen naar offline mogelijkheden omdat "always online" vaak niet aan de beveiligingseisen voldoet en toenemend aan aanvallen blootgesteld is. Overkoepelend staat de wens naar "fire & forget": een secundaire storage moet ongecompliceerd en langdurig betrouwbaar zijn werk verrichten: data veilig bewaren.

Opslagsystemen van FAST LTA

FAST LTA heeft met de **Silent Cubes** en de **Silent Bricks** twee opslagsystemen ontwikkeld die door lineaire opslagtechnologie met structuurveiligheid en moderne Erasure Resilient Coding met viervoudige redundantie voor koude opslag – Cold Storage – geoptimaliseerd zijn.

Drievoudige beveiliging tegen dataverlies

Naast de hoge ingebouwde veiligheid door lineaire opslag en structuurzekerheid bieden opslagsystemen van FAST LTA aanvullend een drievoudige beveiliging tegen dataverlies door harddisk-uitval.

Erasure Resilient Coding

FAST LTA gebruikt 12/8 Erasure Resilient Coding. Elk opslagmodule beschikt over twaalf gegevensdragers waarvan vier tegelijk mogen uitvallen zonder dat gegevens verloren gaan. Een belangrijk voordeel van ERC ten opzichte van RAID-systemen is hierbij de duidelijk lagere rebuild-tijd, naast de grotere veiligheid en de betere bruto/netto-verhouding:

> "**Als je harde schijven van grote capaciteiten in een RAID-array plaatst duurt een rebuild weken. Met Erasure Coding praat je over uren,"** zegt bijvoorbeeld George Crump, president van het IT-analyse-bedrijf Storage Switzerland.[1]

Dit is tevens een belangrijk beveiligingsaspect. Gedurende een rebuild is een RAID-systeem in een kritische toestand, uitval van een verdere harddisk kan al dataverlies betekenen. Erasure Resilient Coding met viervoudige redundantie heeft bij uitval van een harddisk nog drie aanvullende reserves zodat de rebuild, die toch al minder ingewikkeld is, met rust en weinig systeembelasting gedaan kan worden.

Digital Audit

Het belangrijkste bij een back-up is een functionerende restore. Deze gemeenplaats veronderstelt dat de opgeslagen gegevens ook betrouwbaar leesbaar zijn. Daarom worden de gegevensdragers in de FAST LTA opslagsystemen regelmatig en automatisch op bit-

[1] http://searchstorage.techtarget.com/feature/Hot-data-storage-technology-trends-for-2016

niveau gecontroleerd – de zogenaamde Digital Audit. Fouten kunnen zo betrouwbaar herkend en bijvoorbeeld door vervanging van de gegevensdrager gecorrigeerd worden.

Disk Mix

Het gebeurt altijd wel eens dat een hele serie van harddisks een fout heeft. Maar ook zonder fouten valt op dat harddisks uit dezelfde serie vaak vlak achter elkaar uitvallen.

Om te voorkomen dat dit effect invloed op de dataveiligheid heeft, worden in elke Silent Cube en in elke Silent Brick harddisks uit drie verschillende series van zoveel mogelijk verschillende fabrikanten[2] ingebouwd. Zelf als de vier harddisks van een serie uitvallen gaan door het 12/8 Erasure Resilient Coding geen gegevens verloren.

De onafhankelijkheid van bepaalde soorten gegevensdragers en fabrikanten heeft tevens voordelen bij het vervangen van defecte harddisks: als bepaalde modellen of fabricaten na jaren niet meer leverbaar zijn, is een vervanging door andere modellen nog altijd zonder problemen mogelijk.

[2] Helaas zijn er voor sommige capaciteiten van harddisks en SSD's geen drie verschillende fabrikanten meer.

Silent Cubes: revisiezekere archiefopslag met WORM-verzegeling

De **Silent Cube** beschermt gegevens aanvullend met een WORM-verzegeling tegen wijziging en verlies. Omdat deze verzegeling op het laagste hardware-niveau geschiedt – de speciaal ontwikkelde harddiskcontroller kan alleen doorlopend schrijven maar niet wissen of elders schrijven – kan geen administrator, ook niet FAST LTA, gegevens wijzigen of wissen.

Deze WORM-verzegeling garandeert de Silent Cubes ook de revisiezekerheid die voor een rechtsgeldige archivering bijvoorbeeld volgens KNMG, AVG en anderen nodig is.

Silent Bricks: flexibel en veilig opslagsysteem voor back-up en archief met uitneembare storagecontainers

De **Silent Brick Library** doelt op minder speciale toepassingen. Als Cold Storage systeem is de library ideaal voor back-up, maar ook voor een actief archief of als netwerkopslag.

De basis vormen de **Silent Bricks**, uitneembare storagecontainers met twaalf harddisks die intern via Erasure Resilient Coding beveiligd zijn. Met de flexibele replicatie op basis van enkele Silent Bricks zijn offline-media en remote replica's eenvoudig en goedkoop aan te maken. In tegenstelling tot de gebruikelijke redundantie door spiegeling naar een tweede locatie kan hier de replicatie van de Silent Bricks individueel voor elke Silent Brick geconfigureerd worden. Het systeem op de tweede locatie blijft hierbij volledig operationeel en kan zelf ook Silent Bricks naar het eerste systeem repliceren (cross-over replicatie).

De Silent Bricks zijn uitgerust met harddisks of snelle FLASH-geheugens en leverbaar in verschillende capaciteiten met of zonder WORM-verzegeling.

De Silent Brick Controller biedt vijf slots voor Silent Bricks en kan via rechtstreeks verbonden uitbreidingseenheden met elk veertien slots uitgebreid worden.

De **Silent Brick Drive** is met zijn twee slots al een ideaal systeem voor kleinere opslagbehoeftes zoals een veilig netwerkback-up met interne replicatie naar een tweede Silent Brick.

Over FAST LTA

Passie voor dataopslag

We secure Petabytes – dit is het motto van FAST LTA AG uit München, Duitsland. Deze slogan bevat de belofte op de gegevens van de klanten te letten. En dit weerspiegelt in elk detail van de door Matthias Zahn en zijn medewerkers ontwikkelde opslagproducten.

De eigen ambitie is: er mogen geen gegevens verloren gaan. Daarom worden alle kritische onderdelen zelf ontwikkeld, uitgebreid getest en permanent verbeterd. Hierbij hoort ook de implementatie van het Erasure Resilient Coding, een redundante codering ter bescherming van gegevens die de gebruikelijke RAID ver voorbij gaat. Deze technologie wordt door FAST LTA vergezeld door Digital Audit, de automatische zelfcontrole van de systemen, en door de aanvullende beveiliging via Disk Mix, het gebruik van drie verschillende harddiskmodellen in ieder storagemodule. Opslagsystemen van FAST LTA zijn zo veilig dat – aangenomen dat de locatie veilig is – geen aanvullende beveiliging door back-up nodig is.

Silent Cubes, het revisiezekere WORM-systeem voor alle data die in geen geval verloren mogen gaan, is sinds de introductie 2008 in duizenden installaties in gebruik. Onder andere de zorgsector, musea, bibliotheken en overheden, de industrie en handel, banken en verzekeringen gebruiken Silent Cubes. De handige storage-kubus is voor talloze applicaties gecertificeerd en met alle opslagnormen compliant.

De Silent Brick Library, het flexibele COLD Storage-systeem met transportabele storagecontainers is evenwel uitgerust met de drievoudige beveiliging door Erasure Resilient Coding, Digital Audit en Disk Mix. De combinatie uit lineaire datastructuur en harddisktechnologie maakt fysiek gescheiden opslag mogelijk en biedt bijzonder lage grenskosten. De Silent Brick Library is met name geschikt voor grote actieve archieven, als back-upopslag en als mediaopslag zoals videoproducties.

FAST LTA is ISO 9001 gecertificeerd.

Over COMEX

Comex is sinds 1992 distributeur voor digitale opslagsystemen en vertegenwoordigt FAST LTA sinds 2008 in Nederland.

Contactgegevens:
www.comex.eu | office@comex.eu | +31-43-3088400