Wissen van een virtuele machine is fluitje van een cent

Data recovery van virtuele SAN is puzzel met extreem hoge moeilijkheidsgraad

Jaap-Jan Visser is country manager van Kroll Ontrack Nederland

Virtualisatie biedt bedrijven de mogelijkheid om systemen te consolideren en kosten te besparen, maar het leidt ook tot meer complexiteit en stelt bedrijfsgegevens bloot aan nieuwe risico's. Ook een SAN die in een cloudomgeving draait kan geheel of gedeeltelijk uitvallen. Als een disaster recovery-plan ontbreekt en de back-ups niet blijken te werken is dit een regelrechte nachtmerrie. Het aantal verzoeken op het gebied van data recovery voor virtuele systemen nam de afgelopen jaren dan ook fors toe.

Problemen met de hardware en het RAID-systeem zijn met 39 procent de belangrijkste oorzaak voor dataverlies in een virtuele omgeving. Menselijke fouten zoals het per ongeluk verwijderen van een virtual disk of een snapshot leiden in 33 procent van de gevallen tot dataverlies. De metadata van het Virtual Machine File System (VMFS) kan corrupt raken. Deze oorzaak is verantwoordelijk voor 17 procent van de gevallen waarbij dataverlies optreedt. Bij het formatteren van schijven of de herinstallatie van virtuele machines worden ook regelmatig fouten gemaakt. Deze fouten zijn verantwoordelijk voor 11 procent van de verzoeken om dataherstel toe te passen.

RAID en SAN

RAID recovery is een van de technische uitdagingen op het gebied van data recovery. RAID 0, ook wel striping genoemd, biedt geen enkele vorm van redundantie. De data wordt slechts verdeeld over de harde schijven. Als één schijf uitvalt en daar helemaal geen RAW data meer van af te halen valt, is van de nog werkende schijf alleen data te herstellen van files kleiner dan de block size. In de praktijk gaat de meeste data van het array verloren. RAID 1, ook wel mirroring genoemd, zorgt ervoor dat data identiek naar twee harde schijven wordt weggeschreven. Hierbij staan alle gegevens dus op elke schijf van de array. Hoewel het kan afhangen van de controller, kunnen sommige schijven in een RAID 1 configuratie individueel worden gelezen. Dit betekent dat een beschadigde RAID 1 schijf vaak eenvoudig zelf kan worden hersteld, mits ten minste één harde schijf nog werkt. RAID 5 verdeelt de data over de harde schijven en distribueert pariteit. Dit zorgt ervoor dat de data in de RAID 5 array niet verloren gaat wanneer een enkele harde schijf defect raakt. Als er een schijf kapot gaat, kan een zogenoemde RAID rebuild worden gedaan met een nieuwe harde schijf. Rebuild van een RAID 5-array na een RAID failure veroorzaakt extra stress op alle nog werkende harde schijven. Elk gebied dat in gebruik was op elke schijf moet namelijk worden gelezen om de redundantie die verloren is gegaan weer te herstellen. Vaak zijn de schijven van dezelfde productiedatum en gaat er tijdens dit proces nog een harde schijf kapot. Dit risico is groter door de toegenomen schijfcapaciteit. Daardoor kan de RAID 5 rebuild uren, zo niet dagen, duren. Een SAN wordt vaak opgebouwd in blokken en combinaties van RAID. Met daarbovenop de eigen blokverdeling van de fabrikant.

SSD

Defecte harde schijven zijn nog steeds de hoofdoorzaak van gegevensverlies, zo blijkt uit een recent wereldwijd onderzoek uitgevoerd in opdracht van Kroll Ontrack. Maar liefst 72 procent van de respondenten geeft aan dat de meeste recente incidenten waarbij gegevensverlies optrad, veroorzaakt zijn door een crash van de harde schijf van de desktop of laptop computer, gevolgd door Solid State Drives (15 procent) en het falen van RAID of virtuele opslagdiensten (13 procent).

Zeven praktijkvoorbeelden

- Hoewel de software pas sinds maart 2014 op de markt is, is het Kroll Ontrack gelukt voor een klant in Nederland data van verschillende harde schijven te herstellen die beheerd werden door VMware Virtual SAN. Engineers slaagden er in om alle gegevens die waren opgeslagen in de virtuele machines van 15 schijven en 3 SSD's te herstellen. Bij de initiële Virtual SAN-herstelpoging zorgden fouten in twee SSD's van de Virtual SAN voor een uitval van tweederde van het opslagsysteem. Dit resulteerde in het verlies van belangrijke bedrijfsgegevens op vier grote virtuele machines. Aangezien Virtual SAN alle gegevens beheert en opslaat in een gecombineerd geheugencluster, moesten de engineers de volledige gegevens van alle 15 schijven herstellen.
- Een RAID 5 storagesysteem met tien drives had al drie maanden een kapotte harde schijf zonder dat dit bekend was. Toen een tweede schijf kapot ging, crashte de server, waardoor de data niet meer beschikbaar was. Gelukkig probeerde de klant niet eerst zelf de drives terug online te zetten, omdat dit alle data zou kunnen beschadigen. Een expert bouwden de array opnieuw op, waardoor een totale recovery mogelijk was.
- Een IT-medewerker in een ziekenhuis probeerde een kapotte harde schijf in een RAID array te vervangen, maar verwijderde per ongeluk een harde schijf uit een andere array waar kritische SQL servers van het ziekenhuis op gehost werden. De array liep schade op als gevolg van meerdere reparatiepogingen door de server administrator. Door middel van remote data recovery kon een specialist de database terughalen.
- Een gefrustreerde werknemer wiste moedwillig alle virtuele machines van een 3PAR SAN met 28 LUNs, 440 VMDKs en meer dan 1.000 snapshots. De LUN's werden overschreven door nullen. Exchange, SQL, Oracle en de File Servers waren allemaal foetsie. Ook de back-ups werden gewist. Door middel van een data recovery op afstand, waarbij meerdere machines werden aangesloten op de SAN en een heel team 24/7 werd ingeschakeld, zijn uiteindelijk alle virtuele machines en snapshots gered. Een puzzel die wel drie weken in beslag nam.
- Om onduidelijke redenen was de metadata van het RAID-systeem corrupt geraakt. De betreffende HP EVA SAN 8400 bevatte 150 harde schijven met daarop 134 LUNs, met vRAID 1 en vRAID 5. Daarop draaide VMware en NTFS filesystemen. Met zelf ontwikkelde tools herstelden de data recovery engineers in totaal 67 terabyte aan data.
- Een organisatie verwijderde per ongeluk tijdens een test project alle 38 virtuele machines van twee arrays. Door middel van remote data recovery kon een engineer op afstand verbinding maken met het bedrijf om de verwijderde bestanden terug te halen en naar een nieuwe array te kopiëren.
- Bij een hostingbedrijf crashten in een tijdsbestek van drie minuten meerdere harddisks, waaronder een aantal disks uit de Centrale Cloud Cluster. De RAID 5 groep ging onderuit. Het gevolg was dat een flink aantal servers en een belangrijk deel van de cloudomgeving uitviel. Het hostingbedrijf had geen disaster recovery-omgeving. Desondanks is 100 procent van de data hersteld.

Data recovery kun je vergelijken met een boek waarvan de paginanummers, de inhoudsopgave, de band en het omslag zijn verwijderd. Vervolgens laat je alle losse bladzijden van een hoge toren naar beneden dwarrelen. Probeer dan maar eens om van de teruggevonden bladzijden weer een boek te maken. Bij een SAN met virtuele systemen is er geen sprake van een boek, maar van een complete bibliotheek. Inderdaad, een puzzel met een extreem hoge moeilijkheidsgraad.

Kijk voor meer informatie op www.ontrackdatarecovery.nl

Jaap-Jan Visser is sinds mei 2008 country manager van Kroll Ontrack Nederland.