Kroll Ontrack op het Oracle-spoor

Data-recovery voor Oracle

De firmanaam Kroll Ontrack klinkt enigszins merkwaardig, als zou Kroll ook ooit niet on track zijn geweest. De ontstaansgeschiedenis van het bedrijf geeft echter een goede verklaring: het is een samenvoeging van Kroll en Ontrack. Later nam het ook nog eens het Noorse IBAS over, dat daarvóór al Vogon overnam, waardoor er in feite geen grote concurrerende data recovery-ondernemingen meer overbleven. Sinds kort heeft Kroll Ontrack ook een serie oplossingen voor Oracle, aanleiding voor een gesprek met Oyvind Nyland en Jaap Jan Visser van Kroll Ontrack.

'Geluk bij een ongeluk' klinkt in dit geval wel heel cynisch. Niettemin: vijf jaar na het tragische ongeval met de Space Shuttle Columbia waarbij alle zeven bemanningsleden omkwamen, werd het onderzoek gebaseerd op de data van een wetenschappelijk experiment aan boord van de Columbia alsnog afgesloten. Van de 400 GB harde schijf die de data van het experiment bevatte, was na de explosie en het daaropvolgende neerstorten van de Shuttle niet veel meer over. Alle plastic delen en alle elektronica waren verbrand. In feite waren alleen de platters, de schijven die de informatie bevatten nog bruikbaar. Bruikbaar is misschien ook overdreven, want ze waren tegen elkaar aan gedrukt, gekrast en uiteraard extreem verhit. Kroll Ontrack wist echter in twee dagen 99% van de data te redden. Het experiment – een poging het gas Xenon in gewichtloze toestand door roeren eenzelfde soort viscositeitsverandering door te laten maken als slagroom - was daarmee ook gered. De wetenschappelijke analyse ervan en het vervolgonderzoek nam nog een paar jaar in beslag.

Visser: "Als we een drive met brandschade die van zestien kilometer hoogte is gevallen kunnen recoveren, dan laat dat wel iets van onze expertise zien. Grappige bijkomstigheid is dat de technicus die de recovery van die data voor de NASA uitgevoerd heeft, nu bij ons in Nederland werkzaam is. Meestal werken wij echter met software die we verkopen. Soms ook volgens het SAAS-principe: de klant kan daarbij op afstand gebruik maken van onze software om de data te redden. Uiteraard kunnen we ook beginnen met de hardware, zoals in het geval van de Space Shuttle, en we kunnen indien nodig ook een JIT-proces starten. JIT staat voor *just in time*, in feite het schrijven van specifieke oplossingen op het moment dat een klant er behoefte aan heeft. De Oracle-oplossingen zijn zo ook ontstaan."

Hoeveel concurrenten hebben jullie nu al die bedrijven gefuseerd zijn?

Nyland: "Natuurlijk zijn er vele bedrijven in de wereld die zich bezighouden met data-recovery, maar niet op onze schaal. We hebben negentien labs over de gehele wereld. "

Wat maakt uw Oracle-oplossing speciaal, wat doet het beter dan Oracle zelf?

Nyland: "In de eerste plaats zijn we gespecialiseerd in hardware, bij 85% tot 90% van onze opdrachten is sprake van een of andere soort fysieke schade. Maar afgezien daarvan is onze kracht op recovery-gebied dat we geen van de originele applicaties nodig hebben. We hebben ons eigen tools-portfolio, zodat we volledige controle over het proces hebben. We weten waarnaar we moeten kijken en we zijn niet afhankelijk van een draaiend Oracle-systeem."

Dus u loopt geen gevaar data te overschrijven, u kunt een medium uitsluitend gebruiken om ervan te lezen.

Nyland: "Ja, we gebruiken alleen de raw data blocks van de

Wat moet je doen om dataverlies te voorkomen:

1. Zorg ervoor dat je procedures goed geregeld zijn, zodat je menselijke fouten vermijdt.
2. Zet ook procedures op voor het testen van backups.
3. Wanneer het alsnog echt mis gaat, zoek dan een expert die je helpt en zorg ervoor dat de originele schijf alleen gebruikt wordt om te lezen. Start de database of een ander op de schijf geïnstalleerd programma zoals een besturingssysteem, niet op.

Wanneer er absolute zekerheid moet bestaan over het wissen van data, dan is degaussen de enige oplossing.

drive om ze veilig te bewaren, we maken altijd een image, of een zo goed mogelijke recoverage van de oorspronkelijke data en slaan die op een server op. De originele data blijven dus altijd zoals ze waren. Natuurlijk kunnen er dingen verloren gaan als er fysieke schade is. Dat is de eerste fase van onze recovery, het veilig opslaan van de raw data. In de tweede fase kijken we in de datastroom en naar de data die met de database verband houden. Om een goede recovery te doen hebben we basis-informatie nodig van de klant, met betrekking tot het probleem en de versie van de software. Daarmee kunnen we sneller, beter en goedkoper ons werk doen. Bij Oracle willen we uiteraard weten welke versie van de database het is, de naam van de table space, tabellen(data-)schema's, bij benadering de grootte van de database, als je weet hoeveel tabellen met hoeveel kolommen, dan is dat ook handig, liefst ook systeemdocumenten, system01 bevat een hoop waardevolle informatie die we kunnen gebruiken om de structuur van de database te herstellen. Het is niet een kwestie van op de recovery-knop drukken, we hebben ook informatie nodig om een goede Oracle-recovery te doen. Daarmee scannen we de data om te kijken of er datablocks zijn, die data van de database bevatten. Wanneer de recovery 100% geslaagd is, kan de database weer gewoon opgestart worden. Kroll Ontrack heeft echter ook post-recovery-applicaties. Daarmee worden de teruggehaalde gegevens terug in een bestaande Oracle-database geplaatst, terwijl de originele tabelstructuur en andere belangrijke metadata behouden blijven."

Ontstaat er dan geen database met deels corrupte data?
"Ja, we hebben weliswaar software om die corruptie te corrigeren, maar het is mogelijk dat er dan nog steeds rijen of kolommen missen. De klant moet daarna de data controleren. Maar

de database-file die wij afleveren kan in ieder geval gewoon geopend worden. Voor het herstellen van corrupte data is het ook afhankelijk van de versie, want er zijn wel heel vele verschillende versies. Mocht iemand echter een versie hebben die wij nog niet ondersteunen, dan hebben we daarvoor het JIT-proces, waarbij we ons hoofdkwartier in Minneapolis vragen die ondersteuning alsnog te leveren."

Wat is het eerste wat je moet je doen in geval van dreigend data-verlies?
Nyland: "Het belangrijkste is niets te veranderen op de originele drive. Wanneer je eenmaal begint te manipuleren met het originele systeem of met de originele drive, dan is er geen weg terug. Als je dan iets fout doet, kan alles verloren gaan. We veranderen nooit iets aan de originele drive, maar werken altijd op kopieën, in feite zelfs op kopieën van kopieën. Iedere keer wanneer je een computer start, veranderen een paar duizend documenten. Wat gebeurt er dan in feite? Je weet het niet, als je bijvoorbeeld gecomprimeerde documenten hebt, dan kunnen ze gedecomprimeerd worden en ruimte overschrijven, er gebeurt veel, meer dan je weet. Dus de eerste regel als je een defecte harddrive hebt of wanneer je iets gewist hebt is: zet nooit iets op het medium. Je zult altijd iets overschrijven."
Visser: "En overschreven data is altijd verloren. Men denkt vaak dat we dat zeggen om angst aan te jagen maar het is de trieste realiteit." *(Zie kader: broodje aap)*

Waarom treedt dit soort fouten op? Je zou toch mogen verwachten dat professionele IT-ers altijd een betrouwbare back-up tot hun beschikking hebben. Zo moeilijk is het toch allemaal niet?
Visser: "De systemen worden veel complexer. Virtualisatie, multiple systemen, multiple back-ups, ook over verschillende locaties heen. Er bestaat wel goede software om het allemaal te managen, maar wanneer dat eenmaal mis gaat, wordt het ook

Broodje aap

Er bestaat een wijd verbeid geloof dat één keer wissen van data onvoldoende is. Eén keer is hier geen keer: pas het Bijbelse aantal zeven geeft zekerheid. Volgens Nyland is dat bij de huidige schijven onzin.
Nyland: "Ene Peter Gutmann heeft op de Unix conferentie in 1996 theorieën gepresenteerd over het herstellen van overschreven data. We hebben over de gehele wereld mensen gevraagd of ze tot zulke wonderen in staat zijn, maar hebben daarvoor nooit enig bewijs gevonden. Met de technieken die in de jaren tachtig gebruikt zijn, was het veel gemakkelijker dan nu. Tegenwoordig is alles veel complexer. De data zitten nu op een kleinere fysieke ruimte opgeslagen. De oude harde schijven hadden dedicated servo. Van de verschillende platen, afzonderlijke schijven met informatie, was er een bestemd voor servo positioneringsinformatie. Maar omdat de afzonderlijke platen nooit helemaal precies waren uitgelijnd, was er een zekere marge. Bij het overschrijven werd dan niet alle informatie overschreven, maar bleef er na de randen iets over, en die informatie kon soms teruggevonden worden. Daarnaast gebruikten die de RLL encodeermethode, die gewoon van nuldoorgangen gebruik maakte om een bit te detecteren. Tegenwoordig gebruikt men PRML, waarmee een veel groter gebied van de sinuscurve gebruikt wordt om middels verschillende algoritmen veranderingen te detecteren én om informatie op te slaan. Daardoor kun je de informatie ook veel dichter opslaan. Als alles overschreven is heb je ook de informatie over de gebruikte algoritmen niet meer en dan wordt het echt heel moeilijk. Bovendien wordt er een andere methode van positionering gebruikt, waardoor er geen onbeschreven randen meer overblijven. Er zijn ook theorieën waarbij je uitgaat van de informatie die je gebruikt hebt om te overschrijven, zodat je die kunt uitfilteren, maar ook dat blijkt in de praktijk niet werken."
Dus het is een broodje aap-verhaal?
"Ja, daar heeft het alle schijn van. Niettemin ondersteunt onze overwrite-software ook de Amerikaanse standaards die zeven keer overschrijven vereisen. Misschien dat NASA of de CIA nog data uit een één keer overschreven data kunnen halen, maar als het al zo is dan heb je enorme hoeveelheden rekenkracht nodig als je een poging wil wagen om met dit soort van dataherstel succes te hebben, anders kost het je tien jaar om twee letters te vinden. Maar als het echt heel gevoelig ligt dan kunnen we de schijf ook degaussen, dat is een veel drastischer methode."

(DdM: De door Nyman aangehaalde Gutmann beweert dat inlichtingendiensten gebruik maken van tunneling microscopen om data terug te vinden. Aan deze methode kleven zelfs nog meer nadelen dan Nyman noemt. Niet alleen ontstaan er enorme hoeveelheden data (in feite beelden) die geanalyseerd moeten worden, ook kan de microscoop geen verschil maken tussen de te ontcijferen data en nog eerdere geschreven data, wat het principe van Gutmann heel dubieus maakt. Tenslotte is er nog het feit dat niemand ooit in staat geweest is de gewiste achttien minuten op één van de Watergate-banden te herstellen. De data-dichtheid van de analoge banden uit de jaren zestig was circa een miljoen keer kleiner dan die bij de huidige harde schijven en het herstellen van audio-data is heel veel eenvoudiger dan het herstellen van digitale informatie. Niettemin is er nooit een enkele seconde uit de achttien gewiste minuten hersteld.)

een stuk moeilijker om te begrijpen wat er allemaal gebeurt."
Nyland: "Naarmate een systeem groter wordt, heb je ook een steeds ingewikkelder configuratie. Wanneer je die eenmaal verliest, dan kunnen de verschillende systemen niet meer met elkaar communiceren. Dat is ook een veel voorkomend probleem, dat je de juiste configuratie verliest."

Of een systeem complex is of niet, uiteindelijk blijkt dataverlies vrijwel altijd het gevolg van menselijke fouten.
Nyland: "Een klassiek voorbeeld zie je bij RAID-systemen. Als je vijf harddisks hebt en eentje gaat er stuk, dan kun je een rebuild maken en alles werkt weer prima. Maar dan vergeet je de defecte schijf te vervangen. De volgende keer dat een schijf kapot gaat, heb je geen parity meer, want je hebt de eerdere defecte schijf niet vervangen. Dan is het voorbij. Het is een veel voorkomende fout. Een ander probleem kan voorkomen bij een gemirrord RAID-syteem. Als systeem A het af laat weten, neemt systeem B het over. Prima! Wat er echter vaak gebeurt, is dat er 's avonds automatisch de inhoud van het ene systeem naar het andere gekopieerd wordt. Op een zeker moment gaat systeem A om welke reden dan ook ineens weer werken, door een reparatie of soms ook gewoon door toeval. Wanneer 's avonds dan de gewone kopieerroutine start, worden dus de data van systeem A naar B gekopieerd, terwijl dat precies omgekeerd had moeten zijn. Zo zie je dus dat ook dit soort heel veilige systemen fout kan gaan. Alweer: een menselijke fout. Stel je hebt tien servers en een back-upsysteem, dat iedere nacht back-ups maakt. Ineens wordt er een server aan toegevoegd, maar hij neemt die server niet op in het script, omdat hij niet van het script op de hoogte is bijvoorbeeld. Als er dan ineens iets mis gaat met die server, dan heb je geen back up. Neem een goed werkend tape back-upsysteem. Je systeem crasht, je herstelt het systeem en de back-upsoftware. Je data kopieer je dan de volgende dag. Maar 's nachts begint de back-upsoftware met de automatische back-up van het lege systeem. Het begin van je tape is daarmee overschreven en je hebt geen back-up meer."
Visser: "Men realiseert zich ook niet hoe kwetsbaar deze technologie is. Men is gewend aan mobiele telefoons die je bij wijze van spreken in het water kunt gooien en die nog steeds werken, en zo gaat men ook met een laptop om. Maar een harde schijf is nog steeds een heel complex instrument."

Worden de extreme prestaties van moderne harde schijven bereikt door het opzoeken van de grenzen van de technologie, ten koste van alle veiligheidsmarges?
Nyland: "Men is daarmee in ieder geval wel heel ver gegaan. Stel je daarbij dan ook nog eens voor wat een harddrive tegenwoordig kost. Je hebt die hoge precisie electro-mechanische apparatuur voor minder dan honderd Euro, het is bijna onvoorstelbaar dat het werkt."

Visser: "Als we een drive kunnen recoveren met brandschade die van 62 kilometer hoogte is gevallen, dan laat dat wel iets van onze expertise zien."

Hét middel om menselijke fouten zo veel mogelijk te beperken zijn procedures. Maar met het opstellen van procedures ben je er nog niet.
Nyland: "Je moet ze ook testen, doorloop de gehele procedure en en kijk waar de gaten zitten. Het gaat vaak om veel geld en de tijdsdruk is hoog. Mensen proberen hun eigen fouten te corrigeren en denken dat ze expert zijn op dit gebied, en zo volgt de ene menselijke fout op de andere. Met procedures voorkom je paniek. Daar horen ook dingen bij als het beheer van sleutels voor data die door encryptie beveiligd is, een groot probleem bij laptops overigens. Zorg er dus voor dat je encryptie-software een gedeelde sleutelstructuur heeft waarbij iemand administratieve rechten heeft en, heel belangrijk, test het.
Het doet er niet toe hoeveel geld je investeert in veilige systemen, logging of waar dan ook aan, als je geen mensen hebt die het allemaal controleren en testen, procedures opvolgen en actie ondernemen, dan is het niets waard. Op een dag zal het dan fout gaan, daar kun je zeker van zijn."

Dré de Man Tekst en foto's