Disaster recovery

Oracle en security (6)

Dinsdagmorgen 8.25: een telefoontje van Klaas, een ex-collega. Hij werkt sinds kort als hoofd ICT bij een Nederlandse vestiging van een multinational, die dagelijks producten levert aan supermarkten. Klaas heeft problemen met het restoren van een Oracle database. Het zou gaan om het restoren van een koude back-up. Een probleem hierbij zou zijn dat er wat archivelog files ontbreken. Ex-collega wil graag ondersteuning on-site om de verschillende opties en hun consequenties door te spreken.

Dinsdagochtend 9.15: Eerste bijeenkomst met Klaas, zijn baas Peter (hoofd administratieve organisatie) en twee SAP-specialisten. Het probleem wordt verder uitgelegd:
Het gaat om een SAP database ten behoeve van het logistieke proces van de Nederlandse vestiging. De database is een paar honderd Gigabytes groot en draait op een Windows-server. Er wordt dagelijks een koude back-up gemaakt op tape. De vrijdag daarvoor is er iets misgegaan en de back-up moet worden teruggezet. De restore duurt 17 uur, is al opgestart en zal nog een uur duren. De reden van het telefoontje is dat de archivelog files van de vrijdag weg zijn. In het verleden is al eens eerder een back-up teruggezet en er moest toen iets met de archivelog files gedaan worden.

Makkie

De eerste gedachte is: 'Makkie, voor het terugzetten van een koude back-up heb je de archivelog files echt niet nodig. Misschien bedoelen ze de redolog files, maar die kun je bij een koude back-up gewoon weer aanmaken. Eerst maar eens uitleggen hoe een koude Oracle back-up werkt en wachten totdat de restore klaar is.'
Nadat de restore klaar is, blijkt er toch recovery nodig te zijn. Toch geen koude back-up misschien? De klant blijft er van overtuigd, dat er elke werkdag een goede koude back-up wordt gemaakt. Daar hoeft niet naar te worden gekeken. De archivelog files ontbreken door een fout in de back-up procedure. De back-up blijkt zes dagen te draaien (maandag t/m zaterdag) terwijl er maar vijf tapes zijn (maandag t/m vrijdag). De back-up van zaterdag overschrijft vervolgens de tape van vrijdag.Deze procedure is in een ver verleden gemaakt door de toenmalige systeembeheerder, die nu niet meer bij het bedrijf werkt. Er is de laatstelijk nauwelijks meer tijd in gestoken omdat de hele infrastructuur op het punt staat om vervangen te worden. De nieuwe servers staan er al, maar zijn nog niet in gebruik genomen. Ook ARCserve zal vervangen worden door Networker.
Er is wel geconstateerd dat de back-up van zaterdag op de tape van vrijdag terechtkwam. Maar omdat er sinds het vertrek van de systeembeheerder niemand meer direct verantwoordelijk is voor de back-up en degene die constateerde dat de back-up van zaterdag op de tape van vrijdag terecht kwam "zeker wist" dat ARCserve "altijd" een append doet is niet opgevallen dat de back-up van vrijdag wel degelijk overschreven werd.
Omdat de nieuwe server klaar staat, wordt besloten om op de oude machine verder te proberen de daar teruggezette database in de lucht te krijgen (de back-up van donderdagavond) en parallel daaraan op de nieuwe machine de back-up van woensdagavond terug te zetten. Deze kan dan met de archivelog files van de back-up van donderdagavond weer worden bijgebracht tot donderdagavond.

Support

In de tussentijd wordt geprobeerd om zoveel mogelijk support van de leveranciers te krijgen. In dit geval is dat nominaal SAP, de leverancier van de ERP-software. Zij leveren ook de support op de onderliggende Oracle database. Sterker nog, volgens de letter van het contract vervalt hun support indien zaken rechtstreeks op de Oracle database worden gedaan, in plaats van via hun zelf geschreven support software. Vanwege de omvang van de ramp wordt er besloten om naast de support via SAP ook rechtstreeks support bij Oracle aan te vragen. Dit lukt: er wordt een speciale 'support identifier' geopend voor dit incident.

Ook de back-up van woensdagavond blijkt recovery nodig te hebben. Tijd om wat nauwkeuriger te kijken hoe de back-up

procedure in elkaar zit. Deze blijkt er als volgt uit te zien:
- Elke werkdag draaien er twee back-up jobs (ARCserve). Job A start op 22h00, job B start op 22h15.
- Job A stopt de database en maakt daarna een back-up van de helft van de datafiles.
- Job B maakt een back-up van de andere helft van de database.
- 's Ochtends wordt de database met de hand gestart en de tapes gewisseld.

Bij nadere bestudering blijkt de back-up procedure niet meer te draaien zoals bedoeld:
Job A en B zijn omgedraaid. Job B start om 22:00 met de helft van de back-up. Job A start om 22:15, begint met het stoppen van de database en doet de andere helft van de back-up. De back-up is dus inconsistent.

OK, het probleem is nu duidelijk en ernstig.

Onverstandig

Vanuit SAP-support komt de aanbeveling om te recoveren met een aantal archivelog files, dat zal het probleem wel oplossen. Oracle-support zegt, dat dit niet zal gaan werken en ook ik kan mij dit niet voorstellen. Omdat we nu toch twee corrupte databases hebben, een op de oude server en een op de nieuwe server, besluiten we beide paden te bewandelen. Ook al weet ik zeker dat de SAP-support oplossing niet gaat werken, blijft het onverstandig om de medewerking van SAP te verliezen door

Ook in de laatste maand van de levensloop van een systeem kan er iets misgaan

een door hen expliciet aangedragen oplossing te negeren. Oracle-support geeft aan dat de enige oplossing is om de database dan maar corrupt op te starten. Vervolgens meten via een export alle relevante data er uitgehaald worden. Hiermee moet een nieuwe database gevuld worden. De corrupte database 'mag' alleen maar gebruikt worden om gegevens uit te halen, er is geen enkele support van Oracle voor het gebruik van een corrupte database voor iets anders.
Het is niet mogelijk op een normale manier een Oracle database te openen, als de datafiles en de controlfiles niet in sync zijn met elkaar. Doordat de kopieeractie van de back-up al een kwartier bezig was voordat de database down ging, is dit niet het geval. De enige mogelijkheid om nu toch de database open te krijgen is door expliciet een aantal controles, die Oracle doet bij het opstarten van de database uit te zetten. Dit gebeurt met het zetten van een of meerdere undocumented initialisatie parameters. Tevens kunnen hiervoor een aantal events gezet worden. Het resultaat hiervan is een database die weliswaar open is, maar ook corrupt. Dit is een onherstelbare actie. Het enige zinvolle wat er met deze corrupte database nog gedaan kan worden is een export van de gegevens die er in zitten. Deze kunnen weer geladen worden in een nieuw aan te maken database, waarna overigens nog wel gekeken moet worden naar de integriteit en juistheid van de gegevens.

Samenloop

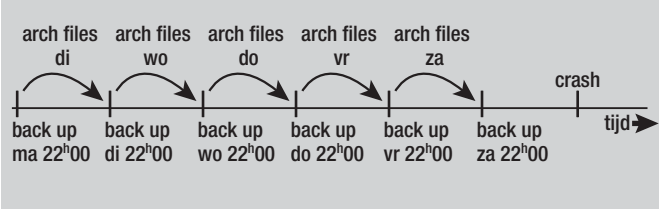
Het lukt om de back-up van donderdag avond op deze manier te openen. Overigens wel met de nodige problemen. Het alleen aanzetten van de nodige events is niet genoeg. Ook een aantal volstrekt ongedocumenteerde acties, waarmee nog wat transacties uit de online redolog files kunnen worden gehaald blijken noodzakelijk.
Besloten wordt om de gegevens uit deze database middels een export veilig te stellen. Hierbij moet worden opgemerkt dat het tunen van deze acties essentieel is. Toch zullen zowel de export als de import aanzienlijk langer gaan duren als een eenvoudige restore actie. En die duurt hier al 17 uur.

Later zal blijken dat de fout in de back-up procedure veroorzaakt is door een ongelukkige samenloop van omstandigheden:
- ARCserve onthoudt niet altijd de geplande starttijd van een job. Indien deze een keer later opgestart wordt, wordt de geplande starttijd vervangen door de actuele starttijd.
- De operator van de back-up heeft geen inhoudelijke kennis van de back-up procedure en was er dus niet van op de hoogte dat de volgorde van job A en job B belangrijk is.
- De operator had geen inhoudelijke kennis, omdat hij nog maar pas deze functie erbij had gekregen en de hele procedure binnen een maand volledig veranderd zou worden met de nieuwe infrastructuur.

Roll forward

Nog wat verder onderzoek levert op dat de fout pas afgelopen woensdag ontstaan is. De back-up van dinsdagavond zou goed moeten zijn. Het restoren van de back-up van dinsdag lukt niet. Eén van de tapes blijkt niet te lezen. Dat wordt dan de back-up van maandag. Dit is wel de laatste kans aangezien de tapes na een week overschreven worden.
Door problemen op woensdag met de back-up (dezelfde problemen waren de oorzaak van het verwisselen van de twee back-up jobs) dreigde de schijf met de archivelog files vol te lopen. Om dit te voorkomen zijn er archivelog files tijdelijk verplaatst naar de nieuwe server. Deze blijken nu goud waard te zijn. De restore van de back-up van maandag lukt en ook kan er een 'roll forward' gedaan worden naar het begin van de vrijdag (zie figuur).
Het eindresultaat is, dat het bedrijf een week lang niet in staat

geweest om artikelen te leveren aan supermarkten. De gegevens van de bewuste vrijdag zijn verdwenen uit de database. (Dat viel mee, er is alleen een aantal rekeningen de deur uitgegaan. Deze konden opnieuw worden aangemaakt in de database. Alleen kloppen de rekeningnummers niet met de verstuurde rekeningen. Er is vast nog wel wat werk en eventueel moet er nog wat uitgelegd worden aan de belastingdienst). Uiteindelijk geen ramp dus, maar het scheelde weinig.



Leermomenten

Eerder controleren van de back-up procedure had een etmaal gescheeld:

- Vertrouw als consultant nooit op de inhoudelijke kennis van je klant. Je wordt er tenslotte niet bijgehaald omdat ze het zelf wel weten.
- Ook in de laatste maand van de levensloop van een systeem kan er iets misgaan.
- Alle software en procedures dienen regelmatig getest te worden. Zeker een back-up procedure.
- Procedures dienen expliciet onder de verantwoordelijkheid van iemand vallen. En deze dient ze ook te begrijpen.

Het bovenstaande verhaal komt in grote lijnen daadwerkelijk uit de praktijk. De namen van de betrokkenen zijn natuurlijk wel aangepast, aangezien de meeste bedrijven het niet prettig vinden om met hun problemen in de pers te komen.

Adv. Oratech

Gerard Uiterwaal is Oracle- en security expert en werkzaam bij Motiv. Indien u in een van de volgende uitgaven van Optimize graag een specifiek onderdeel belicht zou willen zien dan kunt u dit aangeven via e-mail: gerard.uiterwaal@motiv.nl . De auteur streeft ernaar zoveel mogelijk vragen te beantwoorden.