Oracle 9*i* – Data Guard

Niet alles is wat het lijkt

Met de komst van Oracle 9i heeft Oracle een volgende stap gezet op het gebied van beschikbaarheid. Het mechanisme van de Hot Standby Database is aanzienlijk uitgebreid. In dit artikel wil ik de mogelijkheden belichten van Data Guard, zoals de voorzieningen rondom Hot Standby Databases vanaf deze Oracle-versie worden genoemd.

Vanaf september jl. ben ik betrokken bij een project waar honderd procent gegarandeerde beschikbaarheid van gecommitte transacties een bedrijfskritische factor vormt. Alle parameters (o.a. nieuwe techniek, nog weinig kennis in de markt voorhanden, flexibiliteit en mogelijkheden van de oplossing, schaalbaarheid) in ogenschouw genomen is besloten om voor deze omgeving Oracle 9i in te zetten. Als extra horde wordt het systeem fysiek in het buitenland gesitueerd en moet het beheer remote worden uitgevoerd. Dit behelst ook installatie van nieuwe Oracle releases, gegevensconversie als gevolg van software releases etc. De ervaringen met dit project leveren een prima basis op voor dit artikel.

Voorgeschiedenis

Het Hot Standby mechanisme is alweer enige jaren geleden ontstaan. Met Oracle7 werd het principe al door inventieve gebruikers geïmplementeerd. Hierbij werd de Standby Database gevoed met de Archived Redologfiles van de Primary Database. De Standby Database stond voortdurend in Recovery Mode. Op basis van scripts werden de Archived Redologfiles van de Primary naar de Standby Database getransporteerd. Oracle pakte dit idee al snel op voorzag in de nodige uitbreidingen in de beheertools om dit mechanisme wat gebruikersvriendelijker te maken en vanuit de database te ondersteunen. Stap voor stap werden de mogelijkheden uitgebreid. In het begin werden de Archived Redologfiles nog via NFS-koppelingen, ftp of anderszins naar de Standby Database gekopieerd. Later werd het mogelijk dit transport ook door Oracle in plaats van het besturingssysteem te laten verrichten door het Archive Proces de logfiles via Net8 naar de Standby Database te laten transporteren.

In deze opzet blijft het probleem bestaan dat transacties pas op de Standby Database beschikbaar komen nadat een logswitch een volgende Archived Redologfile genereert. Transacties die nog in de Online Redologfile 'verblijven' gaan dus verloren als na een crash van het systeem deze redologfile niet meer benaderbaar is. Oracle beveelt het gebruik van redundante redologfiles aan, waardoor de kans dat tenminste een set van de benodigde Online Redologfiles beschikbaar is, wordt vergroot. Daarmee blijft nog steeds het nadeel bestaan dat na systeemuitval voor de DBA een spanningsveld ontstaat tussen de druk vanuit de organisatie om het systeem op de Standby Server zo snel

> ***Met Oracle 7 al werd het hot standby mechanisme door inventieve gebruikers geïmplementeerd***

mogelijk weer beschikbaar te krijgen en de benodigde inspanning om de Online Redologfiles van de gecrashte Primary Database ter beschikking te krijgen. Als de CPU van de Primary Database het heeft opgegeven moeten immers eerst de schijven aan een ander systeem worden geknoopt om ze te kunnen uitlezen. Daarmee kan de nodige tijd verloren gaan.

Restrictie

Een ander niet te onderschatten nadeel van de implementatie van de Hot Standby Database is de restrictie dat een Standby Database wel de rol van de Primary Database kan overnemen, maar dan niet meer teruggeplaatst kan worden in de rol van Standby Database. Dat levert een forse hoeveelheid werk op als de Primary Server voor bijvoorbeeld onderhoud tijdelijk uit de lucht moet. Zeker als de hardware van de Standby Server lichter is uitgevoerd dan die van de Primary Server is het

gewenst de zwaarst uitgevoerde hardware zo snel mogelijk weer de rol van Primary Database te geven. Als er geen maintenance window beschikbaar is waarin het systeem uit de lucht kan vereist dat het opnieuw creëren van een Standby Database op de hardware van de oorspronkelijke Primary Database, een failover en het opnieuw creëren (re-instatiation) van de oorspronkelijke Standby Server. Dit gecontroleerd switchen gaat met behulp van Data Guard heel wat vriendelijker.

Tot dusver was de enige mogelijkheid om een honderd procent gegarandeerde beschikbaarheid van gecommitte transacties te verzorgen het gebruik van het 2-Phase-Commit (2PC) mechanisme. 2PC wordt onder meer gebruikt in een synchroon gerepliceerde database. Nadeel van deze oplossing is dat als één van de databases uit de lucht is, de 2PC transactie niet kan slagen. Hiermee neemt de MTBF en dus de beschikbaarheid af. Ik schreef over replicatie in de onlangs afgesloten reeks over Distributed Databases.

Data Guard

Met Oracle 9i zijn de mogelijkheden voor Standby Databases aanzienlijk uitgebreid. De Data Guard Manager neemt de DBA veel werk uit handen rondom het inrichten, configureren en beheren van de verschillende instances. Diverse zaken worden geautomatiseerd, beheer kan met behulp van een GUI worden uitgevoerd. Persoonlijk ben ik meer gecharmeerd van het gebruik van de combinatie van 'good old' SQL*Plus, scripts en 'vi'.

Prijsvraag (je)

Wie van de oudgedienden kent er nog het 'Oracle-tool' UFI? Waartoe dient dit tool en wat betekent deze afkorting?

Onder de inzenders van de goede oplossing worden een paar leuke verrassingen verloot. Mijn e-mail adres staat aan het einde van het artikel. Oplossingen zijn welkom tot twee weken na het verschijnen van dit nummer. 'Over de uitslag wordt niet gecorrespondeerd :-)'

Groot voordeel van het gebruik van scripts is de mogelijkheid commentaar op te nemen en werkzaamheden te kunnen herhalen. Daarnaast dwingen scripts tot het verkrijgen van inzicht in de materie. Na tachtig muisklikken in een GUI vraag je je nog wel eens af wat je ook al weer hebt gedaan om het resultaat te bereiken. Data Guard kan gebruik maken van een aparte netwerkverbinding voor het gegevenstransport. Hiermee wordt voorkomen dat de applicaties hinder ondervinden van dit extra netwerkverkeer. Data Guard biedt vier gradaties van gegevensbescherming. De termen laten zich wat lastig vertalen, ik noem de oorspronkelijke benaming er bij:

- Gegarandeerde bescherming (Guaranteed protection);
- Directe bescherming (Instant protection);
- Snelle bescherming (Rapid protection);
- Uitgestelde bescherming (Delayed protection).

De Data Guard Manager neemt de DBA veel werk uit handen rondom inrichting, configuratie en beheer

Het gaat hierbij niet om beschikbaarheid in termen van 'uptime', maar om beschikbaarheid in termen van 'geen gegevensverlies'. Voor een juiste uitleg van deze termen licht ik eerst nog twee andere termen toe: gegevensverlies en gegevensdivergentie. Als de Primary Database transacties verwerkt en deze worden niet tegelijkertijd in de Standby Database verwerkt dan zal de Standby Database gaan achterlopen. Het gevolg is gegevensdivergentie. Normaal gesproken zal de Standby Database de gegevens gewoon verwerken en in principe dezelfde toestand als de Primary Database bereiken. Als echter in een toestand van gegevensdivergentie de Primary Database crasht en de Standby Database de verwerking overneemt dan treedt gegevensverlies op. De verschillende gradaties van Data Guard onderscheiden zich in de mate waarin gegevensverlies kan optreden.

Gegarandeerde bescherming

Bij gegarandeerde bescherming wordt het optreden van gegevensdivergentie voorkómen. Een transactie wordt pas op de Primary Database doorgevoerd als de bijbehorende gegevens eerst door de Logwriter in de online Redologfile van de Standby Database zijn verwerkt. Dit is in feite vergelijkbaar met het 2PC mechanisme, zij het dat de transactie op de Standby Database logisch gezien altijd slaagt. Immers, omdat deze database zelf niet actief is kunnen integriteitsregels in deze database niet worden geschonden. Deze variant heeft het grootste effect op de performance van de Primary Database, ook al is de synchrone verwerking veel minder ingrijpend dan bij 'echte' 2PC. Het effect hiervan is vergelijkbaar met het gebruik van Synchrone Replicatie: De beschikbaarheid in termen van 'uptime' neemt af. Voor bijvoorbeeld financiële systemen is dat echter toch te prefereren boven gegevensverlies.

Directe bescherming

Bij directe bescherming zijn gegevens tot en met de laatste gecommitte transactie beschikbaar in zowel de Primary Database als in de Standby Database(s) zolang beiden beschik-

Primary Database Protection Mode	Database Protectie Status	instellingen Archived Log Bestemming	Status standby netwerk	Resulterende status Primary database	Resultaat switchover	Resultaat Failover
Gegarandeerde Bescherming	Protected	LGWR, SYNC etc.	Verbonden	Geen data-divergentie	Geen gegevens-verlies	Geen gegevens-verlies
			Verbroken	Instance Shutdown	Niet mogelijk	Geen gegevens-verlies
Directe bescherming	Unprotected	LGWR, SYNC etc.	Verbonden	Geen data-divergentie	Geen gegevens-verlies	Geen gegevens-verlies
			Verbroken	Uitgestelde gegevens-bescherming	Niet mogelijk	Gegevens-verlies
Snelle Bescherming	Unprotected	LGWR, ASYNC etc.	Verbonden	Gegevens-divergentie	Geen gegevens-verlies	Gegevens-verlies
			Verbroken	Uitgestelde gegevens-bescherming	Niet mogelijk	Gegevens-verlies
Vertraagde bescherming	Unprotected	ARCH	Verbonden	Gegevens-divergentie	Geen gegevens-verlies	Gegevens-verlies
			Verbroken	Gegevens-divergentie	Niet mogelijk	Gegevens-verlies

Data Guard biedt vier gradaties van gegevensbescherming, die zich onderscheiden in de mate waarin gegevensverlies kan optreden.

baar en via het netwerk met elkaar verbonden zijn. Dat betekent dat er, als we over meerdere Standby Databases beschikken, rustig één uit de lucht mag zonder dat we het gevaar lopen dat gegevens verloren gaan. Het is echter geen gegarandeerde bescherming: Als alle Standby Databases uit de lucht zijn treedt gegevensdivergentie op. Een crash van de Primary Database op dat moment leidt dan tot gegevensverlies.

De keuze voor een 'geen gegevensverlies'-variant leidt tot vertraagde beschikbaarheid van het systeem

Snelle bescherming

Snelle bescherming houdt meer rekening met de performance van de Primary Database. Gegevens worden zo snel mogelijk doorgestuurd naar de Standby Database(s) waarbij het effect op de performance zo klein mogelijk wordt gehouden. Gevolg is dat een storing in de Primary Database vrijwel zeker tot gegevensverlies leidt.

Vertraagde bescherming

Deze optie verdient misschien de term 'bescherming' maar nauwelijks. Met deze optie zullen gegevens 'uiteindelijk' in de Standby Database belanden, zolang het netwerk maar functioneert. Performance impact op de Primary Database is minimaal. Er is onderscheid tussen verschillende vormen van overname van de rol van Primary Database. Als dit op een gecontroleerde manier gebeurt heet dit een 'Standby Database Switchover'. Deze vorm van rolwisseling is omkeerbaar: na een

switchover kan een volgende switchover de oorspronkelijke Primary Database weer in deze rol terugbrengen. Dat is niet mogelijk als de rolwisseling ongecontroleerd gebeurt, dus na een storing in de Primary Database. Deze vorm heet 'Standby Database Failover'. Dit werkt dus vergelijkbaar met het oude Hot Standby Database mechanisme.

Concept

Onderstaand in tabelvorm een (vertaalde) samenvatting uit de conceptuele beschrijving van Data Guard in de Oracle handleiding: Als gebruik wordt gemaakt van meer dan twee databases is het mogelijk hardware te vervangen zonder dat het systeem uit de lucht hoeft. Net8 voorziet in de mogelijkheid van TAF (Transparent Application Failover) voor Oracle Call Interface (OCI) clients. Bij het uitvallen van de Primary Database schakelt de client automatisch over naar de Standby Database. Als de client op het moment van failover niet met een transactie bezig is gaat de failover in principe ongemerkt.

De Standby Database kan in twee vormen worden bijgehouden: de Managed Recovery Mode en Read-only Mode. In de Managed Recovery Mode worden de Archived Redologfiles

De Standby Database kan worden gebruikt voor het uitvoeren van (langlopende) queries.

automatisch naar de Standby Database getransporteerd en verwerkt. In Read-only Mode worden de Archived Redologfiles wel automatisch naar de Standby Database overgezet, maar niet verwerkt. De Standby Database kan worden gebruikt voor het uitvoeren van (langlopende) queries.

Een laatste optie, die ik bij deze introductie van Data Guard nog wil noemen, is het bewust vertraagd verwerken van de Redologs op de Standby Database. Zo kan bijvoorbeeld met twee Standby Databases zowel het risico van een hardware storing als het risico van een software fout worden afgedekt. Eén Standby Database wordt direct bijgewerkt en neemt over als de hardware van de Primary Database uitvalt. De tweede Standby Server loopt een bepaalde tijd, bijvoorbeeld acht uur, achter op de Primary Database. Als een software-fout de gegevens verminkt kan deze Standby Server worden bijgewerkt tot het moment juist voor het optreden van de software fout en vervolgens de taak van de Primary Server overnemen.

Conclusie

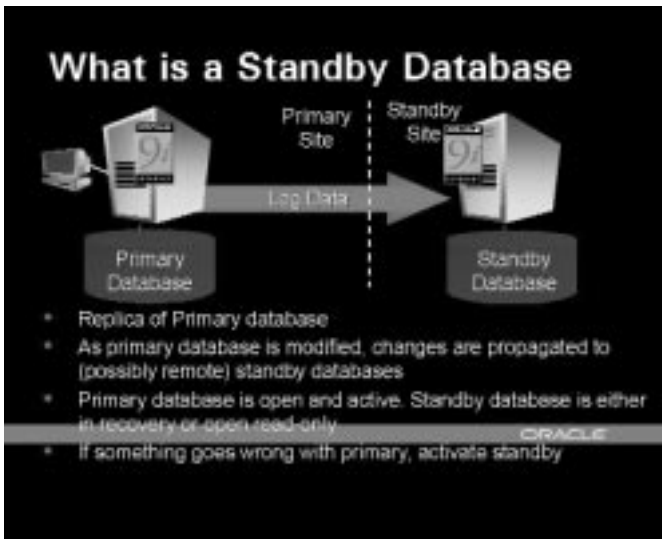
Met Data Guard heeft Oracle worden de mogelijkheden om te komen tot 24x7 beschikbaarheid verder uitgebreid. Het is een uitdaging al deze nieuwe technieken in een belangrijk project succesvol in te zetten. Data Guard biedt heel veel mogelijkheden en opties. Niet alles is wat het lijkt. Kiezen voor een 'geen gegevensverlies' variant leidt tot verlaagde beschikbaarheid van het totale systeem. Vermijding hiervan brengt weer aanzienlijke kosten van nog meer redundante hardware (en beheersuitgaven, software licenties, en, en!) met zich mee. Zorgvuldige afweging vooraf van de wensen en mogelijkheden is vereist. De toegenomen mogelijkheden maken het belang van deze afweging alleen maar groter. Als deze afwegingen op basis van een uitgebreide analyse zorgvuldig worden gemaakt staat de DBA en zijn gebruikers met Oracle 9i een veelbelovend product ter beschikking.

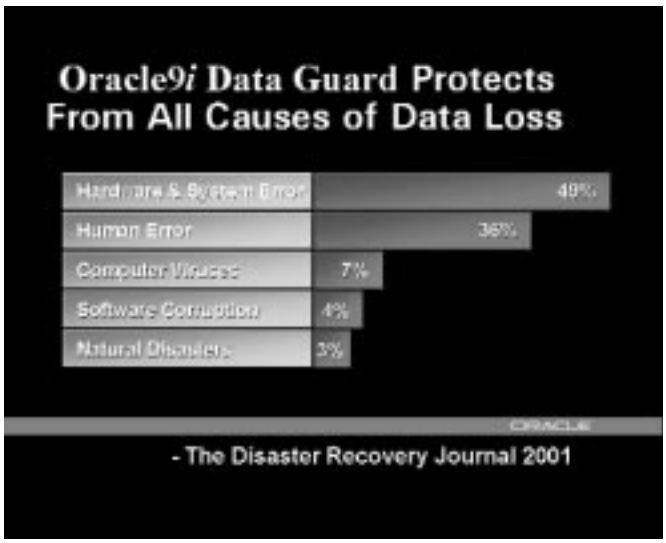
Literatuur:

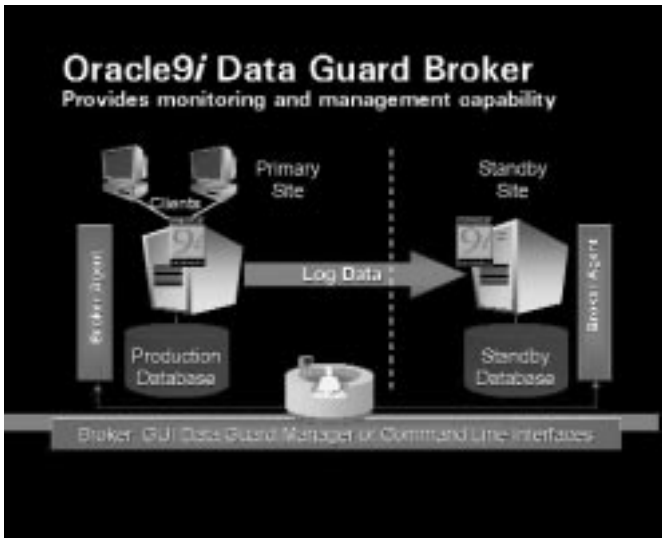
Titel: Data Guard Concepts and Administration Release 1 (9.0.1)
Part No: A88808-01
Uitgever: Oracle Corporation

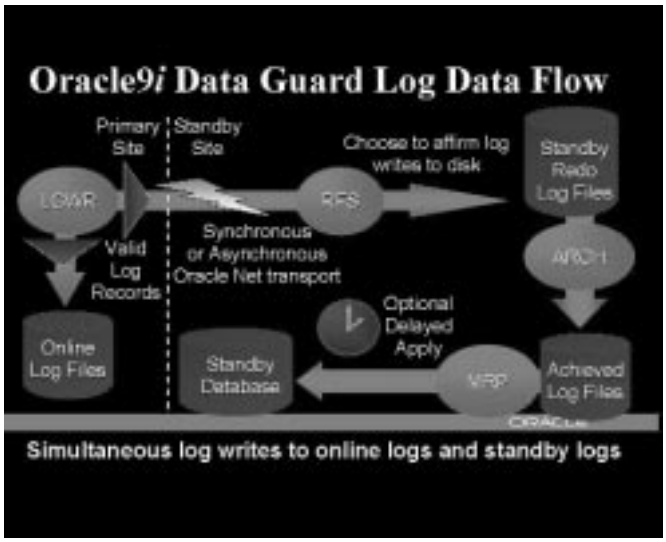
Titel: Data Guard Broker Release 1 (9.0.1)
Part No: A88807-01
Uitgever: Oracle Corporation

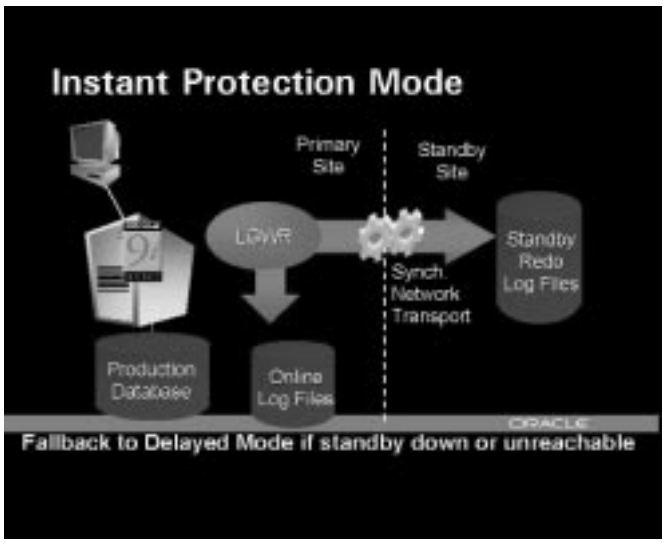
Carel-Jan Engel
is technisch directeur van, en senior problem solver bij Ease Automation BV. Hij is vanaf 1985 in verschillende rollen vrijwel ononderbroken bezig met ontwikkeling en beheer van systemen op basis van Oracle. E-mail: cjpengel@ease.nl

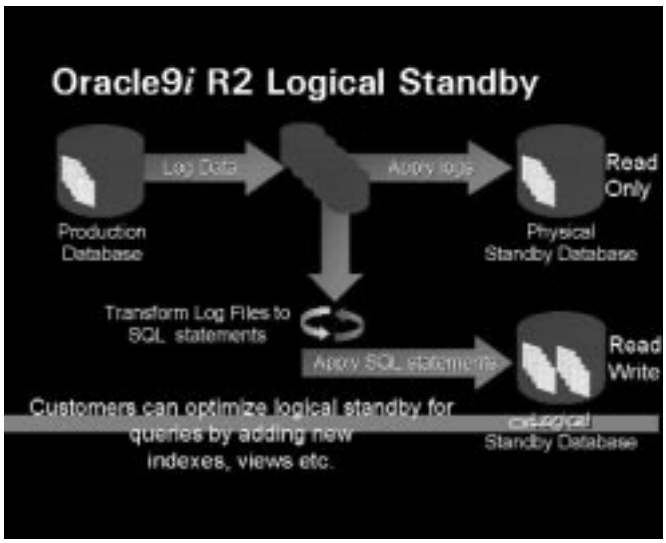












Enkele afbeeldingen uit een Oracle PowerPoint-presentatie over Data Guard.