



Active Data Guard 11g

Een knap staaltje werk van Oracle!

Oracle Database & Service technologieën worden door veel organisaties ingezet om de veiligheid van de bedrijfskritische data en de beschikbaarheid van applicaties en services te waarborgen. Oracle is niet voor niets al jaren lang marktleider in dit segment. Oracle's Database Server is het vlaggenschip van Oracle en versie 11g is op dit moment de meest recente uitvoering.

Met de Maximum Availability Architecture (MAA) biedt Oracle haar klanten een framework voor de inrichting van een infrastructuur met hoge beschikbaarheid. MAA beschrijft de componenten waarmee dit kan worden gerealiseerd. Dit zijn:

- Automatic Storage Management (ASM) voor optimale storage configuratie;
- Flashback Technologie als middel tegen het voorkomen van logische fouten;
- Recovery Manager (RMAN), een zeer solide backup manager;
- Advanced Security voor een optimale beveiliging van vertrouwelijke informatie binnen alle componenten van de infrastructuur;
- Real Application Clusters (RAC): de multi instance variant van de Oracle database, waarborgt > 99,9 beschikbaarheid en biedt ongekende schaalbaarheid m.b.t. CPU en Memory configuraties;
- RAC on Extended Distance Clusters, ook wel bekend als 'stretched' RAC of Geo-RAC;
- Data Guard, het veiligstellen van data op gescheiden fysieke locaties;
- Active Data Guard 11g, waarover straks meer.

In dit artikel gaan we verder in op de nieuwe mogelijkheden van Oracle Data Guard 11g en 11g Active Data Guard in het bijzonder.

Wat is Data Guard?

Data Guard is precies wat de naam aangeeft: een bewaker van data. Data Guard is de technologie waarmee bedrijfskritische

data, opgeslagen in de Oracle database, beschermd en bewaakt kan worden.

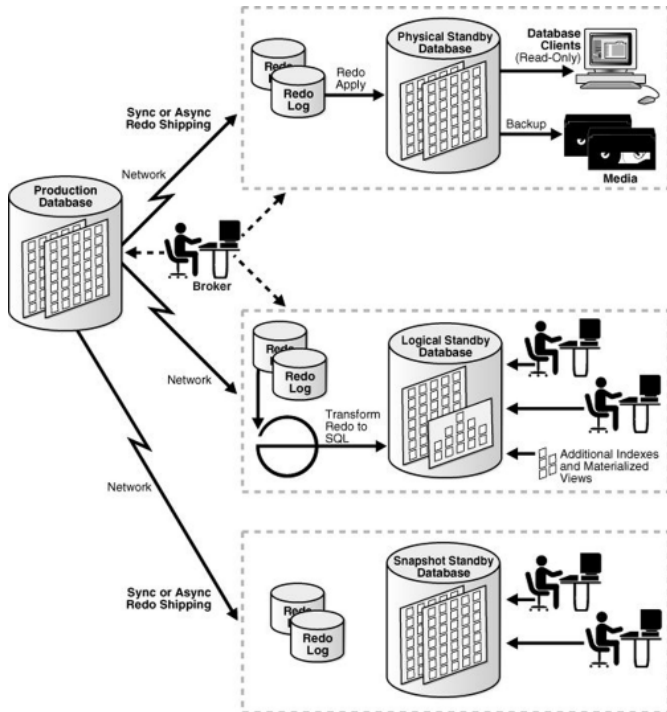
Het principe van Oracle Data Guard wordt sinds Oracle database versie 7 toegepast door DBA's. Naast de productie database werd, op een andere server, een kopie van de productie database gecreëerd en getransformeerd tot gesynchroniseerde 'standby' van de productiedatabase. De DBA zorgde ervoor dat door middel van het toepassen van archived redologs, zogenaamde 'redo logfile apply' de standby voortdurend gesynchroniseerd werd met de productie database. Kwam de productiedatabase om wat voor reden dan ook in de problemen, dan kon handmatig worden overgeschakeld naar de standby database. De netwerkverbindingen werden omgezet naar de standby database en men was weer in bedrijf.

Nadeel van deze opstelling is dat de standby in 'recovery mode' gezet dient te worden (de zogenaamde mount mode) om de redo informatie te ontvangen. Staat een database in mount mode dan is deze niet toegankelijk voor algemeen gebruik. Dit nadeel uit de Oracle 7 tijd is tot en met Oracle 10gR2 nooit echt weggenomen. Voor een standby database moest een normale licentie worden aangeschaft. Echt nuttig was de gesynchroniseerde standby database alleen in die sporadische noodmomenten. De standby kon immers niet zonder meer ingezet worden voor bedrijfsdoeleinden anders dan voor Disaster Recovery.

Sinds versie 7 is er veel veranderd en verbeterd aan het principe, tot het in versie 9 standaard in de database werd geïntroduceerd.

Data Guard configuraties

Data Guard kan op vele manieren worden geconfigureerd. Het principe is eenvoudig: aan een productiedatabase, in Data Guard termen de 'Primary database' kunnen één tot negen zogenaamde 'Standby' databases gecreëerd worden. Een Standby database kent drie mogelijke configuraties. De volgende illustratie laat de deze mogelijkheden zien:



Figuur 1: Schematische weergave Data Guard

In de figuur worden drie soorten standby databases onderscheiden. Deze worden hierna verder toegelicht.

De Physical Standby Database

De Physical Standby is een fysiek identieke kopie van de Primary database en kan zodanig ingericht worden dat deze synchronoos loopt met de Primary database. Synchronisatie vindt plaats door het realtime aanbrengen (Real Time Apply, ook wel RTA genoemd) van alle mutaties die plaatsvinden op de Primary database. Het 'Redo apply' synchronisatie proces kent geen beperkingen, alle mutaties worden verwerkt op de Standby. In een standaard Data Guard opstelling kan de Physical Standby tijdens het synchronisatie proces niet read-only geopend worden.

Logical Standby Database

De Logical Standby is een logische kopie van de Primary database en wordt gesynchroniseerd door middel van zogenaamde 'SQL injection'. Alle SQL afgevuurd op de Primary wordt ook afgevuurd op de Logical Standby. Een Logical Standby kan read/write geopend worden voor algemeen gebruik. Het 'SQL injection' synchronisatie proces kent echter beperkingen: zo wordt bijvoorbeeld het transport van LONG, LONG RAW enz. niet ondersteund.

Snapshot Standby Database

De Snapshot Standby is geïntroduceerd met versie 11g. Een Snapshot Standby database is een Physical Standby database die tijdelijk geopend wordt voor read/write toepassingen. Op de Snapshot kan geen redo apply plaatsvinden. Nadat de test ver-

richt is kan de Snapshot weer op eenvoudige wijze naar Physical Standby geconverteerd worden en kan het synchronisatie proces weer gestart worden. Het switchen van Physical naar Standby kan eindeloos herhaald worden. Verder kan een Snapshot Standby gebruikt worden als kopie van de Primary database in een Disaster Recovery scenario.

Voor elk van deze alternatieven geldt dat de fysieke afstand tussen de Primary en de Standby databases onbeperkt is. Alleen de bandbreedte van het netwerk is bepalend.

Data Guard Cluster: beveiligingsniveaus

Een Data Guard cluster, bestaande uit de Primary en een of meerdere Standby databases, kan in drie verschillende 'Data Guard Protection modes' geconfigureerd worden. De keuze wordt bepaald door de eisen die een bedrijf stelt aan het cluster. Dit zijn de drie Data Guard beveiligingsniveaus:

- maximum performance mode;
- maximum availability mode;
- maximum protection mode.

Maximum performance mode

Dit is de standaard instelling voor Data Guard. Transacties op de Primary database worden ge-commit als de redo data naar het online redolog is geschreven. De redo wordt ook naar één of meerdere Standby databases geschreven maar dit geschiedt asynchroon. Eventuele vertragingen in redo apply naar de Standby hebben geen invloed op de prestaties van de Primary database.

Maximum availability mode

Transacties op de Primary database worden pas ge-commit als de redo data synchronoos naar het online redolog is geschreven en naar tenminste een Standby database. Lukt dat laatste niet dan wordt overgeschakeld naar de standaard modus.

Maximum protection mode

Deze mode garandeert alle ge-commite data in het geval de Primary database down gaat. Een transactie wordt pas ge-commit als de redo data naar het online redolog is geschreven en - synchronoos - naar tenminste een Standby database. Lukt dit niet dan volgt een shutdown van de Primary database. Oracle raadt aan minimaal twee standby databases te configureren in deze opstelling. Alleen deze mode garandeert dat er zich geen data verlies zal voordoen in het geval van een calamiteit.

Data Guard: Disaster Recovery

Voorop het terrein van Disaster Recovery wordt Data Guard al jarenlang met succes ingezet. Het verlies van een rekencentrum komt niet vaak voor, maar kan voor een bedrijf wel het einde van haar bestaan betekenen. Met Data Guard kan

op relatief eenvoudige en kostenefficiënte wijze een zeer betrouwbare Disaster Recovery oplossing geïmplementeerd worden.

Door de introductie van Data Guard in versie 9i Release 1 is het configureren van een of meerdere standby databases sterk vereenvoudigd en makkelijker beheer(s)baar gemaakt. Met de door Data Guard geboden uitwijkmogelijkheden voor de Oracle database wordt ook de afhankelijkheid van OS en storage backup oplossingen sterk verminderd. En dat is een goede zaak. Tot op de dag van vandaag worden we geconfronteerd met Oracle databaseconfiguraties die niet op de juiste manier veiliggesteld worden. Met alle vervelende gevolgen vandien.

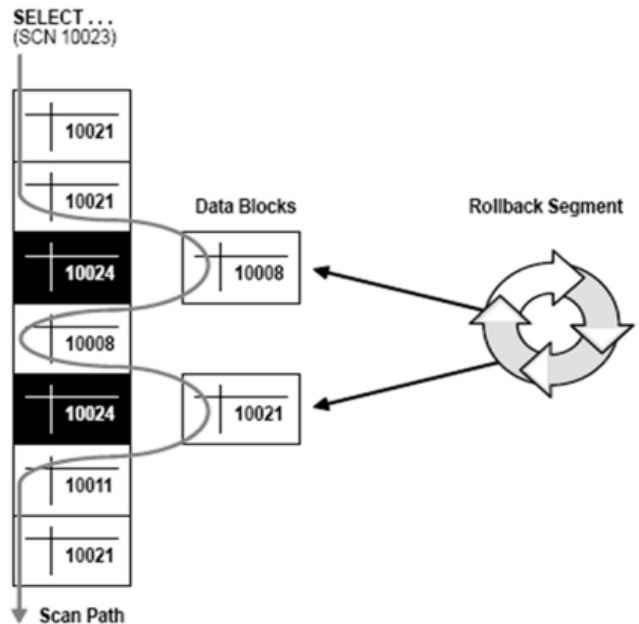
Standby databases: query read consistency

In essentie bleef de gesynchroniseerde physical Standby een enigszins geïsoleerd, nutteloos en duur bestaan leven. Tijdens het redo apply proces kan de Standby niet geopend worden voor algemeen gebruik.

Waarom kan een 10g Standby database niet read-only geopend staan tijdens redo apply? Is dat niet heel eenvoudig? Nee! Oracle staat dit niet toe en met reden! Tot en met release 10gR2 was Oracle namelijk niet in staat de 'read consistency' van queries op de standby database te garanderen. Read consistency houdt in dat, als een query wordt afgevoerd op de database, de query alleen de informatie ophaalt die aanwezig is in de database op het moment van starten van de query. De opgehaalde informatie wordt niet beïnvloed door andere transacties tijdens het uitvoeren van de query.

Hoe werkt dit intern? Op het moment dat een query afgevoerd wordt op een Primary database dan noteert Oracle het op dat moment geldende System Change Number (SCN). Het query mechanisme toetst bij het ophalen van informatie op de waarde van de in de database aanwezige SCN's. Is de waarde kleiner of gelijk aan het 'start SCN' van de query dan wordt de informatie opgehaald. Is het SCN groter dan gaat de query op zoek in het Rollback Segment, nu beter bekend als UNDO segment, naar informatie zoals die was voordat er een mutatie plaatsvond die tot een hoger SCN leidde. In dit voor oudere DBA's ongetwijfeld vertrouwde Oracle 7 diagram werd dit principe al duidelijk geïllustreerd.

Het diagram maakt het probleem waar Oracle mee geconfronteerd wordt duidelijk: informatie aanwezig in de Rollback Segmenten valt niet onder het Redo transport mechanisme en wordt dus NIET naar de Standby database getransporteerd. Had Oracle toegestaan dat we een 10gR2 Standby database read only hadden kunnen openen, dan was het resultaat van uitgevoerde queries ronduit onbetrouwbaar geweest: de staat van de standby database was immers als gevolg van het voort-



Oracle 7 Server Concepts.

durende synchronisatie proces – lees voortdurend olopemde SCN's - met de productie database voortdurend aan verandering onderhevig. Een query afvuren zou het zelfde zijn als 'shooting at a moving target'. Totdat Data Guard 11g uitkwam, en dan met name de Active Data Guard optie.

Active Data Guard 11g!

Met de komst van Oracle's 11g Active Data Guard option kan de Standby database eindelijk ingezet worden voor andere bedrijfsdoelen. De klant krijgt een uitstekende Disaster Recovery oplossing en kan daarnaast ook een of meerdere standby databases configureren die volledig ingezet kunnen worden voor diverse bedrijfsdoeleinden. De gesynchroniseerde standby database kan 'read-only' geopend worden terwijl deze toch voortdurend vanuit de Primary database realtime wordt bijgewerkt. En dat is een knap staaltje werk van Oracle!

De read consistency op de 11g Standby databases wordt afgedwongen door met 'Published READ SCN's en 'Applied' SCN's te werken. Wordt een query gestart dan gaat deze, in plaats van het start SCN, uit van het Published Read SCN terwijl het Applied SCN aangeeft waar de redo apply is gebleven. Wij hebben gezocht in de Standby database naar meer concrete informatie over hoe dit mechanisme werkt maar vooralsnog tevergeefs, het lijkt in de Oracle internals te zitten.

Verder is het redo apply mechanisme ingrijpend veranderd om andere inbreuken op het read consistency mechanisme te voorkomen. Denk bijvoorbeeld aan het voortijdig droppen van

packages die in eerder gestarte queries op de Standby database gebruikt worden.

Wat betekent Active Data Guard 11g voor organisaties?

Oracle's 11g Active Data Guard option betekent dat met een relatief geringe investering de Standby database zowel gebruikt kan worden in een Disaster Recovery configuratie als voor bedrijfsdoeleinden. Naar onze mening is alleen deze optie al voldoende aanleiding om de overstap naar 11g te maken!

Let wel: Data Guard is maakt deel uit van de 11g Enterprise Edition en is een optie bovenop de standaard aanwezige Data Guard functionaliteit. Een optie dus, waarvoor een licentie moet worden afgenomen voor zowel de Primary database als iedere Standby database waar Active Data Guard op wordt geactiveerd. Gelukkig zijn deze kosten relatief laag en gezien de mogelijkheden die geboden worden de investering meer dan waard.

De praktijk: Active Data Guard

Zo krachtig als Active Data Guard is, zo kort zijn de statements die uitgevoerd dienen te worden op de Standby database om de optie te activeren. Onder de motorkap is ongelofelijk veel veranderd, aan het oppervlak ziet het er als volgt uit: de Standby wordt read-only geopend terwijl Real Time Apply actief is:

```
C:\WINDOWS\system32\cmd.exe - sqlplus / as sysdba
SQL>sqlplus / as sysdba
SQLPlus: Release 11.1.0.6.0 - Production on Wed Dec 17 22:19:23 2008
Copyright (c) 1982, 2007, Oracle. All rights reserved.
Connected to an idle instance.
SQL> startup mount
ORACLE instance started.
Total System Global Area 523188352 bytes
Redo Size 1334292 bytes
Writable Size 499123180 bytes
Database Buffers 16777216 bytes
Log Buffers 5872664 bytes
Database mounted.
SQL> alter database recover managed standby database using current logfile disconnect from session;
Database altered.
SQL> select * from scott.dept;
select * from scott.dept
*
ERROR at line 1:
ORA-01219: database not open: queries allowed on fixed tables/views only
SQL> alter database recover managed standby database cancel;
Database altered.
SQL> alter database open read only;
Database altered.
SQL> alter database recover managed standby database using current logfile disconnect from session;
Database altered.
SQL> select * from scott.dept;
DEPTNO DNAME LOC
-----
10 ACCOUNTING NEW YORK
20 RESEARCH DALLAS
30 SALES CHICAGO
40 OPERATIONS BOSTON
SQL>
```

In het voorbeeld wordt eerst de 10gR2 situatie getoond: de select leidt tot een ORA-01219: de database staat in 'mount' mode. Daarna wordt de database read-only geopend en Real Time Apply geactiveerd. Nu levert de select resultaat op. Active Data Guard is actief!

Active Data Guard valt daarmee niet alleen onder Oracle's Maximum Availability Architecture (MAA) maar is ook uitermate beheer(s)baar of te wel 'manageable': een goede kandidaat voor de Maximum Available Manageable Architecture: MAMA!

Meer praktijk: aanmaken standby database(s) met RMAN

Veel klanten vragen ons hoe men snel een Standby database kan aanmaken. De 11g Data Guard handleiding wijst de weg maar doet dit nog op de oude manier: backup maken van de Primary, kopiëren naar de Standby etc. RMAN 11g biedt een elegante oplossing.

Met Oracle Database 11g is het "duplicate database" commando uitgebreid binnen RMAN. Vanaf Oracle 11g is het mogelijk om een database te kopiëren over het netwerk zonder gebruik te maken van de backup bestanden op disk of tape van de desbetreffende database. De nieuwe oracle optie die dit mogelijk maakt heet: "Active Database Duplication" of "Network-aware Database Duplication". Met de Active Duplication methode is het mogelijk om de database live te kopiëren, met minimale netwerk en CPU overhead, naar een andere of dezelfde machine. Het Active Duplication commando kan worden uitgevoerd met RMAN of Database Control.

Voor het uitvoeren van een Active Database Duplicate zijn vanaf de node waar de Primary database op draait het alleen nog maar het volgende RMAN commando's nodig. Let op, RMAN is een backup utility dus met 'Target' database wordt de Primary database aangeduid.

```
RMAN> connect target sys/sys@prim
RMAN> connect auxiliary sys/sys@primsb
RMAN> @rman_build_primsb
run {
    allocate channel c1 type disk;
    allocate auxiliary channel s1 type disk;

    duplicate target database
        for standby
        from active database
        dorecover
        spfile

    parameter_value_convert '\app\jvader\oradata\prim\','\app\jvader\oradata\primsb\'
        set db_unique_name='primsb'

    set db_file_name_convert='\app\jvader\oradata\prim\','\app\jvader\oradata\primsb\'

    set log_file_name_convert='\app\jvader\oradata\prim\arc1\','\app\jvader\oradata\primsb\arc1\'

    set control_files='\app\jvader\oradata\primsb\control01.ct1','\app\jvader\oradata\primsb\control02.ct1'
        set fal_client='primsb'
        set fal_server='prim'
        set standby_file_management='AUTO'
        set log_archive_config='dg_config=(prim,primsb)'

    set log_archive_dest_2='service=prim LGWR ASYNC valid_for=(ONLINE_LOGFILES,PRIMARY_ROLE) db_unique_name=primsb'
```

```

set log_archive_dest_state_2='enable'
set log_archive_format='primsb_%t_%s_%r.arc'
;
sql channel c1 "alter system archive log current";
sql channel s1 "alter database recover managed standby database using
current logfile disconnect";
}

```

Wordt dit script uitgevoerd dan is dit het resultaat:

```

C:\WINDOWS\system32\cmd.exe .rman
RMAN> run {
27 allocate channel c1 type disk;
28 allocate auxiliary channel a1 type disk;
29 duplicate target database
30 for standby
31 from active database
32 datafiles
33 spfile
34 parameter value convert ('app_loader@radata@primb','app_loader@radata@primb')
35 set db_unique_name='primb'
36 set db_file_name_convert='app_loader@radata@primb','app_loader@radata@primb'
37 set log_file_name_convert='app_loader@radata@primb','app_loader@radata@primb'
38 set control_files='app_loader@radata@primb/control01.ctl','app_loader@radata@primb/control02.ctl'
39 set fal_client='primb'
40 set fal_server='primb'
41 set standby_file_management='AUTO'
42 set log_archive_dest_2='service=prim LOGM BYNC valid_for=(ONLINE_LOGFILES,PRIMARY_ROLE) db_unique_name=prim'
43 set log_archive_format='primsb_%t_%s_%r.arc'
44
45 sql channel c1 "alter system archive log current";
46 sql channel s1 "alter database recover managed standby database using current logfile disconnect";
47
48 using target database control file instead of recovery catalog
49 allocated channel: c1
50 channel c1: SID=2 device type=DISK
51 allocated channel: a1
52 channel a1: SID=99 device type=DISK
53 Starting Duplicate Db at 17-DEC-08
54 contents of Memory Script:
55
56 backup as copy reuse
57 file 'G:\APP\loader\product\11.1.0\db_1\DATABASE\p00p01n_000' auxiliary format
58 'G:\APP\loader\product\11.1.0\db_1\DATABASE\p00p01n_000' file
59 'G:\APP\loader\product\11.1.0\db_1\DATABASE\SPFILEPRM_000' auxiliary format
60 'G:\APP\loader\product\11.1.0\db_1\DATABASE\SPFILEPRM_000'
61 sql clone alter system set spfile='G:\APP\loader\product\11.1.0\db_1\DATABASE\SPFILEPRM_000';
62
63 executing Memory Script
64 Starting backup at 17-DEC-08
65 finished backup at 17-DEC-08
66 sql statement: alter system set spfile='G:\APP\loader\product\11.1.0\db_1\DATABASE\SPFILEPRM_000'
67
68 contents of Memory Script:
69
70 sql clone alter system set log_archive_dest_1 =
71 'LOCATION=C:\app\loader\oradata\primb\arc1 UNDEF FOR ALL LOGFILES,ALL ROLES) DB_UNIQUE_NAME=prim' comment=
72 'primsb';
73 sql clone alter system set db_unique_name =
74 'primsb' comment=
75 'primsb';
76 sql clone alter system set db_file_name_convert =
77 'app_loader@radata@primb','app_loader@radata@primb' comment=
78 'app_loader@radata@primb';
79 sql clone alter system set log_file_name_convert =
80 'app_loader@radata@primb','app_loader@radata@primb' comment=
81 'app_loader@radata@primb';
82 sql clone alter system set control_files =
83 'app_loader@radata@primb/control01.ctl','app_loader@radata@primb/control02.ctl' comment=
84 'app_loader@radata@primb';
85 sql clone alter system set fal_client =
86 'primsb' comment=
87 'primsb';
88 sql clone alter system set fal_server =
89 'primsb' comment=
90 'primsb';
91 sql clone alter system set standby_file_management =
92 'AUTO' comment=
93 'primsb';
94 sql clone alter system set log_archive_dest_2 =
95 'service=prim LOGM BYNC valid_for=(ONLINE_LOGFILES,PRIMARY_ROLE) DB_UNIQUE_NAME=prim' comment=
96 'primsb';
97 sql clone alter system set log_archive_format =
98 'primsb_%t_%s_%r.arc' comment=
99 'primsb';
100 sql clone alter system set log_archive_dest_2 =

```

Om Active Database Duplication te kunnen gebruiken dient wel aan een aantal voorwaarden voldaan worden:

- beide omgevingen (Target en Duplicate DB) moeten ontsloten kunnen worden m.b.v. oracle Net;
- de omgevingen moeten hetzelfde OS platform hebben;
- de Primary database dient in archive log mode te staan;
- er dient een volledige RMAN backup van de Primary database te zijn;
- de Primary database dient in 'force logging' mode te staan;
- de Active Duplication optie werkt met Oracle password files die identiek zijn op beide nodes;
- de Primary database dient te beschikken over standby redo log files;
- op de standby dient een initprimsb.ora aanwezig te zijn met een entry: 'db_name=primsb';
- de ORACLE_BASE/admin/primsb directories dienen aanwezig te zijn.

En dat is alles – de Standby kan, aangestuurd vanuit een RMAN script, aangemaakt worden.

Nog een praktijkvoorbeeld: dynamische services

De Primary database draait in read/write mode, de Physical Standby in read-only mode. De gebruikers loggen aan op de Primary, alle reporting toepassingen op de Standby. Wat als er een zogenaamde role-switch plaatsvindt? De Primary & Standby wisselen van rol. Role-switching is een van de mogelijkheden die Data Guard biedt.

De oplossing is even simpel als doeltreffend: afhankelijk van de database rol (DATABASE_ROLE in V\$DATABASE) start de database bepaalde services op. De Oracle NET configuratie zorgt vervolgens voor een correcte afhandeling.

Dit is alles wat we nodig hebben: we maken twee services aan: SALES_RW voor de Primary, SALES_RO voor de Standby read-only database.

Vervolgens definiëren we de volgende database trigger op de databases:

```

CREATE OR REPLACE TRIGGER dynamic_service
after startup on database
DECLARE
    role VARCHAR(30);
BEGIN
    SELECT DATABASE_ROLE INTO role FROM V$DATABASE;
    IF role = 'PRIMARY' THEN
        DBMS_SERVICE.START_SERVICE('sales_rw');
    ELSE
        DBMS_SERVICE.START_SERVICE('sales_ro');
    END IF;
END;
/

```

En ziedaar: vindt een role-switch plaats, dan wordt connectivity via Oracle NET keurig afgehandeld!

Conclusie

Gecombineerd met Active Data Guard II is Data Guard een volwaardige software suite geworden. Deze suite biedt naast een relatief eenvoudig in te richten Disaster Recovery oplossing ook de mogelijkheid deze omgeving in te richten voor bedrijfsdoeleinden.

Veel bedrijven kampen met het probleem dat op de productie database talloze queries afgevuurd worden die vaak een negatieve impact op de performance hebben. Door de inzet van Active Data Guard kan dit probleem op eenvoudige wijze opgelost worden.

Jan Vader en **Jos van den Oord** zijn senior Oracle DBA consultants bij Whitehorses met een focus op het realiseren van beschikbare, veilige en schaalbare IT platformen met behulp van Oracle technologie.



Haal jij eruit wat erin zit?

Bij Truston zoeken we altijd de balans tussen werk en privé. Simpelweg omdat wij vinden dat mensen werken om te leven en niet leven om te werken. Daarom streven we dan ook altijd lange termijnrelaties na. Bouwen we dag in dag uit aan de toekomst van onze klanten en onze mensen. Om nu en in de toekomst aan onze hoge kwaliteitsstandaard te blijven voldoen, zoeken wij voortdurend specialisten om ons team te versterken. Bezoek voor meer informatie en de openstaande vacatures www.truston.com en haal eruit wat erin zit.