Data Guard auf der ODA

David Hueber, dbi services ltd.

Ziel aller IT-Systeme ist es, für die Endbenutzer und/oder Kunden einen Service zu erbringen. Je nachdem, wie kritisch dieser Dienst ist, werden „Service Level Agreements" geschlossen, die von der IT-Infrastruktur gewährleistet werden müssen. Damit wird die System-Verfügbarkeit zu einem Schlüsselbegriff beim Aufbau von produktiven IT-Systemen. Die Oracle Database Appliance (ODA) unterstützt mehrere solcher hochverfügbaren Lösungen – eine davon ist Data Guard.

Verfügbarkeit besteht auf drei Ebenen:

- Verfügbarkeit der Hardware
- Verfügbarkeit des Dienstes
- Verfügbarkeit der Daten

Man könnte dieser Liste noch die Verfügbarkeit der Website hinzufügen. Die Verfügbarkeit der Hardware ist im Grunde die Kapazität der zugrunde liegenden Hardware, physische Ausfälle zu unterstützen beziehungsweise zu überdauern. Das reicht von Themen wie „Netzwerk" über elektrische Ausfälle bis zu Festplattenfehlern. Um diesen Bereich abzudecken, wurde die ODA als hochredundante Architektur ausgelegt, die Lösungen wie Netzwerkbindung, redundante Stromversorgung, mehrere Controller und natürlich ASM-Redundanz umfasst.

Dienst- und Datenverfügbarkeit bei der Oracle-Datenbank schützen im Wesentlichen vor Instanz- und Datenbank-Abstürzen *(siehe Abbildung 1)*. Für die Verfügbarkeit der Dienste integriert die ODA mehrere Out-of-the-Box-Lösungen:

- RAC One Node
- RAC

Diese sind direkt in OAKCLI integriert *(siehe Listing 1)*. Nach der Beantwortung von sechs Fragen und rund dreißig Minuten Verarbeitungszeit erhält man eine voll funktionsfähige Zwei-Knoten-Real-Application-Cluster-Datenbank.

Eine ODA umfasst eine ASM-Redundanz mit normaler oder hoher Redundanz, aber es bleibt ein gemeinsam genutzter Speicher zwischen beiden Knoten, der ausfallen kann und noch anfälliger für eine logische Korruption ist. Wenn die ODA mit der Oracle Database Enterprise Edition läuft, bedeutet das, dass Data Guard ohne zusätzliche Kosten zur Verfügung steht. Von daher kann man eine Data-Guard-Konfiguration zwischen zwei ODAs einrichten, um die Verfügbarkeit der Daten und sogar Dienste zu erhalten, wenn man einen Fast Start Failover konfiguriert. Leider hat die ODA die Data-

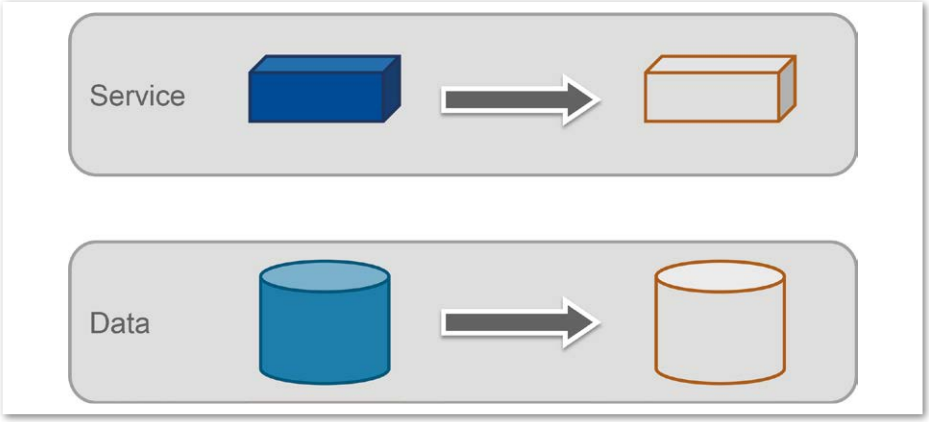

Abbildung 1: Typen der Hochverfügbarkeit

```
Bitte wählen Sie eine der folgenden Optionen für die Datenbankbereits-
tellung [1 … 3]:
1 => EE: Enterprise Edition
2 => RACONE
3 => RAC
3
Ausgewählter Wert ist: RAC
```

Listing 1

```
[dhu-oda1]# oakcli create dbhome
Bitte geben Sie das Benutzerpasswort für den Root ein:
Bitte geben Sie das Benutzerpasswort für den Root nochmals ein:
...
...
```

Listing 2

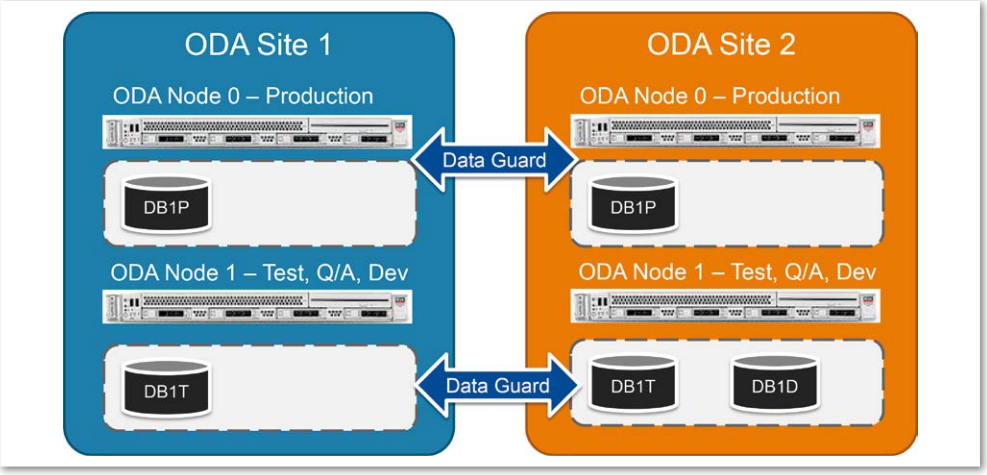

Abbildung 2: ODA-Data-Guard-Implementierung

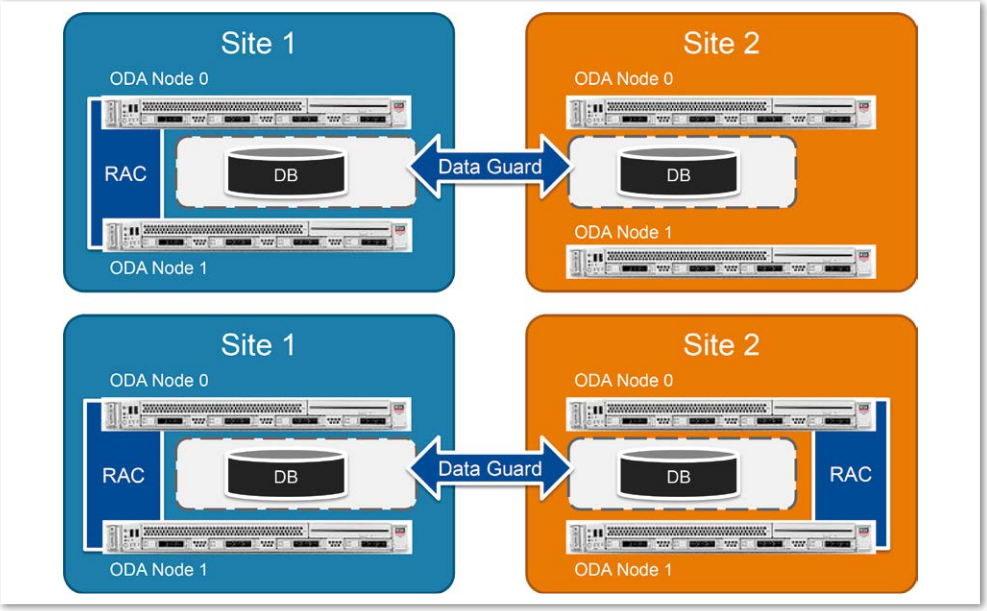

Abbildung 3: Maximal-Available- und Maximum-Availability-Architektur

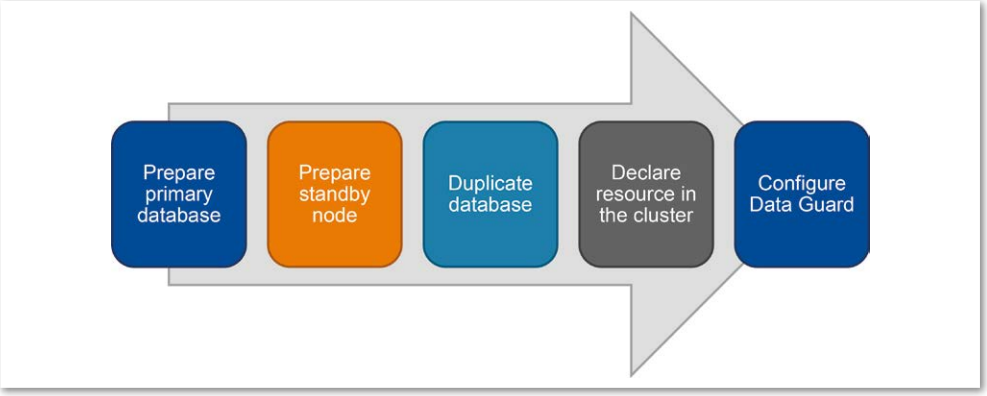

Abbildung 4: Prozess-Überblick

```
[root@dbi-oda2 snaps]# acfsutil snap create -w DBITEST /u02/app/oracle/
oradata/datastore/

acfsutil snap create: Snapshot-Vorgang ist abgeschlossen.
```

Listing 3

Guard-Einrichtung in OAKCLI (noch?) nicht integriert. Das bedeutet, dass der DBA dies noch manuell erledigen muss.

Es ist zu beachten, dass Data Guard (oder Data Guard alleine) nicht alle Fälle abdeckt. Wie immer sind einige Analysen erforderlich, um die optimal geeignete Lösung auszuwählen. Aber aus Erfahrung des Autors decken die verschiedenen Möglichkeiten, um Data Guard und ODA zu implementieren, etwa 75 bis 90 Prozent der Fälle ab.

ODA- und Data-Guard-Implementierung

Das Einrichten von Data Guard zwischen zwei ODAs trägt zu einer Antwort für eine Verfügbarkeitslösung bei, kann jedoch auch einen anderen Punkt lösen, der nicht unterschätzt werden sollte, nämlich die Verfügbarkeit einer Prüf-Umgebung. Eine brandneue ODA in der Produktion ist sehr gut, aber man möchte vielleicht Patches oder neue Versionen von Oracle oder der Anwendungen testen. Die ODA-Architektur ermöglicht eine Implementierung, die beide Fragen durch die Bereitstellung von Knoten für die Produktion beantwortet und Data Guard zwischen den ODAs einrichtet *(siehe Abbildung 2)*.

Grundsätzlich sind mehrere Implementierungslösungen, Test- oder Entwicklungsdatenbanken möglich. In der Tat lässt sich dank der In-Memory-Option, die in der ODA vollständig integriert ist, auch die zweite ODA für eine BI-Umgebung nutzen. Man könnte auch Lösungen wie beispielsweise Fast Maximal Available (AMA) oder Maximum Availability Architecture (MAA) wählen *(siehe Abbildung 3)*.

Die Einrichtung einer Data-Guard-Konfiguration kann grundsätzlich durch ein Verfahren zusammengefasst werden *(siehe Abbildung 4)*. Die Vorbereitung des Primärdatenbank-Schritts verläuft wie bei jeder anderen Umgebung. Man sollte alle Parameter wie „FORCE LOGGING“ oder „DG_BROKER_CONFIG_FILE1/2“ konfigurieren.

Auf der Standby-Seite gibt es, ausgehend von einer brandneuen ODA, ein bisschen mehr zu erledigen:

- *Erstellen eines „ORACLE_HOME“*
  Falls nicht der Standard verwendet wird
- *Erstellen der Ordner-Struktur*
  Seit Version 12 sind Datenbanken auf ACFS-Volumes gespeichert. Diese müssen für die neue Datenbank eingerichtet sein.

```
[root@dbi-oda2 ~]# oakcli create dbstorage -db DBITEST
INFO: 2015-06-08 00:00:31: Beachten Sie die Protokolldatei /opt/oracle/oak/log/
...
...
INFO: 2015-06-08 00:02:36: Speicherstruktur für die Datenbank ‚DBITEST' erfolgreich eingerichtet
INFO: 2015-06-08 00:02:36: Legen Sie für die Datenbank DBITEST die folgende Verzeichnisstruktur fest
INFO: 2015-06-08 00:02:36: DATA: /u02/app/oracle/oradata/datastore/.ACFS/snaps/DBITEST
INFO: 2015-06-08 00:02:36: REDO: /u01/app/oracle/oradata/datastore/DBITEST
INFO: 2015-06-08 00:02:36: RECO: /u01/app/oracle/fast_recovery_area/datastore/DBITEST

SUCCESS: 2015-06-08 00:02:36: Speicher für die Datenbank erfolgreich eingerichtet: DBITEST
```

Listing 4

```
  (SID_DESC =
      (GLOBAL_DBNAME = DBITEST_SITE2.it.dbi-services.com )
      (ORACLE_HOME   = /u01/app/oracle/product/12.1.0.3/dbhome_1 )
      (SID_NAME = DBITEST)
  )
```

Listing 5

```
RMAN>duplicate target database for standby from active database dore-
cover nofilenamecheck;
...
...
archived log file name=/u01/app/oracle/fast_recovery_area/datastore/
DBITEST/DBITEST_SITE2/archivelog/2015_04_28/o1_mf_1_2081_bmynm39y_.arc
thread=1 sequence=2081
media recovery complete, elapsed time: 00:00:03
Finished recover at 28-APR-2015 11:27:07
Finished Duplicate Db at 28-APR-2015 11:27:15
```

Listing 6

```
oracle@dbi-oda2:$ srvctl add database –db DBITEST_SITE2
-oraclehome $ORACLE_HOME
-dbtype SINGLE
-role PHYSICAL_STANDBY
-spfile /u02/app/oracle/oradata/datastore/.ACFS/snaps/DBITEST/DBITEST_
SITE2/spfileDBITEST.ora
-pwfile /u01/app/oracle/product/12.1.0.2/dbhome_1/dbs/orapwDBITEST -db-
name DBITEST
-startoption mount
-stopoption immediate
-instance DBITEST
-node dbi-oda2
-acfspath "/u01/app/oracle/oradata/datastore,/u02/app/oracle/oradata/
datastore,/u01/app/oracle/fast_recovery_area/datastore"
```

Listing 7

- *Vorbereiten von „SPFILE" für eine Standby-Datenbank*
  Eingeben eines temporären statischen Eintrags in „LISTENER"

Sobald das Duplikat erstellt wurde und die Standby-Datenbank funktionsfähig ist, bestehen die letzten Schritte darin, die neue Datenbank im Cluster der Standby-ODA zu erklären und die Data-Guard-Konfiguration zu erstellen.

Standardmäßig verfügt jede neu installierte ODA bereits über ein „ORACLE HOME" des neuesten verfügbaren Release (derzeit 12.1.0.2.3). Wird ein separates „ORACLE HOME" für die Standby-Datenbank benötigt, kann man es mit „OAKCLI" installieren *(siehe Listing 2)*.

Beim Wechsel der ODA von Version 2.10 auf 12.1.2.0.0 kommt es zu einer umfassenden Änderung der Architektur. Der Datenbank-Speicher wechselt von „Raw ASM" zu „ACFS". Dies hat Einfluss auf die Art und Weise, wie die Speicherung für die Standby-Datenbank vorbereitet werden muss. Für Nicht-CDB-Datenbanken gibt es im Grunde drei Standard-ACFS-Volumes:

- *Redo- und Steuerdatei-Volumes*
  Gemountet unter „/u01"
- *Daten-Volumes*
  Gemountet unter „/u02"
- *Wiederherstellungs-Volumes*
  Gemountet unter „/u01"

Bei jedem dieser Volumes ist eine Struktur für jede Datenbank vorgesehen. Zudem ist das Daten-Volume Snapshot-basiert, was bedeutet, dass alle Datendateien in einem ACFS-Snapshot gespeichert sind. Bis Version 12.1.2.1.0 musste man diese Struktur manuell mit „mkdir", „chown", „chmod" und „acfsutil" erstellen. Die Redo- und Reco-Struktur werden einfach mit „mkdir" angelegt und die Zugriffsrechte wie für andere Datenbanken. Für das Daten-Volumen ist ein Befehl erforderlich, um den neuen Snapshot zu erstellen *(siehe Listing 3)*. Seit der Version 12.1.2.2.0 ist der gesamte Prozess in „OAKCLI" integriert und funktioniert jetzt ziemlich einfach *(siehe Listing 4)*.

Wie bei jeder Data-Guard-Einrichtung muss die Standby-Datenbank in „NOMOUNT" gestartet werden, bevor das Duplikat laufen kann. Dafür ist ein „SPFILE" erforderlich. Die einfachste Möglichkeit ist die Verwendung einer der primären Datenbanken sowie die folgende Anpassung:

- *db_unique_name*
  Wird nicht auf der Primär-Datenbank festgelegt, die mit „OAKCLI“ erstellt wurde.
- *control_files*
  Der Parameter, der Namen und Pfad der Steuerdatei(en) definiert, muss aus „SPFILE“ gelöscht werden. Da alle Oracle Managed Files (OMF) auf Basis der ODA sind, lässt sich der Name der Steuerdatei(en) nicht vorab definieren. Durch Löschen des/der Parameter(s) wird/werden er/sie von RMAN während des Duplizierens mithilfe des OMF-Mechanismus neu erstellt.
- *db_create_file_dest, db_create_log_file_dest, db_create_log_file_dest2*
  Diese Parameter definieren, wo Steuerdatei(en), Redo-Logs und Datendateien erstellt/gespeichert werden. Die ersten beiden sollten bereits ordnungsgemäß konfiguriert sein. Es könnte sich jedoch lohnen, „f db_create_log_file_dest2“ festzulegen, um einen Mirror von Redo-Logs und Steuerdateien zu erhalten. Um Leistungsverluste zu vermeiden, benutzt man einen Pfad auf den SSD-Festplatten.

Die Erstellung der Standby-Datenbank erfolgt üblicherweise mit einem Duplikat der aktiven Datenbank. Das bedeutet, dass sowohl auf die Ziel- als auch auf die Hilfs-Datenbank mit „TNS“ zugegriffen werden muss. Da sich die Standby-Datenbank an diesem Punkt nur im „NOMOUNT“-Zustand befindet, ist ein statischer Eintrag im Listener erforderlich, um darauf zuzugreifen.

Der Zuhörer wird vom Netz-Benutzer verwaltet und die Datei „listener.ora“ befindet sich unter „$GRID_HOME/network/admin“. Im Abschnitt „SID_LIST_LISTENER“ muss ein Eintragstyp hinzugefügt werden *(siehe Listing 5)*. Dieser kann entfernt werden, sobald die Duplizierung abgeschlossen ist. Es ist zu beachten, dass Data Guard in 12*c* den Namen des DGB-Dienstes verwendet. Das bedeutet, dass der traditionelle „DGMGRL-Eintrag“ nicht mehr erforderlich ist. An diesem Punkt kann man seinen bevorzugten RMAN-Befehl verwenden *(siehe Listing 6)*.

Sobald die Standby-Datenbank erfolgreich erstellt ist, muss sie im Cluster deklariert werden, um die Vorteile von Oracle Restart nutzen zu können. Dieser Vorgang erfolgt als Oracle-Benutzer durch „SRVCTL ADD DATABASE“ *(siehe Listing 7)* mit folgenden Optionen:

- db_unique_name
- ORACLE_HOME
- Datenbank-Typ
- Datenbank-Rolle
- SPFILE -Standort
- Speicherort der Passwortdatei
- db_name
- Startmodus, „OPEN“ ist Active Guard, anderweitig lizenziert „MOUNT“
- Stopp-Modus
- instance_name
- Running-Knoten
- ACFS-Volumes

Das Erstellen der Data-Guard-Konfiguration ist ähnlich wie bei jeder anderen Data-Guard-Konfiguration und erfolgt mithilfe von „DGMGRL“. Man wählt den Übermittlungsmodus der Logs und den für die Bedürfnisse und die Erstellung am besten geeigneten Schutzmodus *(siehe Listing 8)*.

Der Punkt ist erreicht, an dem Data Guard voll funktionsfähig ist und eine Umstellung durchgeführt werden kann. *Listing 9* zeigt den Status, den die Datenbanken auf beiden ODAs jetzt haben. Die Umstellung verläuft geradlinig *(siehe Listing 10)*. Bei der erneuten Überprüfung der Datenbanken sind diese korrekt eingestellt *(siehe Listing 11)*. Ab jetzt ist die frühere Primär-Datenbank definiert als „PHYSICAL_STANDBY“ und wird im „MOUNT-Modus“ gestartet, während die neue Primär-Datenbank als „PRIMARY“ deklariert ist und im OPEN-Modus gestartet wird.

Tipps und Tricks

Auf einer ODA, die noch mit Version 2.10 läuft, wird die Duplizierung für den Standby mit einem Fehler fehlschlagen *(siehe Listing 12)*. Der Blick in die „alert.log“-Datei der Datenbank offenbart ein Zugriffsproblem *(siehe Listing 13)*. Dieses Problem ist auf einen Zugriffsfehler der Oracle-Binärdateien zurückzuführen, der im MOS-Hinweis 1.084.186.1 beschrieben wird. Die Lösung ist die Verwendung von „setasmgidwrap“ für „ORACLE HOME“ *(siehe Listing 14)*.

In einer AMA-Architektur ist die Primär-Datenbank eine RAC, während die Standby-Datenbank eine einzelne Instanz ist. Das bedeutet, dass die Primär-Datenbank über zwei Redo-Logs-Threads und die Standby-Datenbank nur über einen einzigen verfügt. Damit eine solche Data-Guard-Einrichtung jedoch ordnungsgemäß funktioniert, sind für die Standby-Datenbank zwei Standby-Redo-Logs-Threads erforderlich.

Umstellung auf Oracle 11*g*

Bei einem 11*g*-Data-Guard unterscheidet sich das Verhalten der Datenbank-Ressourcen während einer Umstellung etwas. *Listing 15* zeigt den Zustand vor der Umstellung und *Listing 16* danach. Wie wir sehen, sind die Ressourcen nur teilweise angepasst, was folgende Konsequenzen hat:

- Die neue Primär-Datenbank wird bei einem ODA-Neustart nur in „MOUNT“ gestartet und der 11*g*-Broker wird sie nicht öffnen
- Die Standby-Datenbank wird im „OPEN“-Modus gestartet, womit Active Guard aktiviert ist

Nach Überprüfung im Oracle-Support und Öffnen eines Service Request kam heraus, dass es nur zwei Lösungen/Workarounds gibt:

- Lizenzierung von Active Guard und Konfigurieren des Einrichtungsmodus „OPEN“ für beide Datenbanken
- Manuelles Ändern der Cluster-Ressourcen-Parameter nach jeder Umstellung oder Failover

Fazit

Die Kombination von Data Guard und ODA ist definitiv eine interessante Lösung, um mehrere Anliegen wie beispielsweise Datenverfügbarkeit, Standort-Notfälle oder Test-Umgebungen zu lösen. Falls es seit der ersten Version zur Verfügung steht, sind es die erheblichen Verbesserungen mit Version 12*c* wert, alle Vorteile solcher Architekturen zu nutzen.

Alle weiteren Listings finden Sie online unter:
www.doag.org/go/doagsoug/201506/listing

David Hueber
david.hueber@dbi-services.com