Backups im HA Umfeld, nur für Ewiggestrige? – am Bsp. Exadata MAA Setup

Konrad Häfeli
Trivadis AG
CH-3014 Bern

Schlüsselworte:

Backup, BR, Hochverfügbarkeit, High Availability, HA, Maximum Availability Architecture, MAA, Oracle Database Machine, Exadata

Einleitung

Backups sind Redundanzen die zur Absicherung von bestimmten Ausfallszenarien erstellt werden. Ist aber in einer Hoch- resp. Höchst-Verfügbarkeits Umgebung ein physisches Backup überhaupt noch angebracht? Ueberlegungen zu Backupstrategien, daraus resultierenden Konzepten und deren Implementation in einer Maximum Availability Architecture (MAA) eines Exadata Setups werden aufgezeigt. Der Vortrag stellt die in der Praxis angetroffenen Einschränkungen von Rechenzentren, deren Netzwerktopologien und die zum Teil bestehenden Backupinfrastrukturen vor. Die damit verbundenen Risikoabschätzungen die zum Konzept und einer Implementation mit RDBMS und RMAN Funktionalität geführt haben, werden diskutiert. Es soll dem Leser Anregungen geben das eigene Konzept zu hinterfragen und den einen oder anderen Lösungsansatz aus der Praxis vermitteln.

.

Klassische Backups

Ja, die guten alten Zeiten! Der Datenbankserver mit seinen lokalen Disks, welche die Datenbankfiles beinhalten und die Backups auf eine meist sehr kleine Tape-Library wegschrieb. Online, meist aber Offline Backups wurden praktiziert, früher noch ohne RMAN mit sogenannten „User Managed Backups“. Die Disklayouts wurden mit der Zeit redundant mit sogenannten RAID Levels ausgelegt und auch die Backupinfrastruktur wurde grösser, ausfallsicherer und automatischer. Die Angst vor einem produktiven Restore vor korrupten Backup-Bändern blieb aber. Auch die Desastersicherheit, der Backuptapes wurde noch lange mittels auschecken der Bänder in einen feuerfesten Tresor, oder für kleinere Volumen sogar durch das Mitnehmen nach Hause durch die verantwortliche Person wahrgenommen.

Die Auswirkungen von ungenügenden Backupverfahren, welche sich durch Ausfallzeiten der Systeme oder vielfach auch Datenverlust manifestiert, sind je nach Unternehmung verschieden. In einer Umfrage von IDG Research im Mai 2012, hatten 2/3 der Unternehmen Produktivitätsverluste, gefolgt von Reputationschäden, Finanzielle Auswirkungen, sowie Verlust von sensitiven oder unersetzbaren Daten zu beklagen.

Backupstrategie im HA Umfeld

Backup ist für jedes Unternehmen etwas Individuelles:

- Anforderungen
- Risiken und deren Beurteilung
- Massnahmen für die Risikominimierung

Müssen für die jeweiligen Umstände definiert und betrachtet werden.

Es gibt keine harte Grenze zwischen einer Hochverfügbarkeit (HA) und Backup/Recovery (BR) Strategie. In den meisten Fällen führen hohe BR Anforderungen zu einer HA Stategie.

Backup/Recovery ist keine „Best Effort“ Angelegenheit, es basiert auf klar definierten Anforderungen bezüglich Verfügbarkeit der Systeme und Daten

- Maximale Ausfallzeit (RTO -> Recover Time Objective)
- Maximaler Datenverlust (RPO -> Recover Point Objective)

Auch der Einsatz von Produkten, Funktionalitäten und Tools wird aus den Anforderungen abgeleitet. Es führt in den meisten Fällen zu ungenügenden Umsetzungen, wenn man das Backupkonzept aus der vorhandenen Infrastruktur ableitet.

Über ein einfaches Wasserfall Vorgehen kommt man zu strukturierten Lösungen im BR Umfeld:

- Strategie
    - Konzept
        - Implementation
            - Dokumentation (Handbuch)

Wie wird nun so eine **Backupstrategie** definiert? Zuerst muss eine Verfügbarkeitsanalyse zur Bestimmung der Anforderungen gemacht werden:

- Verfügbarkeit generell (z.B. 99.9%)
- In welcher Periode (z.B. Mo-Fr 06:00-21:00)
- Auswirkungen von Ausfallzeiten (geplante sowie auch ungeplante)
- Auswirkungen der Anzahl sowie der Dauer von Ausfällen
- Auswirkungen von Datenverlust

Danach müssen Checklisten für die Anforderungen durchgearbeitet werden:

- Maximum unplanned downtime (mean time to recover, MTTR)
- Maximum data loss (pro Ereignis)
- Retention time für backup data
- Anforderungen für data archiving (bestimmte snapshots ausserhalb der retention time)
- Auch Lösungen ausserhalb des BR einbeziehen (Datenreproduktion)

Eine detaillierte Risikoanalyse ergibt die Szenarien und deren möglichen Auswirkungen welche mit der Strategie angegangen oder auch ausgelassen werden. Dabei ist die Reduktion der Szenarien eine wichtige Tätigkeit, da dadurch eine Implementation meist erheblich vereinfacht werden kann.

- ***Der grösste Feind der Verfügbarkeit ist die Komplexität!***

Eine Umfrage der IOUG von diesem Jahr zeigt auf, dass nebst menschlichen Fehlern (45%) und klassischen Server und Storage Ausfälle vor allem Netzwerkprobleme auf die Verfügbarkeit der Systeme drücken. Das ist nicht verwunderlich, ist die Vernetzung der Systeme in den letzten Jahren dermassen komplexer geworden, dass Abhängigkeiten meist nicht mehr eruiert werden können.

Ist die Strategie definiert muss das Konzept erarbeitet werden, darin ist die Umsetzung beschrieben, welche nun auch das physische Volumen der Daten und der Backups miteinbezieht. Das Backupkonzept ist im HA Konzept integriert.
Folgende Themen werden definiert:

- … “advanced HA features” (z.B. Data Guard) wenn nötig
- … die B&R Szenarien
- … die adequaten B&R Utilities
    - User or server managed backup (physical), data pump (logical), flashback, log miner…
- … die Anwendung der Utilities
    - Type of backup (full, incremental, skip read only, archive log, controlfile, spfile, logical)
    - Type of device (disk, tape)
    - Type of destination (file system, flash recovery area, media manager software)
- … die Intervalle der Backups
    - Daily/weekly/…

    - Hourly/… archive log backup
- … die Methode des Scheduling
    - Scheduled by media manager, crontab, enterprise manager,…
- … das Monitoring
    - Via backup script's own error handling, media manager scheduler, EM, …
- … die Verantwortlichkeiten

Im Folgenden muss die Implementation des Konzeptes gemacht werden, werden die Abläufe gescripted oder kommen Tools zum Einsatz. Die Implementation ist nicht fertig bis die Dokumentation (B&R Handbuch) geschrieben ist, alles getestet, die Backups verifiziert und die Verantwortlichen geschult sind.

Es kann heute festgestellt werden, dass mit physischen Restores die hohen RTO Anforderungen meist nicht erfüllt werden können. „Near zero" oder "zero data loss" Szenarien sind mit klassischen Backup Methoden nicht möglich. Vielfach treffen auf hohe RTO/RPO Anforderungen auch hohe Desaster Recovery (DR) Anforderungen, was meist eine Duplizierung der Lokationen benötigt. Eine Lösung könnten die angepriesenen sekundenschnellen Backups und restores auf Disk-Snapshot Technologien sein, die sind aber (meist) nicht DR fähig.

Daraus lässt sich schliessen:

➔ ***Ein physisches Backup ist nicht mehr die Methode für die Abdeckung des ersten Fehlerfalles, hat aber in der Backupstrategie immer noch Relevanz***

Denn die komplexen HA Funktionalitäten müssen auch noch zusätzlich abgesichert werden, denn wenn die nicht greifen, dann haben wir nichts mehr… Die physischen Backups sind somit das Fangnetz für einen doppelten Fehlerfall. Murphy lässt grüssen ;-)

Eine immer währende Diskussion ist der Einsatz des richtigen Mediums für diese physischen Backups. Die gute alte Tape-Technologie wird immer mehr von den Disk-Backups Systemen verdrängt. Die Frage aber ob Kosten/Nutzen dasselbe sind ist nicht einfach zu beantworten (hängt von den verschiedenen Argumentarien ab, mal ist das Eine besser mal das Andere). Meist aber ist ein Tape-Backup für Langzeitarchivierung um einiges im Vorteil.

Backupkonzept für Exadata MAA
Folgende Anforderungen und Umsetzungen ergaben sich nach der Analyse in einem Kundenbeispiel:

- RPO: "Near zero data loss"
- RTO: < 10 Minuten (ungeplant)
- Unterstützung der geplanten Downtime < 30 Minuten

➔ Standby System mit Oracle Data Guard im MAX_AVAILABILITY Mode

- Retention 10 Tage
- Archiving 1 Jahre (Monat, Quartal, Halbjahr, Jahr)

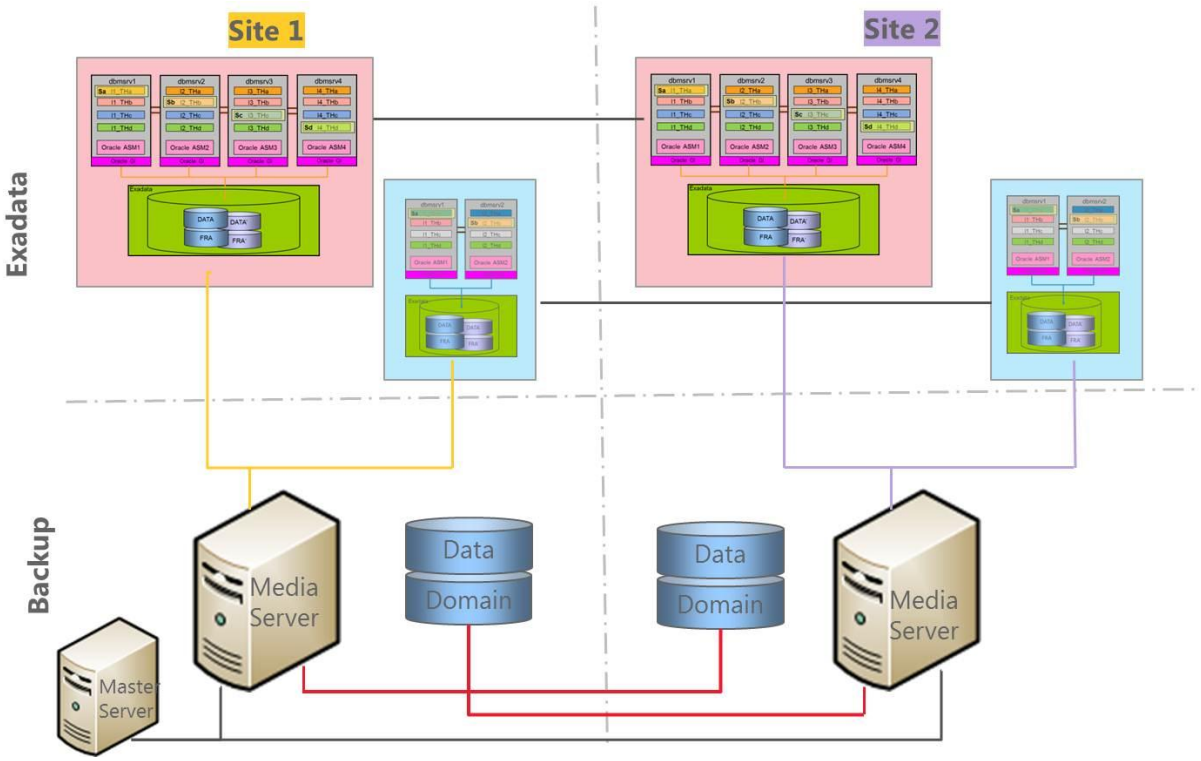
➔ Symantec NetBackup mit EMC DataDomain

- Automatisation der Backups
- Standardisierung der Recovery Szenarien
- Automatisierte Bereitstellung von Test und Abnahme Umgebungen

➔ Script Umgebung mit TVD-BackupTM
➔ Scheduler Oracle Enterprise Manager

➔ Monitoring via Tool Mailinterface, plus EM User Defind Metrics (UDM) an Nagios

Vielfach kann ein System nicht optimal an eine Backupinfrastruktur angebunden werden, da schon gewissen Fakten, man könnte auch sagen Altlasten, herrschen. Beim hier beschriebenen Kundenprojekt liess der Dienstleister für das Backup nur folgende Architektur zu:



Für die Implementation wurde ein hochverfügbarer Backupservice, erstellt, welcher gleichzeitig eine virtuelle IP als Abhängigkeit mit sich zieht:

- Pro Site pro Datenbank eine VIP konfiguriert als Backup Client (NB_ORA_CLIENT)
- Hochverfügbarer Backup Service pro DB pro Rolle (Primary/Standby)
- Die VIP fix an den Service als Cluster Resource gebunden

➔ Ermöglicht die Sicherstellung des Backups unabhängig vom physischen Server

➔ Ermöglicht den Restore einer Datenbank unabhängig auf welchem Server das Backup gemacht wurde

➔ Ermöglicht ein rollenspezifisches Backup und auch Houskeeping der Oracle Files (archlogs, backups) auf beiden Sites

- Implementiert mit Cluster Befehlen (appvipcfg, srvctl, crsctl)

Dadurch ergab sich ein recht flexibles Konstrukt, das weder an einen physischen Host (beim Backup, aber vor allem auch nicht beim Restore) gebunden ist, gleichzeitig aber über den Cluster hochverfügbar bereitgestellt werden konnte:

- Tägliches INC0 auf den konfigurierten Backup-Knoten (Service running)
    - Auf dem Standby Service
    - Auf die Flash Recover Area
    - Backup der FRA auf Tape

    - Housekeeping auf der FRA und auf Tape
- Alle 3 Stunden ein Archivelog Backup mit delete input
    - Auf dem Standby Service
- Alle drei Stunden ein Archivelog_Housekeeping Job
    - Auf dem Primary Service

Implementationsrestriktionen aus der Praxis
Die Hauptursache, dass es Restriktionen gegeben hat, beruht auf der Tatsache, dass der Backupdienstleister sein Infrastrukturkonzept OHNE die DBAs gemacht hat und somit die Anforderungen der Datenbankbackups nicht eingeflossen sind. Das ist natürlich ein grosses Problem, kann aber im Nachhinein nur mit einem Workaround und der Flexibilität auf DB Seite umgangen werden.

Was können wir mitnehmen:
- B&R ist ein Verfügbarkeits-Thema (Anforderungen/Risiken)
- Reduktion der Komplexität erhöht die Verfügbarkeit
- B&R implementieren, dokumentieren, testen, trainieren
- Physische Tapes sind immer noch im Einsatz, der Markt bietet heute aber auch interessante Disk Storage basierende Produkte
- Bei HA Systemen soll auch der Backup-Service hochverfügbar sein
- Restore muss unabhängig vom physischen Server möglich sein
- Frühzeitig an der Konzeption von Backup Infrastruktur mitwirken, erspart viel Diskussion und Unzulänglichkeiten

➔ ***Nicht nur Ewiggestrige machen Backup im HA Umfeld, Backup ist Konzept, basierend auf einer Strategie!***

Es gibt noch viel Interessantes im Bereich Funktion und Anwendung beim Einsatz der Exadata Database Machine und Backupstrategien zu erzählen, der Autor steht gerne für Fragen zur Verfügung.

Kontaktadresse:

Konrad Häfeli
Trivadis AG
Papiermühlestrasse 73
CH-3014 Bern

Telefon: +41(0)31-928 09 60
Fax: +41(0)31-928 09 64
E-Mail konrad.haefeli@trivadis.com
Internet: www.trivadis.com