Safety First – Sicherungskonzepte von Oracle-E-Business-Suite-Umgebungen für Oracle Cloud Infrastructure

Johannes Michler, PROMATIS Gruppe, Ettlingen (TechnologieRegion Karlsruhe)

Die Oracle Cloud Infrastructure (OCI) wird von vielen unserer Kunden für den Betrieb ihrer Oracle E-Business Suite verwendet. Besonders, wenn nicht nur Entwicklungs- und Testsysteme in der OCI betrieben werden, wird hier ein solides Konzept zur Sicherung (und Wiederherstellung) der Umgebung für den Katastrophenfall benötigt – egal ob dieser durch Benutzer- oder Systemfehler ausgelöst wird. Sehen wir uns die möglichen Optionen hierfür einmal genauer an.

Grundkonzepte und Terminologie – RPO und RTO

Die beiden wichtigsten Begriffe beim Entwurf einer Backup-Strategie sind zweifellos Recovery Point Objective (RPO) und Recovery Time Objective (RTO). RPO ist die akzeptierte Datenmenge, deren Verlust im Falle einer Katastrophe in Kauf genommen wird. Beispielsweise bedeutet ein RPO von 30 Minuten, dass man nach Eintritt einer Katastrophe in keiner Situation mehr als 30 Minuten an Transaktionen verlieren möchte. RTO bezeichnet die Zeit, die benötigt wird, um die Instanz nach einer Katastrophe wieder betriebsbereit zu machen. Die Oracle-Dokumentation der Datenbank – insbe-

sondere „High Availability Overview“ – bietet weitere Einzelheiten dazu *(vgl. [1])*.

OCI-Isolationsgrade

Es gibt drei mit der Oracle Cloud Infrastructure verbundene Isolationsgrade, die zum Schutz vor Ausfällen beitragen, siehe dazu die OCI-Dokumentation:

- Region: Eine Region ist ein stark isolierter Teil der Oracle-Cloud-Infrastruktur, der sich in einem geografischen Gebiet befindet, zum Beispiel EU-Frankfurt oder US-West (Phoenix). Die regionale Trennung bietet beispielsweise sogar Schutz vor großen Naturkatastrophen.
- Verfügbarkeitsdomäne (Availability Domain; abgekürzt mit AD): Die meisten Regionen sind in drei Verfügbarkeitsdomänen unterteilt. Dabei handelt es sich um isolierte Datenzentren, wodurch ein gleichzeitiger Ausfall sehr unwahrscheinlich ist. Da Verfügbarkeitsdomänen die Infrastruktur (wie Stromversorgung oder Kühlung) oder das interne Netzwerk der Verfügbarkeitsdomänen nicht gemeinsam nutzen, ist es unwahrscheinlich, dass ein Ausfall in einer Verfügbarkeitsdomäne innerhalb einer Region die Verfügbarkeit anderer Domänen innerhalb derselben Region beeinträchtigt.
- Fehlerdomäne: Dies ist eine Partition innerhalb eines Rechenzentrums. Indem Recheninstanzen in verschiedenen Fehlerdomänen platziert werden, hat der Ausfall einer physischen Maschine in Fehlerdomäne 1 keine Auswirkungen auf eine physische Maschine (und deren virtuelle Maschinen) in Fehlerdomäne 2.

Block, Object und File Storage

Die Oracle Cloud-Infrastruktur bietet drei persistente Speichertypen mit unterschiedlichen Vor- und Nachteilen. Alle drei Typen sind auch für Backups relevant:

Block Storage ist ein Speichertyp, der an eine Recheninstanz entweder als Boot- oder als zusätzliches Volume angeschlossen ist. In der Regel erfolgt die Anbindung über iSCSI. Obwohl die Performance sehr hoch ist, befindet sich der Block Storage in nur einer Verfügbarkeitsdomain (Domain, in der die Recheninstanz läuft). Block-Volumes können bequem zu definierten Zeiten durch Backup-Richtlinien gesichert werden, wobei diese Backups auch regionenübergreifend in Object Storage abgelegt werden können. Alle Daten von Oracle-E-Business-Suite-Instanzen (Apps- und DB-Tier) befinden sich normalerweise auf Block-Volumes *(siehe [2])*.

Object Storage kann als „Web-Service“ betrachtet werden, mit dem besondersgroße Objekte gespeichert und abgerufen werden können. Wie in *[3]* genannt, handelt es sich um einen Service „pro Region“; Object Storage ist dabei durch die automatische Speicherung zahlreicher Kopien über mehrere Verfügbarkeitsdomains hinweg äußerst robust.

File Storage bietet einen NFS-Einhängepunkt, der an mehrere Recheninstanzen gemountet werden kann, letztendlich auch über Verfügbarkeitsdomains hinweg (oder sogar Regionen, wenn diese verbunden sind). Während der Dienst ein „pro AD“-Dienst ist, kann sich der File Storage in AD1 befinden und eine Recheninstanz in AD2, was einen bequemen Zugriff auf den Speicher ermöglicht (vgl. *[4]*). Der Dienst bietet Snapshot-Funktionen und speichert mehrere (dauerhafte) Kopien aller Daten (innerhalb eines AD).

Ziele dieser Diskussion

Für den weiteren Umfang dieses Artikels werde ich Strategien beschreiben, die dabei helfen, ein RPO und RTO (für Produktionssysteme) von jeweils etwa 30 Minuten zu erreichen. Die Strategie sollte in der Lage sein, Ausfälle einer Verfügbarkeitsdomain zu bewältigen, muss aber nicht „regionale Ausfälle“ abdecken.

In diesem Beitrag werde ich drei verschiedene Szenarien behandeln, da für diese unterschiedliche Verfahren geeignet sind:

- Umgang mit Entwicklungsinstanzen
- Umgang mit Conference Room Pilot oder anderen Testinstanzen
- Umgang mit Produktivinstanzen

Entwicklungsinstanzen

Bei Entwicklungsinstanzen ist ein komplettes Backup der Instanz in der Regel nicht notwendig. Im Falle einer Katastrophe ist man normalerweise in der Lage, eine neue Entwicklungsinstanz als neue Kopie des Produktionssystems einfach zu erstellen. Wenn alle Entwickler nach „gängigen Best Practices“ arbeiten, befindet sich ihr gesamter Quellcode in einem Quellcode-Verwaltungssystem und kann wieder problemlos auf dem neuen Entwicklungssystem installiert werden.

In der Realität ist dies jedoch nicht immer der Fall. Insbesondere bei der PL/SQL- und APEX-Entwicklung ist es eine weit verbreitete Praxis, direkt in der Datenbank zu entwickeln und nur gelegentlich den Quellcode in ein Versionskontrollsystem zu übernehmen – oft erst beim Übergang von der Entwicklung zum Testen.

Um dieses Szenario zu bewältigen, ist es ratsam, auch „einige Backups“ von Entwicklungssystemen durchzuführen. In der Regel ist es jedoch ausreichend, die folgenden Inhalte zu sichern:

- (Benutzerdefinierte) Datenbankobjekte wie Pakete, Prozeduren oder Views: Diese können leicht durch expdp mit einem Filter auf Objektnamen im Muster „XX%“ gesichert werden, der beispielsweise um 8 Uhr morgens, mittags und um 16 Uhr nachmittags ausgeführt wird. Das Ergebnis kann auf File Storage in einer anderen Verfügbarkeitsdomain gesichert und von dort nach Erstellung einer neuen Entwicklungsinstanz wiederhergestellt werden.
- APEX-Anwendungen können mit sqlcl gesichert werden *(siehe [5])*. Dies kann wiederum mehrmals täglich ausgeführt und das Ergebnis auf File Storage geschrieben werden.
- XML Publisher Reports werden in der Tabelle xdo_lobs gespeichert. Diese Tabelle kann regelmäßig unter Verwendung von expdp gesichert werden.

Wir packen alle drei Exporte in ein Shell-Skript, das alte Daten nach vier Wochen bereinigt und so ein Sicherheitsnetz für Entwickler bietet, die ihren Quellcode nicht sofort in das GIT-Repository einchecken. Das bedeutet ein RPO von 4 Stunden (nur für den Quellcode) und ein RTO von 2 bis 12 Stunden (Erstellung einer neuen P2T-Kopie und Wiederherstellung des aktuellsten Quellcodes). Die Kosten sind minimal – ca. 1 GB werden im File Storage gespeichert.

CRP- und Testinstanzen

CRP- oder Test-Instanzen können vor allem bei der Umsetzung eines neuen Oracle-E-Business-Suite-Implementierungsprojekts eine entscheidende Rolle spielen. Oftmals ist es gar nicht so einfach, diese durch neue Kopien der Produktion zu ersetzen, besonders während der heißen Phasen, beispielsweise im Rahmen eines Benutzerakzeptanztests.

Ich habe gute Erfahrungen mit Block-Volume-Backups gemacht, die entweder manuell oder zu festen Zeiten (teils inkrementell) unter Verwendung benutzerdefinierter oder vorgefertigter Backup-Richtlinien erstellt wurden. Solche Backups können leicht vom Apps- und DB-Block-Volume sowie vom Boot-Volume erstellt werden *(vgl. [6])*. Die Backups sind „konsistente Momentaufnahmen" der zugrunde liegenden Volumes zum Zeitpunkt ihrer Erstellung. Es ist einfach, aus den Backups wieder Boot- und Daten-Volumes zu erstellen und dann eine neue Datenbank- und Apps-Tier-VM-Instanz basierend auf diesem Backup zu starten. Dies kann innerhalb weniger Minuten geschehen.

In der Regel füge ich eine Richtlinie wie folgt an:

- Durchführung eines vollständigen Backups jeden Sonntagmorgen um 2 Uhr, das 2 Wochen behalten wird.
- Durchführung eines täglichen inkrementellen Backups um 4 Uhr, das 5 Tage behalten wird.

Das bedeutet ein RPO von bis zu einem Tag und ein RTO von ca. 30 Minuten. Die Kosten hängen von der Größe der Instanz ab, bei einer mittelgroßen Instanz liegen sie im Bereich von ca. 25 bis 50 Euro pro Monat.

Produktivumgebung

In der Produktion ist es oft nicht tragbar, im Katastrophenfall einen ganzen Arbeitstag zu verlieren. Die klassische Art, dies zu bewältigen, basiert auf der Verwendung regelmäßiger RMAN-Gesamt-/Inkrement-Backups in Kombination mit einem Backup der aktuellen Archive Logs. Damit lässt sich ein RPO von ca. 30 Minuten recht einfach erreichen. Der Nachteil dieser Methode ist die RTO: Wenn die Datenbank sehr groß ist, wird das letzte komplette Backup wiederhergestellt, gefolgt von einem inkrementellen Backup, woraufhin anschließend alle aktuellen Archive Logs hinzugezogen werden. Bei Instanzen mit vielen Terabyte an Daten kann der Restore-und-Recovery-Vorgang durchaus einen ganzen Tag in Anspruch nehmen.

Es gibt jedoch einen bequemen „Turbomodus" für diesen Ansatz: Beginnend mit dem Oracle-Datenbank-Release 12c kann die Wiederherstellung auf der Basis von „3rd Party Storage Snapshots" durchgeführt werden. Dies ermöglicht die Kombination eines Snapshot-Ansatzes – wie im vorigen Abschnitt gezeigt – mit der Anwendung der Archive Logs nur vom aktuellen Tag an.

Die wichtigsten Schritte, um dies einzurichten, sind:

- Einrichten eines File Storage in einer anderen Verfügbarkeitsdomain und Einhängen in die Datenbank-Tier.
- Einrichten dieses Einhängepunkts als zweites/optionales Ziel der Archive Logs.
- Sicherstellen, dass mindestens alle 30 Minuten ein Archive Log unter Verwendung des Parameters archive_lag_target erstellt wird.
- Optional: Definieren des obigen Einhängepunkts als sekundären Kontrolldatei-Speicherort.

Dieser Ansatz ergibt ein RPO von 30 Minuten mit einem RTO von 30 bis 90 Mi-

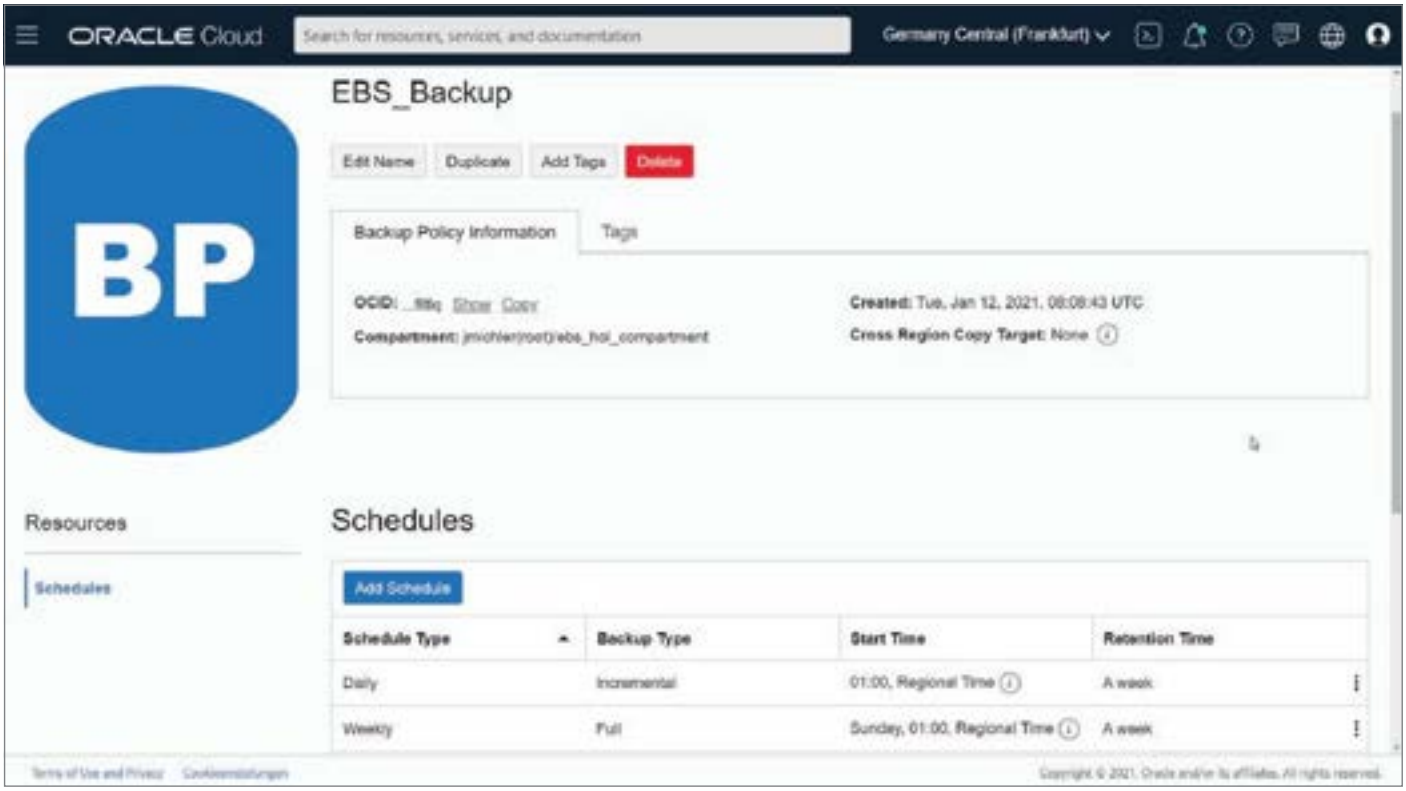

Abbildung 1: Definition einer BLOCK Storage Backup Policy (Quelle: PROMATIS)

nuten (abhängig von der Menge der zu „apply-enden“ Archive Logs). Die Kosten entsprechen den zuvor beschriebenen 1-Tages-Speicher-Snapshot-Kosten zuzüglich des File Storage für die Archive Logs von einem Tag.

Hybrider Ansatz

Dem einen oder anderen Datenbankadministrator ist das beschriebene Verfahren eines Recovery auf Basis von „3rd Party Storage Snapshots“ zu „modern“ und noch zu wenig etabliert. So ist auch eine Kombination von klassischen RMAN-Sicherungen mit Storage-Snapshots möglich. Einer unserer Kunden hat mit folgender Vorgehensweise gute Erfahrungen erzielt:

- Nächtlich um 1 Uhr erfolgt ein Snapshot der Datenbank (Software und Datenfiles); jeweils sonntags „voll“ (5 TB) und ansonsten inkrementell (20-50 GB).
- Täglich um 21 Uhr erfolgt ein RMAN-Backup auf OCI Object Storage; samstags als „Level 0“-Voll-Backup (ca. 3 Stunden; 600GB) und ansonsten inkrementell (10 Minuten; 10-30 GB).
- Stündlich erfolgt ein Backup der Archive-Logs auf OCI Object Storage (wenige Sekunden).

Im Falle eines Desasters wird dann zunächst der neueste Storage-Snapshot in seinen alten Zustand gebracht und auf diesem (bereits komplett konfigurierten) das neueste Control-File-Autobackup aus dem OCI Object Storage wiederhergestellt. Dann kann mit folgendem Befehl ein Recovery und anschließendes „alter database open resetlogs“ erfolgen (wobei RMAN automatisch gegebenenfalls hilfreiche inkrementelle Backups anwendet und dann Archive-Logs wiederherstellt und anwendet):

```
recover database UNTIL SCN
6232192258870 SNAPSHOT TIME "TO_
DATE('20.01.2021 01:00:52','DD.
MM.YYYY HH24:MI:SS')";
```

Sollte das Recovery basierend auf dem Snapshot aus irgendeinem Grund scheitern, so steht auch ein RMAN Full/Incremental Backup zur Verfügung, das dann (mit deutlich erhöhter Laufzeit) repariert werden kann.

Das Verfahren kombiniert daher die niedrigen Kosten bei geringer RTO mit bewährten RMAN-Backups.

Apps-Tier für die Produktion

Bisher haben wir hauptsächlich die Datenbank-Ebene einer Oracle-E-Business-Suite-Instanz abgedeckt. Für die Apps-Tier könnte – neben den oben beschriebenen, in der Regel nächtlichen, Snapshots – einer der folgenden Ansätze verwendet werden:

- Platzieren des $INST_TOP auf eine NFS-Freigabe auf dem File Storage oder
- Implementierung eines rsync-Backups von $INST_TOP auf einem Block-Volume zu einem entfernten Dateispeicherort oder
- Sicherstellen, dass sich keine wichtigen Daten auf dem Apps-Tier befinden: Häufig sind diese Daten nur temporär und müssen nicht mehr als einmal täglich gesichert werden.

Fazit

Wie oben gezeigt, bietet die Oracle-Cloud-Infrastruktur sehr leistungsstarke, benutzerfreundliche und dazu kostengünstige Möglichkeiten, alle Backup- und Wiederherstellungsanforderungen für Oracle-E-Business-Suite-Instanzen abzudecken.

Kurze RPO- und RTO-Zeiten können viel einfacher erreicht werden als mit herkömmlichen On-Premises-Rechenzentren.

Referenzen

[1] Oracle High Availability Overview and Best Practices *https://docs.oracle.com/en/database/oracle/oracle-database/19/haovw/index.html*

[2] Oracle Cloud Infrastructure Documentation, Overview of Block Volume *https://docs.oracle.com/en-us/iaas/Content/Block/Concepts/overview.htm*

[3] Oracle Cloud Infrastructure Documentation, Overview of Object Storage *https://docs.oracle.com/en-us/iaas/Content/Object/Concepts/objectstorageoverview.htm*

[4] Oracle Cloud Infrastructure Documentation, Overview of File Storage *https://docs.oracle.com/en-us/iaas/Content/File/Concepts/filestorageoverview.htm*

[5] Oracle User’s Guide, 1 Working with Oracle SQLcl *https://docs.oracle.com/en/database/oracle/sql-developer-command-line/19.4/sqcug/working-sqlcl.html#GUID-1343FA2B-BDB4-4645-B4D4-CD7C3E200AC9*

[6] Oracle Cloud Infrastructure Documentation, Overview of Block Volume Backups *https://docs.oracle.com/en-us/iaas/Content/Block/Concepts/blockvolumebackups.htm*

Über den Autor

Johannes Michler ist als Senior Principal Consultant, Systemarchitekt und Projektleiter für die PROMATIS Gruppe mit Fokus auf serviceorientierte Architekturen (SOA), Web-Portale sowie BPMN- und BPEL-basierte Prozessautomatisierung tätig. Seit 2014 bekleidet er die Funktion „Senior Vice President – Head of Platforms & Development“; bei der Horus software GmbH ist er Mitglied im Management Board. Seit 2010 ist er für die DOAG als Referent und Autor mit zahlreichen wissenschaftlichen und anwendungsnahen Beiträgen aktiv. Daneben nimmt er regelmäßig als Referent zahlreiche Veranstaltungen der Oracle Community (IOUG & OATUG) wahr.

Johannes Michler
johannes.michler@promatis.de