Überblick Sicherheit & Oracle Database Cloud

André Lutermann

DOAG Competence Center Security

Überlegungen vor einem Cloud Deployment

- Wo macht Oracle Database Cloud Sinn, wo nicht?
- Welche Daten in die Cloud?
- Welche Sicherheitsvorkehrungen sind durch Oracle getroffen oder muss ich noch treffen?
- Was passiert bei Ausfall? Besteht eine Exit Strategie?

Oracle Database Cloud Angebot

Database as a Service

- Dedizierte Virtual Machine zur Ausführung einer Oracle Database-Instanz – Wählen Sie Oracle Database 11g oder 12c
- Vorinstallierte Datenbanksoftware – Erstellen Sie mithilfe eines Assistenten eine Datenbank mit vordefinierten Konfigurationsoptionen
- Ihre Daten in den Tablespaces sind standardmäßig verschlüsselt
- Vollständiger Oracle Net-(SQL*Net-)Zugriff
- Vollständiger Root-Zugriff mit Administratorrechten auf BS und SYSDBA für eine Selbstverwaltung der Datenbank
- Neue Cloud-Tools für ein vereinfachtes Management, einschließlich automatisierten Backups mit Point-in-Time Recovery sowie Patching und Upgrades per Mausklick
- Beinhaltet Oracle Application Express (APEX), Version 5.0, ein hoch produktives, browserbasiertes Anwendungsentwicklungs-Framework zum Erstellen dynamischer Anwendungen mit SQL und PL/SQL

Exadata Service

- Ermöglicht Oracle-Datenbanken (11.2.0.4 oder 12.1.0.2) mit vollem Funktionsumfang unter Exadata – alle Datenbankoptionen, Enterprise Manager Packs und Exadata-Performanceoptimierungen erhältlich
- Vollständige Kompatibilität mit Oracle-Datenbanken on-Premise
- Ihre Daten in den Tablespaces sind standardmäßig verschlüsselt
- Wählen Sie Quarter Rack, Half Rack oder Full Rack, und skalieren Sie dann elastisch
- Vollständiger Root-Zugriff mit Administratorrechten auf BS und SYSDBA für eine Selbstverwaltung der Datenbank
- Unterstützt OLTP-Datenbanken, analytische Datenbanken und Datenbanken mit gemischter Workload in allen Skalierungen
- Ermöglicht Konsolidierung, Test/Entwicklung, Proof of Concept, Zertifizierung usw.
- Gesicherter Netzwerkzugriff, Kundendatenbanken werden in separater VM ausgeführt
- Backup und Recovery in Exadata oder Oracle Database Backup Service
- Server, Speicher und Netzwerkinfrastruktur von Oracle verwaltet

Database Schema Service

- 1 Schema unter Oracle Database 11g
- Auswahl zwischen 5, 20 und 50 GB Datenbankspeicher (1 GB für Testaccount)
- Beinhaltet Oracle Application Express (APEX), Version 5, ein hoch produktives, browserbasiertes Anwendungsentwicklungs-Framework zum Erstellen dynamischer Anwendungen mit SQL und PL/SQL.
- Datenzugriff über RESTful Web Services
- Ihre Daten in den Tablespaces sind standardmäßig verschlüsselt
- Kein Oracle Net-(SQL*Net-)Zugriff
- Vollständig von Oracle verwaltet – kein DBA erforderlich

KÜNFTIGE AUSRICHTUNG

Database as a Service – Managed

- Systembetreuung und -administration durch Oracle
- Vollständiger Zugriff auf dedizierte Oracle Database-Instanz
- Ihre Daten in den Tablespaces sind standardmäßig verschlüsselt
- Vollständiger Oracle Net-(SQL*Net-)Zugriff
- Von Oracle verwaltetes Backup mit Point-in-Time Recovery
- Von Oracle verwaltetes Patching und Upgrading

Quelle: Oracle

Inhalte & Funktionen

Database

Datenbankversionen

Dedizierte Datenbankinstanzen mit Oracle Database 11g oder 12c mit der Wahl zwischen Standard Edition One, Enterprise Edition (keine Datenbankoptionen enthalten), Enterprise Edition High Performance (enthält die meisten Datenbankoptionen) oder Enterprise Edition Extreme Performance (enthält alle Datenbankoptionen)

Clouddatenbank

Oracle Database 12c beinhaltet die Oracle Multitenant-Option für das Verwalten von integrierbaren Datenbanken in der Cloud

Datenzugriff

Administrativer Zugriff

Administrativer Zugriff über SSH, SQL Developer, Data Pump, SQL*Plus und andere Tools

Standard-Netzwerkzugriff

Sie können jede Art von Netzwerkkonnektivität wie Oracle Net (SQL*Net), JDBC, JSON und andere Treiber für den Zugriff auf Ihre dedizierten Instanzen nutzen

Tools

Verwenden Sie Enterprise Manager, SQL Developer, Application Express oder ein anderes Tool von Oracle oder von einem Drittanbieter

Management

Verwaltungsoptionen

Übernehmen Sie die vollständige Verwaltung Ihrer Datenbank, oder überlassen Sie Oracle die Administration und Betreuung von Standardoperationen, wie Backup, Patching und Upgrade (künftige Ausrichtung)

Sicherheit

Nutzen Sie die Sicherheitsregeln und -listen im Computing-Service für eine flexible Unternehmenssicherheit

Elastisch

Elastische Ressourcen

Je nach Bedarf können Sie Computing-Ressourcen, Arbeits- und Datenspeicher hinzufügen oder entfernen

Lifecycle Management

Flexible Steuerung von Datenbanken für Production-Umgebungen sowie einfache Speicherverwaltung auf Virtual Machine-Instanzen

Quelle: Oracle

Oracle Database Cloud Service – Ausprägungen

Database as a Service
Vollwertiger Datenbank-Instanz Service mit VM Zugriff

Database Cloud Service Virtual Image
VM + DB + Disk Image

- Ähnlich Azure Image oder AMI
- Vollst. DB-Installation auf virt. Platte
- Verhält sich wie "on premise"

Database Cloud Service
VM + DB + "Cloud Tooling"

- Backup/Recovery Automatisierung
- Patching und Upgrade Automatisierung
- Data Guard setup
- Monitoring & management portals
- Local management console

- Oracle Linux 6.4
- On-demand storage & compute
- Wahlweise: SE1, EE sowie Database 12c 12.1.0.2, und 11g 11.2.0.4
- Bundles: EE High Performance (fast alle Optionen), EE Extreme Perf (Alle Optionen)
- Vollständige Netzwerk, VM und OS Isolation, Voller SQL*Net Zugriff
- "Self-managed" mit SSH Zugriff in die VM inkl. root Privileg

Database Schema Service
Shared Schema Service

Database Schema
Shared Database

- "Fully managed"
- Eigenes DB Schema
- Größen: 5GB, 20GB, 50GB
- Datenzugriff mittels: Java Service, Oracle Application Express, Oracle RESTful Web Services

Quelle: Oracle

Oracle Database Cloud - Voraussetzungen

- Account mit Zugriff auf Database Cloud Service ist vorhanden und aktiviert
  - als „Metered Service“ („nach Verbrauch“)
  - als „Non-Metered Service („Monatsflat“)
  - als 30 Tage Trial

- Benötigte Werkzeuge
  - Browser mit Internetzugriff
  - Putty (oder OpenSSH) und Putty Key Generator (PuttyGen)
  - Administrationswerkzeuge (Oracle SQL Developer/TOAD...)

Quelle: Oracle

Oracle Database Cloud - Voraussetzungen

- Account mit Zugriff auf Database Cloud Service ist vorhanden und aktiviert
  - als „Metered Service“ („nach Verbrauch“)
  - als „Non-Metered Service („Monatsflat“)
  - als 30 Tage Trial

- Benötigte Werkzeuge
  - Browser mit Internetzugriff
  - Putty (oder OpenSSH) und Putty Key Generator (PuttyGen)
  - Administrationswerkzeuge (Oracle SQL Developer/TOAD...)

Quelle: Oracle

Erste Schritte nach Aktivierung

- Erzeugen eines SSH Schlüsselpaars
- Erzeugen einer neuen Database Cloud Service Instanz
- Erster Login via SSH
- Konfiguration über Administrationswerkzeuge wie SQL Developer oder Alternativen

SSH Schlüsselpaar erzeugen

- VM des Database Cloud Service ist NUR mit SSH Schlüsseln zugänglich
  - Kein Username/Passwort
- Grundsätzlich zwei Schlüssel-"Hälften":
  - „Private Key": geheim, sicher aufbewahren
  - „Public Key": wird in die Cloud VMs hochgeladen
- Hier verwendet: „Putty" unter Windows
  - Andere SSH Tools (z.B. MobaXTerm, OpenSSH auf der Kommandozeile) funktionieren ähnlich

Stichwort Cloud Outsourcing

- Cloud/Outsourcing Anbieter haben in der Regel vollständigen Zugriff auf die Daten
- Klare Trennung von Verantwortlichkeiten ist wichtig, aber technisch nicht immer einfach
- Kostenvorteile
- Datenbank oder Entwicklungsumgebung in wenigen Minuten

Das Business will die Vorteile des Outsourcings ohne die verbundenen Risiken

Welche Daten in die Cloud?

- Einfache Möglichkeiten mit anonymisierten Testdaten
- Personenbezogene Daten verursachen meist Kopfschmerzen
- (Steigerung der Anforderungen bei z.B. Gesundheindheitsdaten)

Welche Sicherheitsvorkehrungen sind durch Oracle getroffen oder muss ich noch treffen?

- 99.999% Verfügbarkeit von Strom und Kühlung
- Redundante Firewalls
- Redundante F5 load balancers with SSL acceleration
- DDOS Protection
- Verschlüsselungoptionen für alle Pakete (?)
- Key Management SSH

Rollen in der Cloudverwaltung

Service Administrator, who can create, modify and delete Database Cloud Service - users and their privileges, both in the Cloud Identity Manager and the Administration area of the
Database Cloud Service - Multitenant Edition development platform
Developers, who can use the development platform within a Database Cloud Service - to create applications, but who cannot create, modify or delete users for that Database Cloud
Service
End users, who can run applications within the Database Cloud Service – Multitenant Edition

Verschlüsselung

Verschlüsselung ist der Standard

- Alle Oracle Cloud Datenbanken sind standardmäßig verschlüsselt
  - Das gilt auch für die Standard Edition
- Neuer Datenbank Parameter
  - encrypt_new_tablespace (Default AES 128)
    - ALWAYS : Alle neuen Tablespaces werden verschlüsselt. On Premises und Cloud Datenbanken
    - CLOUD_ONLY: Nur Datenbanken als Datenbank Cloud Service werden Verschlüsselt
    - DDL: Verschlüsselung muss explizit angeben werden

Backups

Verschlüsselung ist der Standard

- Alle Oracle Cloud Datenbanken sind standardmäßig verschlüsselt
  - Das gilt auch für die Standard Edition
- Neuer Datenbank Parameter
  - encrypt_new_tablespace (Default AES 128)
    - ALWAYS : Alle neuen Tablespaces werden verschlüsselt. On Premises und Cloud Datenbanken
    - CLOUD_ONLY: Nur Datenbanken als Datenbank Cloud Service werden Verschlüsselt
    - DDL: Verschlüsselung muss explizit angeben werden
- Backups in die Oracle Storage Cloud sind standardmäßig verschlüsselt
  - Das gilt auch für die Standard Edition
- Backups auf lokalem Storage sind nur in der Enterprise Edition verschlüsselt

In der Cloud macht Database Vault Sinn

Aktivieren von Database Vault

- Ab der Database Cloud Service High Performance Enterprise Edition
  - Anlegen der Database Vault Benutzer
    - Database Vault Administrator
    - Database Account Manager
- Konfiguration der Datenbank
- Aktivierung von Database Vault durch den Database Vault Administrator

Informationen zum Datenschutz

Eine Checkliste für den DBA

Der DBA trägt auf Grund seiner Tätigkeit eine besondere Verantwortung für den Datenschutz und die Datensicherheit. Oft scheint er sich zwar deren Verantwortung bewusst, kann sie aber häufig nicht richtig einschätzen.
Diese Checkliste mit typischen Fallbeispielen soll Ihnen als DBA dabei helfen, ein besseres Gefühl für den „Datenschutz" zu entwickeln, damit Sie nicht selbst zum Ziel der Datenschutzfahndung werden!

http://www.doag.org/formes/servlet/DocNavi?action=getFile&did=7014947&key=

Was passiert bei Ausfall? Besteht eine Exit Strategie?

- Ausfall bedeutet hauptsächlich Cloudkosten- Erstattung (event. weit entfernt von tatsächlichen Kosten)
- Oracle behält sich Sperrung bei Sicherheitsanomalien vor (unscharfe Bedeutung?)

- Oracle stellt Daten 60 Tage nach Beendigung des Clouddienstes zum „sicheren“ Download zu Verfügung (SFTP)