Oracle Data Platform Foundations Associate

3. Exadata and Base Database Service

Chapter 3.4: Cloud Management Responsibilities

Exadata Database Service

Cloud Management Responsibilities

Presented by: Eddie Ambler
Senior Technical Product Manager, Oracle

Exadata Database Service: Management Responsibilities

Simple Cloud Management Model

The Exadata Database Service operates on a shared responsibility model. The following outlines the division of management tasks between the customer and Oracle.

- **Data/Schema**
    - Customer manages: Data, schema, encryption keys.
- **Database**
    - Customer subscribes to database services.
    - Customer manages everything above the Hypervisor using Cloud Automation (UI / APIs).
- **Customer VM**
    - Cloud Automation is provided to create, delete, patch, backup, scale up/down, and more.
    - Runs all supported Oracle Database versions.
- **Hypervisor**
    - Customer can install and manage additional software in the customer VM.
    - Customer controls who has access to the customer VM.
    - **Oracle staff is not authorized to access the customer VM.**
- **Internal Fabric**
- **Oracle owns and manages the infrastructure**
    - This includes Database Servers, Storage Servers, Internal Networking, and the Hypervisor.
    - Oracle performs Infrastructure Patching, Security scans, and Security updates.
    - Customers can schedule maintenance windows for Infrastructure Maintenance.

- **Customers are not authorized to access the Oracle infrastructure.**

Automated Database Lifecycle Operations Under Customer Control

The service provides full automation for key database operations, which remain under customer control:

- **Provisioning**
- **Resource Scaling**
- **Patching & Upgrades**
- **Automated Backup & Recovery**
- **Built-in Security**
- **Disaster Recovery with Oracle Data Guard**

Exadata in Oracle Cloud Architecture

Exadata Components in the Cloud

- Database and storage servers connected by a secure internal fabric.
- Horizontally scalable database and storage layers.

Secure Isolation

- Databases run in secure virtual machines that are isolated from the underlying infrastructure.

Networking Connectivity

- Separate Client & Backup Subnets for network segmentation.
- Utilizes Virtual Cloud Network (VCN) and VLANs.

Cloud Management

- **Infrastructure** is managed by **Oracle**.
- **Database VM Content** is managed by the **Customer**.

Control Plane

- Enables customer management of the Exadata Database VM contents.

Architecture Diagram

Customer VCN/VLAN	
Client Subnet	**Backup Subnet**
Database Servers	Database VMs
	Database VMs
	Grid Infrastructure
	Databases

Customer VCN/VLAN		
		Cloud Automation
Secure RoCE Network Fabric		
Storage Servers		NodeFlex
		NodeFlex
		NodeFlex
Customer Admin	**Cloud Control Plane**	
	Oracle Cloud Ops	

Hybrid Cloud: Public Cloud Simplicity and Elasticity Behind Your Firewall

Exadata Cloud@Customer is the cloud solution for when it is not possible to move to the public cloud.

Key Scenarios for Cloud@Customer:

- **Restrictions**
    - Regulations or corporate policies require data to be kept on-premises.
- **Response Time**
    - Real-world systems have complex relationships requiring low-latency communication.
    - It is difficult to disentangle one system from others.
- **Perceived Risk**
    - There are concerns about a multitenant public cloud environment.

Exadata Cloud@Customer addresses all these concerns.

Exadata Database Service Cloud@Customer Architecture

Access Method: Invoke Cloud UI or REST APIs.

Deployment Location:

- **ExaDB-C@C** instance located on the customer **Intranet**.
- Database access is provided to application servers within the **Customer Data Center**.

Division of Responsibilities:

- **Customer Actions:**
    - Database and Grid Infrastructure lifecycle operations.
    - VM lifecycle management.
    - Infrastructure lifecycle calls (via cloud control plane).
    - Scaling resources up and down.

        - Troubleshooting and incident management.
- **Oracle Actions:**
    - Infrastructure monitoring.
    - Infrastructure maintenance.

Security and Operations:

- **Customer Tenancy** includes an **Admin VCN** with:
    - Oracle Auditing and Access Controls.
    - FIPS 140-2 compliant Multi-Factor Authentication (MFA).
    - Access for **Oracle Cloud Ops** personnel.
- The entire system is managed through **Oracle Cloud Infrastructure (OCI)**.

Chapter 3.5: Billing and Licensing

Exadata Database Service: Billing & Licensing

Presented by: Eddie Ambler
Senior Technical Product Manager, Oracle

Cost-Effective Software Licensing Models

Subscribe to infrastructure and choose a licensing model.

License Included Pricing
Ideal for organizations with new workloads and dynamic utilization.

- **Includes Oracle Database Enterprise Edition, Options, and Management Packs** at one low price.
- Pay-per-use pricing for software and active OCPUs, all paid for with Universal Credits.

Bring Your Own License (BYOL) Pricing
Ideal for organizations moving existing workloads with consistent usage to the cloud.

- Utilize **existing on-premises licenses** and save on existing software support.
- **Includes** Transparent Data Encryption, Data Safe, Oracle Machine Learning, and select management packs at **no additional cost**.

Elastic OCPU Scaling - Pay Only for What You Use

On-Premises – Static

- Purchase server processors and software licenses for the highest projected peak load.

Cloud – Elastic

- Adjust enabled OCPUs to match actual load via APIs and web UI.
- OCPUs are charged per second.

Integrated Security from Data to Identity: Defense in Depth

Data

- Transparent Data Encryption (TDE)
- Data Reduction
- Data Masking
- Data Subsetting
- OCI Vault
- Oracle Database Vault
- Oracle Database Firewall
- Data Safe
- NIST SP-800-88r1 erase

Compute

- STIG Hardened
- Minimal Base: Token-based SSH access

Networking

- Network Isolation
- Oracle Native Network Encryption
- Dedicated Client and Backup networks
- FastConnect

Infrastructure

- Operator Access Control (OpCtl)
- Vulnerability Scanning
- FIPS 140-2
- HIPAA
- FedRAMP
- ISO 27001
- SOC 1/2/3

OCI Tenancy

- Identity and Access Management (IAM)
- Federated Identity providers
- Multi-Factor authentication (MFA)
- IP-based access control
- Users, groups
- Compartments
- Instance Principals
- Resource Principals

Operator Access Control (OpCtl)

Prevent, Detect, and Respond

OpCtl enables customers to grant, audit, and revoke access to Exadata Cloud@Customer infrastructure managed by Oracle.

Customers control access to infrastructure by Oracle operators by limiting:

- Components they can access
- When they have access
- Commands they can execute

Customers can observe and record Oracle operator commands and keystrokes.
Can terminate Oracle operator connection & process.

Customer Security for Regulated Industries

- **Oracle:** Requests Access
- **Customer:** Approves, Logs, Terminates Access

Chapter 3.6: Exadata Database Lifecycle Management - Administering Exadata

Exadata Database Service: Database Lifecycle Management

Presented by: Eddie Ambler
Senior Technical Product Manager, Oracle

Objectives

After completing this lesson, you should be able to:

- Create Custom Database & Grid Infrastructure Software Images
- Create Database Home

- Create Database
- Perform PDB Management
- Enable Data Guard
- Perform User-Managed Maintenance Updates

Create Custom Software Image

[This section was primarily visual. The concept is to create a customized database software image for patching.]

Create Database Home

UI Screenshot Description: "Create database home" dialog box

- **Database Home display name:** Field for a custom name (e.g., `MyOwn19CDBHome01`).
- **Database Image:** Dropdown to select the version (e.g., "Oracle Database 19c").
- Text note: "A 19c based database home can only be purchased on a VM cluster running Grid Infrastructure 19c and later."
- **Create button:** To proceed.

Create Database

[This section was primarily visual. The process involves using the UI to create a new database.]

Oracle Key Vault Integration for Exadata Cloud@Customer

- You can integrate your on-premises Oracle Key Vault (OKV) with Exadata Cloud@Customer to secure your critical data on-premises.
- Oracle Key Vault integration enables you to take complete control of your encryption keys and store them securely on an external, centralized key management device.
- OKV is optimized for Oracle wallets, Java keystores, and Oracle Advanced Security Transparent Data Encryption (TDE) master keys.
- OKV also provides a REST interface for clients to auto-enroll endpoints and setup wallets and keys.

Diagram Description: Oracle Key Vault Integration

- Shows an **Oracle Key Vault Cluster** centralizing keys for:
    - **Oracle Wallets**
    - **Java Key Store**

- **Oracle Database / RAC** (TDE Master Encryption Keys)
- **OS / Volume Encryption Keys**

Pluggable Database Lifecycle Management

- Create additional PDBs within the same container database (CDB).

UI Screenshot Description: "Pluggable Databases" list view

- Shows a table with columns: **Name**, **State**, **Refreshable clone**, **Created**.
- Example entry: `MYPDB01`, State: `Available`, Refreshable clone: `No`, Created: `Mon, May 20, 2024, 17:54:22 UTC`.
- A second PDB named `MyPDB02` is shown as being added to the list.

From the Pluggable Database Details page you can perform the following:

- **Connect** to individual PDBs using either Easy Connect or Long Connect strings.
- **Open Performance Hub.**
- **Clone PDB.**

UI Screenshot Description: PDB Details Page

- Shows an overview for `MYPDB01`.
- Buttons for **PDB connection** and **Performance Hub**.
- **Lifecycle state** is `Available`.
- **Container Name:** `MYPDB01`.
- **Created** date.
- **Refreshable clone:** `No`.
- **Open Mode:** `Read Write`.

From the "More Actions" Menu you can perform the following:

- **Start** and **Stop** a PDB.
- **Relocate** and **Restore** a PDB.
- **Delete** a PDB.

Role Transitions: Switchover and Failover

Oracle Data Guard supports two role-transition operations:

- **Switchover**
    - Planned role reversal.
    - Reduces downtime for OS/hardware maintenance/upgrade & database patching.

- **Failover**
    - Unplanned role reversal.
    - Emergency use.
    - Invoked from Standby that will become the new Primary database.
    - Can enable automatic failover by manually configuring *fast-start failover*.

Data Guard Requirements

- Both DB Systems must be in the same compartment.
- If your primary and standby databases are in the same region, then both must use the same virtual cloud network (VCN).
- If your primary and standby databases are in different regions, then you must peer the virtual cloud networks (VCNs) for each database.
- The database versions must be the same.
- Each database in a Data Guard association must have a unique `DB_UNIQUE_NAME` value; the primary and standby database can use the same `DB_NAME` value.
- Configure the security list ingress and egress rules for the subnets of both DB systems in the Oracle Data Guard association to enable TCP traffic to move between the applicable ports; ensure that the rules you create are stateful (the default).
- The minimum requirement for Oracle Data Guard to work is to enable egress for TCP traffic only for the SCAN listener port, which has a default of 1521.

Chapter 3.7: User-Managed Maintenance Tasks (Part 1)

Exadata Database Service: User-Managed Maintenance Tasks

Customer Responsibility

Managing Maintenance Updates

User-Managed Maintenance Updates

- Patch Database Home Software
- Patch Oracle Grid Infrastructure (GI)
- Update Operating System of the VM

Oracle-Managed Infrastructure Maintenance Updates

- Apply Quarterly Infrastructure Updates to:
    - Physical Compute and root VM on Database Server

    - Exadata Storage Servers
    - Internal Network Switches
    - Power Distribution Units (PDU)
    - ILOM Interfaces
    - All Firmware & BIOS

Diagram Description: Maintenance Responsibility Stack

- **Customer Responsibility (User-Managed):**
    - Database Server (DomU)
    - Exadata VM (DomU): Grid Infrastructure, Database Software
    - VM Operating System
- **Oracle Responsibility (Oracle-Managed):**
    - Secure Network Fabric
    - Storage Servers
    - Exadata Infrastructure (Physical Compute, etc.)

Prerequisites & Best Practices for Applying Updates & Patches

- Back up your databases before you apply any updates to the DB Home.
- Move the database to a new DB Home if possible instead of updating the DB Home.
- Update Grid Infrastructure before updating or creating a DB Home.
- Before you apply any update, run the precheck operation.
- Ensure all servers and database instances are up and running.
- Ensure `/u01` (GI Home directory) has 15GB of free space before a Grid Infrastructure update.
- Ensure `/u02` (DB Home directory) has 15GB free space before a DB Home update.
- Use the OCI Management Interfaces to perform the update & patching operations.

Finding Available Updates & Patches, & Viewing Update History

Customer Responsibility

View Update & Patch History

UI Screenshot Description: "Update History" table for a VM Cluster

- Table with columns: **Description**, **Date**, **Version**, **Component**, **Operation Type**, **Method**.

- Example entries show operations like "Patch Apply" and "Patch Precheck" for components like "Grid Infrastructure" and "Database Home", with their respective dates and version numbers.

Guest VM OS Image Updates

Customer Responsibility

- **Exadata Image** contains the virtual machine OS (Oracle Linux) updates.
- Provides **precheck** function to ensure virtual machine update readiness.
- Option to rollback in case any issues are encountered during the update process.
- Minor & Major version updates to OS image version can be done from the UI and REST APIs.
- To maintain secure systems, only the 4 latest Exadata Image minor version updates are available in the console.

UI Screenshot Description: "Apply Exadata OS Image Update" dialog

- Text: "Exadata OS image updates are applied to the VM cluster + virtual machines in a rolling manner. Databases remain available during the update operation."
- Prompt: "Do you want to update the OS image of VM cluster MyDemoVMCluster from version 22.1.10.0.0.2024 to be version 22.1.20.0.2.04.0001?"
- Checkbox: "Last successful precheck was run at Thu, May 25, 2024, 03:31:13 UTC."
- Buttons: `[Cancel]` and `[Update]`.

Patch Grid Infrastructure Software

Customer Responsibility

- Update GI using OCI Console or REST APIs.
- Choose desired Grid Infrastructure version.
- Run **Precheck for update** prior to maintenance window to validate system readiness.

GI Update is performed in a rolling fashion

- Database instances in the virtual machine undergoing a GI update will not be available.

Chapter 3.8: User-Managed Maintenance Tasks (Part 2)

Exadata Database Service: Patching Database Home Software

Customer Responsibility

Database Home Patching

- Customers can use **Oracle provided database software images** or **custom database software images** to update the Database Home Software.

To update a database home:

- **Option 1:** Update an existing Database Home to the desired patch level, which updates all of the databases using the Database Home.
- **Option 2:** Create a new Database Home with the desired patch level and move a database to the new Database Home.
- **Using the "Move to Another Home" function is the quickest way to patch a database.**
- Update Database Home using OCI Console or REST APIs.
- Choose desired Database Home patch version from Oracle Standard or Custom Database Software Images.
- Run **Precheck for update** prior to maintenance window to validate system readiness.

Updates are done in a rolling manner across RAC database instances in the VM Cluster

- Update all databases in an existing Database Home.
- You can update one database at a time by moving it to a new Database Home.

Database Home Patching with Custom Images

To update a database using a custom database software image there are 2 options:

Option 1: Create Database Home with custom database software image and move the databases individually to the new Database Home.

Option 2: Update Database Home by applying a custom database software image to it. This option causes all of the databases using the Database Home to be updated at the same time.

Grid Infrastructure & Database Home Patching Impact

- Zero database service downtime with RAC database rolling updates.
- Maximum database compute performance and throughput is temporarily reduced while restarting RAC database instance.
- To achieve zero application downtime, follow Exadata Cloud MAA best practices documentation for achieving continuous availability for applications.

Upgrade Grid Infrastructure Software

Customer Responsibility

Upgrading the GI:

- Allows you to provision Oracle DB Homes and Databases with the most current Oracle Database software.
- Involves upgrading the GI software on all the compute nodes in the VM Cluster.
- Is performed in a rolling fashion, with only one node being upgraded at a time.
    - Database instances in the VM undergoing grid infrastructure upgrade will not be available.
- You can monitor the progress of the GI upgrade operation by viewing the associated work requests.
- Oracle recommends running an **upgrade precheck** prior to the maintenance window.
- **Note:** The GI upgrade feature is not available if you have an Exadata infrastructure maintenance operation scheduled to start within 24 hours of the upgrade.

Also note that the following Data Guard operations are not allowed on the VM cluster undergoing a GI upgrade:

- You cannot Enable Data Guard.
- Conduct a Switchover.
- Failover to the database using the VM cluster undergoing maintenance.
- Management operations such as starting, stopping or rebooting nodes, scaling CPU, provisioning or managing database homes or databases, restoring a database, or editing IORM settings.

Upgrade Database

Customer Responsibility

Preparing for a Database Upgrade

- **Back up your database** and test the new software version on a test system before you upgrade your production database.
- **Run an upgrade precheck operation** before your upgrade maintenance window.
- **Create an Oracle Database Home** that contains the target database software version.
- You can use **Oracle-published software images or a custom database software image**.
- **Ensure all pluggable databases** in the container database being upgraded **can be opened**.
- Oracle recommends **disabling automatic backups** and **performing an on-demand full backup** before you start the upgrade operation.
- **Note:** After the database upgrade, **you cannot use automatic backups taken prior to the upgrade to restore the database to an earlier point in time.**

Understanding the Database Upgrade Process
During the database upgrade process, the following steps are automatically performed:

1. Conduct a **Precheck**.
2. Set a **Guaranteed Restore Point**, for use in the **Rollback process** in the event of an upgrade failure.
3. Move the database to a user-specified Oracle Database Home with the desired target software version.
4. Run the **Database Upgrade Assistant (DBUA)** software to perform the upgrade.

Upgrade a Database with a Data Guard Association

- If your database uses Data Guard, you can upgrade the primary or the standby first.
    - **Standby First Patching & Upgrades are recommended.**
- Upgrading a primary or standby will disable redo apply during the upgrade operation.
- Oracle recommends checking the redo apply and open mode configuration after upgrading.

Summary

In this lesson, you should have learned how to:

- Create Custom Database & Grid Infrastructure Software Images
- Create Database Home
- Create Database
- Perform PDB Management
- Enable Data Guard
- Perform User-Managed Maintenance Updates