MYTestCustomer
Oracle Database@Google
<Workload>

Solution Definition

Date | Version

Copyright

Table of Contents

DOCUMENT CONTROL **4**

2.1 VERSION CONTROL **4**
2.2 TEAM **4**
2.3 DOCUMENT PURPOSE **5**

BUSINESS CONTEXT **5**

3.1 EXECUTIVE SUMMARY **6**
3.2 WORKLOAD BUSINESS VALUE **7**

WORKLOAD REQUIREMENTS AND ARCHITECTURE **7**

4.1 OVERVIEW **7**
4.2 NON-FUNCTIONAL REQUIREMENTS **9**
4.2.1 REGULATIONS AND COMPLIANCES REQUIREMENTS 9
4.2.2 ENVIRONMENTS REQUIRED IN GOOGLE CLOUD 9
4.2.3 ORACLE DATABASE@GOOGLE CLOUD HIGH AVAILABILITY AND DISASTER RECOVERY REQUIREMENTS 10
4.2.4 PRE-MIGRATION CHECKS – CPAT (APPLICABLE TO ADB ONLY, ALSO FOR LOGICAL MIGRATIONS) 11
4.2.5 BACKUP AND RECOVERY 12
4.2.6 SECURITY REQUIREMENTS 14
4.2.7 GOOGLE CLOUD / OCI NETWORKING REQUIREMENTS 15
4.2.8 MANAGEMENT AND MONITORING 17
4.2.9 AUTOMATION & INTEGRATION (IAC) 19
4.3 CURRENT STATE ARCHITECTURE **20**
4.4 FUTURE STATE ARCHITECTURE **22**
4.4.1 SOLUTION BEST PRACTICES 22
4.4.2 LOGICAL ARCHITECTURE 25
4.4.3 PHYSICAL ARCHITECTURE 31
4.4.4 KEY SOLUTION PROPOSAL COMPONENTS 34
4.5 SOLUTION CONSIDERATIONS **36**
4.5.1 ORACLE DATABASE@GOOGLE CLOUD HIGH AVAILABILITY AND DISASTER RECOVERY 36
4.5.2 TRANSPARENT APPLICATION CONTINUITY 38
4.5.3 SECURITY 39
4.5.4 NETWORKING 40
4.5.5 RELIABILITY AND RESILIENCE / BACKUP AND RECOVERY 45
4.5.6 MONITORING 47
4.5.7 GOVERNANCE 47
4.5.8 MANAGEABILITY AND OBSERVABILITY 49
4.5.9 ORACLE DATABASE@GOOGLE CLOUD OPERATING MODEL 51
4.6 SIZING AND BILL OF MATERIALS **51**
4.6.1 BILL OF MATERIALS SCOPE 52
4.6.2 COLLECTED DATA FOR SIZING 52
4.6.3 DEFINED VM CLUSTERS FOR SIZING 54
4.6.4 SIZING ANALYSIS 54

Copyright @2024, Oracle and/or its affiliates

4.6.5 Sizing Assumptions 55
4.6.6 Proposed Hardware Shapes 56
4.6.7 Licensing models and Elastic Expansion of Exadata on Oracle Database@Google Cloud 56
4.6.8 Exadata Database@Google Cloud Bill of Materials 57
4.6.9 Base Database@Google Cloud Bill of Materials 57
4.6.10 Autonomous AI Database@Google Cloud Bill of Materials 57

Copyright @2024, Oracle and/or its affiliates

Guide:

Author Responsibility

- *Chapter 1-3: Sales Consultant*
- *Chapter 4: Implementer*

Document Control

Guide:

The first chapter of the document describes the metadata for the document. Such as versioning and team members.

2.1 Version Control

Guide:

A section describing the versions of this document and its changes. It is mandatory to describe the document version, the authors' and co-authors' names, the change date, and the changes as a comment.

Example:

Version	Authors	Date	Comments
0.1	DB@Google Team	1st June 2025	Published first version of SDD.
0.9	Himesh Bhatt	23rd June 2025	Updated template following review by CTO.
1.0	Kabad Ul Hasan	4th August 2025	Creating the first version of Database@Google SDD for. To be used for iterative review and improvement.
1.1	Maximilian Jerg	1st Sept 2025	Added Shared VPC chapter, minor fixes
1.2	Maximilian Jerg	20th Feb 2026	Added Multi-zone architecture within a region, minor fixes
1.3	Miguel Ferreira	7th Mar 2026	Added BaseDB@Google related information in the Word Template
1.4	Neeraj Pandita	24th Mar 2026	Updated the Word document to add section and exampleas specific to ADB
1.5	Kabad Ul Hasan	31st Mar 2026	Consolidated all the information for ExaDB/ExaXs, BaseDB, and ADB into single template and publised new MD
1.6	Kabad Ul Hasan	20th Apr 2026	Update information related to TAC/AC
1.7	Miguel Ferreira	5th Aug 2026	Incorporated the latest corrections and document updates. Replaced Figure 9 – Current State Architecture with an updated, higher-quality diagram for improved clarity. Masked all OCIDs to comply with security and confidentiality requirements

Copyright @2024, Oracle and/or its affiliates

2.2 Team

Guide:

A section describing the team with all its members, including professional services. It is mandatory to describe the team with: A name, a role, an email, and the company.

Example:

Name	Email	Role	Company
Himesh Bhatt	himesh.bhatt@oracle.com	DB@GCP Black Belt	Oracle
Neeraj Pandita	neeraj.pandita@oracle.com	DB@GCP Black Belt	Oracle
Miguel Ferreira	miguel.mf.ferreira@oracle.com	DB@GCP Black Belt	Oracle
Kabad Ul Hasan	kabad.ul.hasan@oracle.com	DB@GCP Black Belt	Oracle

2.3 Document Purpose

Guide:

Use the exact text you see in the example and ONLY replace the Service Provider.

Example:

This document provides a high-level solution definition for the Oracle solution and aims at describing the current state, and to-be state as well as a potential high-level project scope and timeline for <Service Provider>.

The document may refer to a 'Workload', which summarizes the full technical solution for a customer (You) during a single engagement. The Workload is described in the chapter Solution Requirements and Architecture.

This is a living document, additional sections will be added as the engagement progresses resulting in a final Document to be handed over to the <Service Provider>.

Business Context

Guide:

It is mandatory to describe the customer's business and background. This could include:

- *What is the context of the customer's industry and LoB?*
- *What are the business needs and goals that this solution is an enabler for?*
- *How does this technical solution impact and support the customer's business goals?*
- *Does this solution support a specific customer strategy, or maybe certain customer values?*
- *How does this solution help our customers to either generate more revenue or save costs?*

It is mandatory to describe a clear statement of a business value as part of the full solution scope. Try to keep it SMART: Specific, Measurable, Assignable, Realistic, and Time-Related - Agree on the business value with the customer. Keep it business-focused, and speak the language of the LoB: "Increase Customer Retention by 3% in the next year" or "Grow Customer Base with Executive Decision-Making from our Sales and Support Data". Avoid technical success criteria such as "Migrate App X to Oracle Cloud" or "Provision 5 Compute Instances" (Describe it in the Overview instead). Avoid Oracle success criteria and language "Get Solution Consuming on OCI".

Furthermore, it is mandatory to highlight Oracle's differentiators and key values of our solution for the customer, allowing the customer to make decisions quickly.

Copyright @2024, Oracle and/or its affiliates

Example

MYTestCustomer is a large airline operator, looking to modernize their application platform. Through this modernization, MYTestCustomer aims to improve the customer experience, enhance performance by 30%, cope with the larger forecasted transaction volume, and simplify future expansion into additional geographies.

3.1 Executive Summary

Guide:

A section describing the Oracle differentiator and key values of the solution for the customer, allowing the customer to make decisions quickly.

Example Generic

Over the past year, MYTestCustomer has embarked on a strategic transformation initiative to migrate it's IT assets to the public cloud, aligning the broader goals of agility, scalability and operational efficiency. As part of this initiative, Google cloud has been selected as the primary public cloud provider for MYTestCustomer

Key workloads within this transformation are the ERP and Business Intelligence (BI) ecosystem, which are currently hosted on an on-premises Oracle Exadata X7 infrastructure.

This environment supports two mission critical Oracle 19c Container Databases (CDBs)

- A highly transactional OLTP database that underpins the ERP system
- A data warehouse (DWH) database supporting a Business Intelligence solution. The database is optimised for analytics through features such as partitioning, parallel query execution, and Hybrid Columnar Compression (HCC)

To ensure continuity and performance parity in the cloud, MYTestCustomer has selected Oracle Database@Google Cloud as the foundation for migrating these databases. This solution enables MYTestCustomer to run Oracle database on Exadata infrastructure with a Google Cloud data center, delivering Exadata-level performance and advanced Oracle capabilities without the burden of hardware ownership or infrastructure management.

Oracle Database@Google Cloud offers a seamless Multicloud approach that preserves enterprise-grade database performance while advancing MYTestCustomer's Multicloud strategy.

This Multicloud deployment provides the following benefitis

- The elasticity and innovation of Oracle Database@Google Cloud
- Robust performance and advanced features of Oracle Exadata
- Simplified operations through managed services
- Reduced infrastructure overhead and TCO

Example BaseDB/ADB Specific

Over the past year, MYTestCustomer has embarked on a strategic transformation initiative to migration it's IT assets to the public cloud, aligning the broader goals of agility, scalability and operational efficiency. As part of this initiative, Google cloud has been selected as the primary public cloud provider for MYTestCustomer.

MYTestCustomer is migrating its order and dispatch application from GCP IaaS VMs to Oracle Base Database Service@Google Cloud (Base DB@GCP). The workload uses a single-instance Oracle Database 19c (~0.8 TB) and does not require Oracle RAC for clustering—zonal high availability is sufficient for business needs.

To ensure continuity and performance parity in the cloud, MYTestCustomer has selected Oracle Database@Google Cloud as the foundation for migrating these databases. This solution enables MYTestCustomer to run Oracle database on Base Database Service. Oracle Base Database Service provides a fully managed shared infrastructure for running single instance Oracle Databases using low-cost general-purpose infrastructure to provide VM compute and network attached storage. Suitable for running your choice of Database editions.

Copyright @2024, Oracle and/or its affiliates

3.2 Workload Business Value

Guide:

A clear statement of specific business value as part of the full workload scope. Try to keep it SMART: Specific, Measurable, Assignable, Realistic, and Time-Related - Agree on the business value with the customer. Keep it business-focused, and speak the language of the LoB which benefits from this Workload: "Increase Customer Retention by 3% in the next year" or "Grow Customer Base with Executive Decision-Making from our Sales and Support Data". Avoid technical success criteria such as "Migrate App X to Oracle Cloud" or "Provision 5 Compute Instances". Avoid Oracle success criteria and language "Get Workload Consuming on OCI".

Example Generic

Workloads in the scope are of vital importance for MYTestCustomer. Both the OLTP workload and the DWH workloads are needed for the company operation and any disruption in the applications would be costly and would badly affect customer satisfaction. Furthermore, a recent security assessment and a review of the Disaster Recovery plan has revealed that the current architecture must be improved in terms of security and resilience. For this reason, MYTestCustomer has decided to move these workloads to Google Cloud, and leverage the Oracle Database@Google Cloud Exadata solution. The main reasons for this migration to Oracle Database@Google Cloud are:

- Leverage the availability of Exadata database services in Google Cloud to achieve the best database performance (Google Cloud is preferred choice of MYTestCustomer for application's tier)
- Reduce the TCO leveraging the dynamic scaling capabilities of Database resources, and be able to scale dynamically without buying new hardware
- The possibility to transfer existing Oracle licenses to the cloud (BYOL)
- Avoid the cost of maintaining the underlining Exadata infrastructure and re-focusing the IT personnel on more business-oriented tasks
- Implement a Disaster Recovery strategy, leveraging the availability of Oracle Database@Google Cloud in multiple regions, and multiple availability zones within each region
- Generational performance improvements by going from Exadata X7 to Exadata X9M

Example BaseDB/ADB Specific

The workloads in scope are essential for MYTestCustomer's daily business. Migrating to Oracle Base Database Service@Google Cloud eliminates manual database maintenance and automates backups and patching, while simplifying security and compliance. Without the need of RAC, the company benefits from a cost-efficient, fully managed database service that's well-suited for single-instance workloads where basic resilience is acceptable.

Workload Requirements and Architecture

4.1 Overview

Guide:

Describe the Workload: What applications and environments are part of this Workload migration or new implementation project, and what are their names? The implementation will be scoped later and can be a subset of the Solution Definition and proposed overall solution. For example, a Workload could exist of two applications, but the implementer would only include one environment of one application. The workload chapter is about the whole Workload and the implementation scope will be described later in the chapter Solution Scope.

You can describe an existing solution in the optional chapter for a Current State Architecture , which is typically located after the Non functional requirements and before the Future State Architecture.

Example Generic

Currently, the database environment is deployed on a single Exadata system, while the application servers for both the ticketing application and BI application are deployed on a virtual machines within a VMWare estate. The batch processes that update the DWH database run as custom Python programs on number of Linux hosts, also hosted on the same VMWare estate.

Example BaseDB/ADB Specific

Workload consists of several Oracle Databases supporting core business applications, including customer management, billing, and reporting. Currently, these databases run on virtual machines hosted on-premises, with separate environments for production, test, and development. Application servers are deployed in Google Cloud using Google Compute Engine and managed Kubernetes clusters, while integrations and analytics are handled through Google Cloud services such as Pub/Sub and BigQuery.

This migration aims to modernize the database layer by adopting Oracle Base Database Service on Google Cloud, providing a managed and scalable database platform with full compatibility for existing Oracle workloads.

Below is the list of databases with their existing known versions, platforms, size, life cycle environment and virtual cluster.

Database Name	Database Version	Database Platform	Database Size	Env.	Cluster
OLTP	19.19	Exadata (Linux x86-64)	1.2 TB	Prod	clu-oltp-prod
DWH	19.19	Exadata (Linux x86-64)	7 TB	Prod	clu-dwh-prod
OLTP-TEST	19.19	Exadata (Linux x86-64)	700 GB	Non Prod	clu-oltp-nonprod
OLTP-DEV	19.19	Exadata (Linux x86-64)	500 GB	Non Prod	clu-oltp-nonprod
DWH-TEST	19.19	Exadata (Linux x86-64)	3 TB	Non Prod	clu-dwh-nonprod
DWH-DEV	19.19	Exadata (Linux x86-64)	1 TB	Non Prod	clu-dwh-nonprod

Example 2

Workload consists of several Oracle Databases supporting core business functions . These databases run on Virtual Machines on a 4-node VMware cluster backed by shared SAN storage. Databases are protected with managed backups and supported by SAN-level replication for DR . Applications are running on Google Compute engine and managed Kubernetes clusters.

Scoping Questions	DB1	DB3	DB4	DB5	DB6	DB7	DB8
DB Name	SLPROD01	SLPROD03	SLPROD04	SLPROD05	SLPROD06	SLPROD07	SLPROD08
DB Version [e.g 11.2.0.4 / 8.1.7.4]	19.28.0.0.0	19.28.0.0.0	19.28.0.0.0	19.28.0.0.0	19.28.0.0.0	19.28.0.0.0	19.28.0.0.0
Database Edition	Standard Edition	Standard Edition	Standard Edition	Standard Edition	Standard Edition	Standard Edition	Standard Edition
If 12c mention CDB or Non-CDB	19C (non-pluggable)	19C (non-pluggable)	19C (non-pluggable)	19C (non-pluggable)	19C (non-pluggable)	19C (non-pluggable)	19C (non-pluggable)
Env Type (Prod / Non-Prod) Acceptance, UAT, DEV, TEST are considered as Non-Production Env Type. Standby Databases - DO NOT INCLUDE, Standby DBs do not need migration, instead these are setup as part of post-migration activity.	PROD	PROD	PROD	PROD	PROD	PROD	PROD
DB Size (In GB)	3200	800	400	1400	1600	800	600
Criticality (5-: Highly Critical; 1-> Low Criticality) Highly critical DBs would imply that near-zero downtime migration is required	5	5	5	5	5	5	5
Downtime window [Select from drop-down list]	23:00 - 06:00	23:00 - 06:00	23:00 - 06:00	23:00 - 06:00	23:00 - 06:00	23:00 - 06:00	23:00 - 06:00
Source DB Characterset	AL32UTF8	AL32UTF8	AL32UTF8	AL32UTF8	AL32UTF8	AL32UTF8	AL32UTF8
Characterset Conversion to AL32UTF8 Required ? [Y/N]	N	N	N	N	N	N	N
RAC [Y/N]	N	N	N	N	N	N	N
DR [Y/N]	Y Backup based	Y Backup based	Y Backup based	Y Backup based	Y Backup based	Y Backup based	Y Backup based
Operating System with version & Release (e.g. Solaris SPARC, HPUX, AIX, Windows 32bit/64 bit etc)	Oracle linux	Oracle linux	Oracle linux	Oracle linux	Oracle linux	Oracle linux	Oracle linux
Target Database Edition & Version	ATP 19C	ATP 19C	ATP 19C	ATP 19C	ATP 19C	ATP 19C	ATP 19C
Target Platform & OS	GCP	GCP	GCP	GCP	GCP	GCP	GCP

Sizing Questionnaire

Copyright @2024, Oracle and/or its affiliates

4.2 Non-Functional Requirements

Guide:

Describe the high-level technical requirements for the solution. Consider all sub-chapters, but decide and choose which Non-Functional Requirements are necessary for your engagement. You might not need to capture all requirements for all sub-chapters.

This chapter is for describing customer-specific requirements (needs), not to explain Oracle solutions or capabilities.

4.2.1 Regulations and Compliances Requirements

Guide:

This section captures specific regulatory or compliance requirements for the solution. These may limit the types of technologies that can be used and may drive some architectural decisions.

The Oracle Cloud Infrastructure Compliance Documents service lets you view and download compliance documents: https://docs.oracle.com/en-us/iaas/Content/ComplianceDocuments/Concepts/compliancedocsoverview.htm

However, the Oracle Database@Google Cloud solution provides a part of OCI inside Google Cloud. Therefore, any compliance documents relevant to either Google Cloud or OCI do not automatically apply to Oracle Database@Google Cloud. It is vital that any requirements are captured so that they can be checked against assessments already done, or on the roadmap.

What needs to be captured are any requirements of the Oracle Database@Google Cloud elements, and anything running in OCI. Requirements for specific elements of the solution that will be running completely in Google Cloud (for example Google Cloud VMware Engine) do not have to be captured here.

If there are no requirements at this stage, then please state it. Leave the second sentence as a default in the document.

Example:

At the time of this document creation, no Regulatory and Compliance requirements have been specified.

In addition to these requirements, the latest version of the CIS Oracle Cloud Infrastructure Foundation Benchmark v1.2 will be applied to the Customer OCI tenancy.

4.2.2 Environments Required in Google Cloud

Guide: ExaDB

A diagram or list detailing all the required environments (e.g. development, text, live, production, etc.). Focus on the Oracle Database@Google Cloud/OCI elements, but also keep in consideration how they interact with the rest of the environments in Google Cloud.

As a minimum we should capture the Exadata hardware requirements of Oracle Database@Google Cloud in this section.

If you like to describe a current state, you can use or add the chapter 'Current State Architecture' before the 'Future State Architecture'.

Example:

Production and DR will each require a separate ¼ rack Exadata in different availability zones within the same Google Cloud region Germany West Central (linked to OCI region Frankfurt). Dev and Test are co-located on another ¼ rack Exadata.

The Production and DR Exadata infrastructures will host different VM clusters for each of the databases. The Dev/Test databases will share clusters between workload types.

Copyright @2024, Oracle and/or its affiliates

Name	Size	Location	DR	High Availability	RPO	RTO
Prod	Quarter rack X9M	Google Cloud Germany West Central	Yes	Yes	0	2 hrs
Dev + Test	Quarter rack X9M – 50% of Prod size	Google Cloud Germany West Central	No	Yes	24 hrs	24 hrs
DR	Quarter rack X9M – 100% of Prod size	Google Cloud Germany West Central	No	Yes	4 hrs	12 hrs

Example Autonomous DB:

Customer would like a cross region Autonomous data guard set up between London and Frankfurt for their Prod databases. Test databases have no DR requirement

Name	DB Size (in GB)	Location	DR	High Availability	RPO	RTO
PRODDB1	3200	Europe West 2	Yes(Cross region AuDG)	Yes	2 min	15 min
PRODDB2	3200	Europe West 2	Yes(Cross region AuDG)	Yes	2 min	15 min
TEST DB1	1600	Europe West 2	No	Yes	24 hours	24 hours

Guide BaseDB/ADB

As a minimum, this section should define the required database shapes, storage capacity, and availability setup for Base Database Service, as well as the region and zone configuration. Note the limitations for Base DB: scale up to 200 ECPUs and 40TB of storage

If describing both current and future states, you can include an additional chapter titled Current State Architecture before Future State Architecture.

Example:

Production and Disaster Recovery environments will each be deployed as separate Base Database Service instances in different availability zones within the same Google Cloud region (e.g., europe-west3 – Frankfurt). Development and Test environments will be deployed as smaller Base Database Service instances in the same region, using independent subnets.

The Production and DR databases will use different Base DB instances for isolation and high availability. Dev/Test databases will share smaller instances to optimize cost and resource utilization.

Name	Size	Location	DR	High Availability	RPO	RTO
Prod	16 ECPUs, 1TB Storage	Google Cloud Germany West Central	Yes	Yes	0	2 hrs
Dev + Test	8ECPUs, 500 GB Storage	Google Cloud Germany West Central	No	Yes	24 hrs	24 hrs
DR	16 ECPUs, 1TB Storage	Google Cloud Germany West Central	No	Yes	4 hrs	12 hrs

4.2.3 Oracle Database@Google Cloud High Availability and Disaster Recovery Requirements

Guide:

This section captures the resilience and recovery requirements for the solution. Note that these may be different from the current system.

The Recovery Point Objective (RPO) and Recovery Time Objective (RTO) requirement of each environment should be captured in the environments section above, and wherever possible.

- *What are the RTO and RPO requirements of the Application?*
- *What are the SLAs of the application?*

Copyright @2024, Oracle and/or its affiliates

- *What are the backup requirements*

Note that if needed, this section may also include an overview of the proposed backup and disaster recovery proposed architectures. Due to the Multicloud nature of the Oracle Database@Google Cloud solution, there can be considerable traffic between Google Cloud and OCI datacenters in Disaster Recovery scenarios, which can incur data transfer cost. For more information see chapter 'Oracle Database@Google Cloud High Availability and Disaster Recovery' under 'Solution Considerations'.

This chapter is mandatory, while there could be no requirements on HA/DR, please mention that in a short single sentence.

Example:

At the time of this document creation, no Resilience or Recovery requirements have been specified.

4.2.4 Pre-migration Checks – CPAT (Applicable to ADB only, also for logical migrations)

Guide:

This section captures the pre migration checks needs for ADB-S@Google Cloud.

Example:

Oracle Cloud Pre-migration Advisory Tool is a utility developed by Oracle to help customer to assess suitability of on-premise or cloud databases before migrating them to Oracle Autonomous Database. This tool highlights any potential recommendations, concerns, and blockers which may need to be resolved before migration. In some cases, the blocker may be a hard blocker resulting in non-suitability to migrate to Autonomous DB.

This tool can be downloaded from the support note https://support.oracle.com/epmos/faces/DocumentDisplay?_afrLoop=107972386933173&id=2758371.1&_afrWindowMode=0&_adf.ctrl-state=13n5cz0gy1_4 Run CPAT with following recommended parameters for JDBC thin service connection – ./premigration.sh --connectstring 'jdbc:oracle:thin:@:/' --username system --targetcloud ALL --migrationmethod ALL --reportformat HTML JSON --schemas --gatherdetails SCHEMA_OBJECTS --outfileprefix --zip

An example of summary and details in generated file for MYTestCustomer is as follows –

Premigration Advisor Report Summary

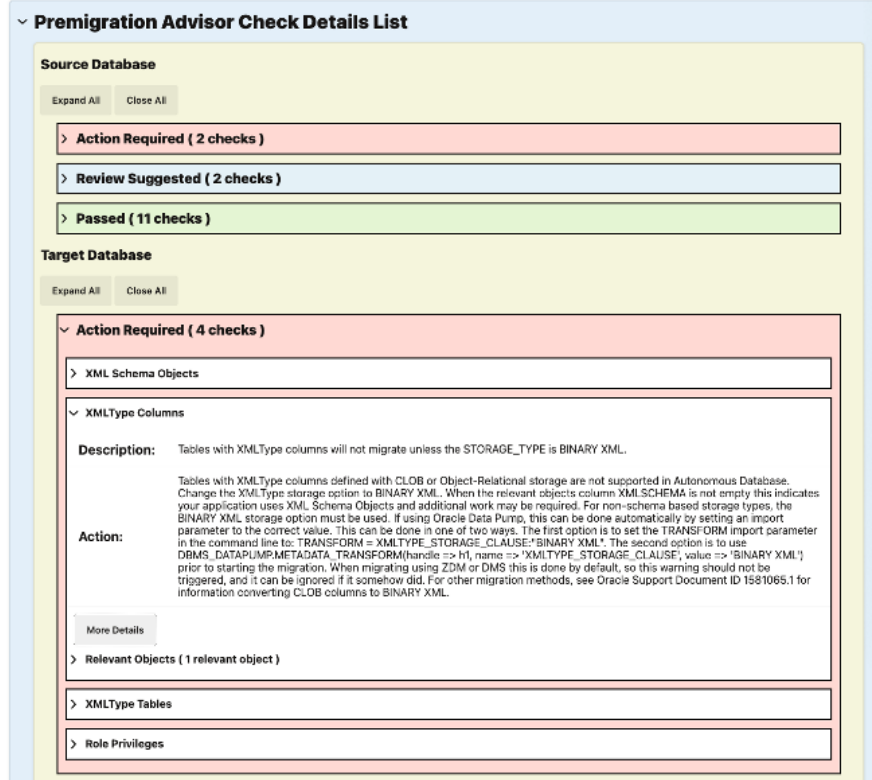
Report Result	**Action Required**
Number of schemas analyzed:	34
List of schemas analyzed:	[PRINT_SERVER, EMX, LIMS1, TEST_DB, DEV_DB_NEW, DEV_DB_UPDATE, DEV, UI, UIF, PRE, LIMS051012018, LIMS, UIPC20181011, CSW_TEST_DB, REL, RELEASE_DB_NEW, RELEASE_DB_UPDATE, RELEASE_TEST_DB, QAU, QA, VOICE, TEST, PPOLAPSK, PENTEST, AISERVICE, AISERVICE_REL, MLESKO, RJEDRZEJ, SIEM_QAU, SIEM_REL, RSK, UIPC, AAA, DEBEZIUM]
Fixup Summary:	A total of 3 fixup scripts were generated

Report Results Overview

Source Database		Target Database		Migration Method		Additional Tasks	
Action Required	2	Action Required	4	Action Required	0	Action Required	0
Review Required	0	Review Required	3	Review Required	1	Review Required	0
Review Suggested	2	Review Suggested	3	Review Suggested	0	Review Suggested	3
Passed	11	Passed	20	Passed	0	Passed	10

Return to Table of Contents

CPAT Sample 1



CPAT Sample 2

4.2.5 Backup and Recovery

Guide:

This section defines the backup and recovery needs for the workload, which may differ from the current system.

RPO/RTO: Specify the Recovery Point Objective (RPO) and Recovery Time Objective (RTO) for each environment.

Backup Retention: Define retention periods based on compliance, business and operational needs.

Database or Storage Server Expansions: If not applicable to storage/database expansion, mark as "N/A due to limited-scope activity: Only Expansion Needed"

Example: Please Edit according to the service capabilities

The current backup approach relies on a combination of local storage and NFS-based scripts. In the target architecture, backups will be modernized by using Oracle-managed automatic backups provided by Oracle Base Database Service on Google Cloud. Oracle recommends enabling automatic backups for all databases to ensure consistent recovery and compliance with corporate data protection standards. For ExaDB/ADB-S/Base Database Service, two backup destination options are available via the OCI Console:

- Object Storage
- Autonomous Recovery Service (RCV) — Recommended (only available for ExaDB, Exascale and BaseDB)

The proposed configuration will use Autonomous Recovery Service (RCV) as the centralized backup and recovery solution. Backup operations are policy-driven and automatically managed by the target Database Service, eliminating the need for manual backup scheduling or traditional full backup cycles.

Copyright @2024, Oracle and/or its affiliates

Autonomous Recovery Service uses an always incremental backup approach, where only changed database blocks are transmitted during each backup operation. Recovery Service maintains these block versions and automatically presents each recovery point as a full backup, ensuring efficient storage utilization while supporting fast and predictable recovery.

Backup protection levels, retention, and recovery objectives are enforced through Recovery Service policies aligned with the customer's data protection requirements.

Environment	Backup Frequency	Retention	Recovery Time	Backup Target
Production	Daily, Incremental, Weekly Full	60 days	2 hours	Recovery Service / Object Storage
Dev + Test	Daily, Incremental, Weekly Full	30 days	24 hours	Recovery Service / Object Storage
DR	Daily, Incremental, Weekly Full	30 days	4 hours	Recovery Service / Object Storage

Note that special consideration needs to be given for to the specifics of HA/DR in Oracle Database@Google Cloud. Specifically:

- *The (limited) regional availability of the solution (see "Where can I use the service?" in the FAQ: https://www.oracle.com/cloud/google/oracle-database-at-google-cloud/faq/*
- *Differences in naming conventions (Availability Zones in Google Cloud rather than the OCI Availability Domains)*

ExaDB/ExaXs/BaseDB cloud tooling supports both OCI Object Storage and Autonomous Recovery Service as backup destination through automatic backups.

ADB-S cloud tooling supports OCI Object Storage only as backup destination through automatic backups.

- *Note that Autonomous Recovery Service is also available either @OCI or @Google Cloud, the customer has the choice to leverage RCV in either Google Cloud or at OCI. Oracle Database Autonomous Recovery Service and Oracle Cloud Infrastructure Object Storage are the recommended backup services for automated database backup and will draw down on a customer's Google Cloud commitments.*

If there are any (security) requirement to keep all data within the Google Cloud data centers at all times, then DR and Backup solutions need to be considered with some care, and this would have to be captured in this section.

This chapter is mandatory, while there could be no requirements on HA/DR, please mention that in a short single sentence.

Example: ExaDB/Exascale

The databases will be implemented on 2-node Exadata clusters, thereby providing high availability. Oracle MAA Best Practices and Reference Architectures should be considered for all environments.

Both applications have a RPO of 0, with an RTO of 5 minutes. For this reason, Active Data Guard will be used to keep the Production and DR databases in sync. The traffic between the Primary and Standby databases will run through the Google-Managed network.

In addition, OCI Autonomous Recovery service (with Real-time data protection, i.e. Zero Data Loss mode) in the Google Cloud data center will be used to accommodate increasing demands for Ransomware Protection (Compliance and Immutability) and near-zero RPO.

Example: BasedDB

The databases will be deployed on Oracle Base Database Service on Google Cloud, configured for high availability within a single Google Cloud region using zonal redundancy. Oracle Maximum Availability Architecture (MAA) best practices and reference architectures will be followed for all environments to ensure consistency and resilience.

For disaster recovery, Oracle Data Guard will be configured between the primary and standby databases located in different Google Cloud zones within the same region, or in separate regions if required by the business continuity plan. This configuration supports rapid failover and minimizes downtime in case of an outage.

Copyright @2024, Oracle and/or its affiliates

Both critical applications require an RPO of 0 and an RTO of 5 minutes. Active Data Guard in synchronous mode will therefore be used to maintain real-time data protection between the Production and DR databases. All Data Guard traffic will run through the Google-managed network, ensuring low latency and secure connectivity between sites.

At this stage, automatic backups to Object Storage will be configured for all databases. Once available, Autonomous Recovery Service (RCV) may be adopted to enhance ransomware protection, immutability, and achieve near-zero RPO for critical workloads.

Example: ADB

The databases will be implemented as Autonomous AI Transaction Processing having built in high availability. The databases have an RPO of 2 minutes and RTO of 15 minutes, Autonomous dataguard will be used to set up cross region DR from primary site (Europe West2) to Europe West 3.

For Autonomous AI database@Google, backups are managed by Oracle and automatically created and stored in Oracle Object Storage. Retention period will be selected between 1-60 days.

4.2.6 Security Requirements

Guide:

Capture the Non-Functional Requirements for security-related topics. The requirements can be (but don't have to be) separated into:

- *Identity and Access Management*
- *Data Security*

Other security topics, such as network security, application security, key management, or others can be added if needed.

Take note that parts of the solution running on Google Cloud but which are not directly related to Oracle Database@Google Cloud, are not required to be captured here. For example, Google Cloud application security does not have to be captured here.

For Oracle Database@Google Cloud there are a number of specific considerations which can be clarified during this phase, or later. For more details on the following requirements you can visit this link

- OCI access for (Database) Management
- Oracle Database@Google Cloud onboarding requirements (required privileges)
- Google Cloud governance: Capture Google Cloud subscription design, resource groups and users/groups details. E.g. current application environments subscriptions/resource group design to be used with Oracle Database@Google Cloud deployment. Take care to compare with limitations of Oracle Database@Google Cloud in terms of mapping to subscriptions, resource groups, etc.
- Identity and Access Management (IAM)

4.2.6.1 Identity and Access Management

Guide:

You can capture all the Identity and Acess Management related requirements here. This can also cover the any SSO federation, users and groups mapping, additional privileges which may be necessary to document

Example:

MYTestCustomer has an existing IAM setup based on Google Cloud IAM. OCI IAM will be federated with Google Cloud IAM.

The Oracle Database@Google Cloud service will automatically create groups with administrative privileges, which will be assigned to the correct admins e.g. (odbg-db-family-administrators). The groups will also be replicated in OCI during the (optional but highly recommended) identity federation process.

Copyright @2024, Oracle and/or its affiliates

Additionally, all resources for these workloads will run in the same Google Cloud subscription. There will be different Google projects for the production, DR and non-production workloads.

4.2.6.2 Data Encryption / Key Management

Guide

Capture all the data encryption and key management requirements for the customer. Ensure that details related to current key usage (if any) and how it will be migrated for the Database@Google deployment are documented here

Oracle ensures comprehensive data security with default encryption for data at rest and data in transit. Customers can manage their own encryption keys through Oracle Key Management for greater control. Oracle Data Safe enhances protection with features such as activity auditing, sensitive data discovery, user risk assessment and data masking. Additionally, Oracle Audit, Oracle Database Vault and Transparent Data Encryption (TDE) provide layered security controls to prevent unauthorised access and ensure compliance.

For Key Management, if customer-managed keys are required, then additional consideration needs to be given to the implication of choosing between the options:

- *Oracle Key Vault, running on Google Cloud VMs. This option is normally positioned as the default "right" choice, unless there are specific reasons not to use this. Oracle Key Vault enables customers to securely manage security objects for Oracle Database@Google Cloud in Google Cloud, that includes encryption keys, Oracle wallets, Java Keystores (JKS), Java Cryptography Extension Keystores (JCEKS), and credential files with SSH private keys, etc.*
- *OCI Vault (running in OCI). Due to the additional latency between Google Cloud and OCI, this should not be the default choice. However, for example in solutions where the keys need to be held in hardware, it would be the only valid choice. (OCI subscription needed)*
- *File based. Unless this is a very simple solution, file based key management is not recommended.*
- *Google Cloud Key Management Service is Google's Cloud native key management solution.*

It is recommended to work with Data Security team to educate the customer about key management decisions.

Example:

MYTestCustomer has a requirement to manage their own Oracle Database@Google Cloud encryption keys. For this there are 4 options:

- Oracle Managed Keys
- OCI Vault
- Oracle Key Vault (OKV)
- Google Key Management System

Utilizing Oracle Key Vault with Base Database Service@Google Cloud provides customers the following benefits:

- Fault tolerance
- High availability
- Scalability
- Security
- Standards-compliance

Oracle strongly recommends the use of OKV for the key management of Oracle Database@Google Cloud, which is indeed what will be used for this deployment.

4.2.7 Google Cloud / OCI Networking Requirements

Guide

Copyright @2024, Oracle and/or its affiliates

Capture the Non-Functional Requirements for networking-related topics as it relates to how Oracle Database@Google Cloud communicates with the rest of the Google Cloud network.

- *Understand Google Cloud Network topology – existing and new requirements.*
- *How should the application connect to the database (same VPC, Hub & Spoke peered VPCs, shared VPC, cloud WAN)?*
- *Connectivity from other locations (on premises, other Google Cloud regions, other clouds, etc.)*
- *Any requirement of using private endpoints*
- *DNS requirements (managed, or manually integrated)*
- *Latency requirements (both from Google Cloud to Oracle Database@Google Cloud, and if required, from OCI to Oracle Database@Google Cloud).*

If the OCI network elements of Oracle Database@Google Cloud are to be leveraged in this workload, then standard OCI network requirements can also be described here, and you can use the networking questions in the Annex

Capture the Non-Functional Requirements for networking-related topics. You can use the networking questions in the Annex

Customers evaluating network security solutions typically prioritize the following requirements:

- *Data Protection: Safeguarding sensitive information against unauthorized access, theft, or modification is a primary concern for any organization and industry today.*
    - *Threat Prevention: Advanced capabilities like IDPS and malware detection for blocking threats.*
    - *Data Loss Prevention (DLP): Monitoring and controlling sensitive data transmission.*
    - *Encryption and Decryption: Inspecting encrypted traffic without compromising privacy.*
- *Threat Prevention: Proactively identifying and mitigating security threats is essential for maintaining the integrity of network infrastructure.*
    - *Intrusion Detection and Prevention: Monitoring for suspicious or malicious activity.*
    - *Application Control: Granular control over specific applications or services.*
    - *URL Filtering: Controlling access to permitted URLs.*
- *Security compliance: Does your organization have network security requirements based on industry or organization compliance? For example - SAMA (Saudi Arabia Monetary Authority), HIPAA (Health Insurance Portability and Accountability Act), GDPR (General Data Protection Regulation), SWIFT, etc.*

Example: Generic

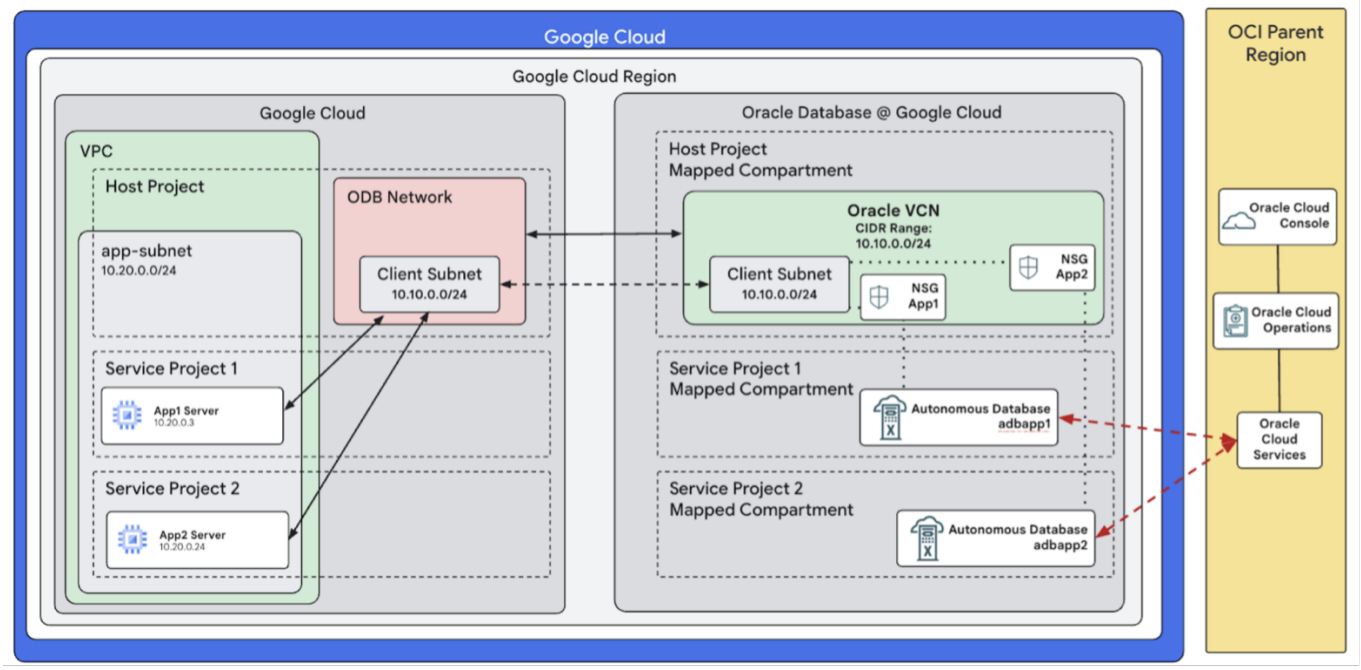
The default implementation for MYTestCustomer is to use a Hub-and-Spoke model within Google Cloud, leveraging a centralized Hub VPC for traffic inspection and management. However, for Oracle Database@Google Cloud workloads, the applications and databases will be deployed in separate VPCs, directly peered to minimize latency. This approach ensures optimized performance for application-to-database traffic while maintaining a secure and scalable architecture. DNS for Oracle Database@Google Cloud will be integrated with the existing Google Cloud DNS environment.

Example: BaseDB/ADB-S

The default implementation for MYTestCustomer is to use a shared VPC model. This will allow MYTestCustomer to connect Base Database Service@Google Cloud resources from multiple projects to a common Virtual Private Cloud (VPC) network in a Host project. Organization administrators can delegate management of applications to Service Project Administrators while maintaining centralized control over network resources. This simplifies the configuration and allows these resources to communicate securely and efficiently with each other using an internal IP address from the Shared VPC network.

Shared VPCs simplify networking configuration in Google Cloud. Service owners, like database users, use the network configuration defined by their network teams, instead of manually configuring the networks between different resources. It reduces the need to enable and configure VPC Peering and associated configurations.

Copyright @2024, Oracle and/or its affiliates



Networking High Level

4.2.8 Management and Monitoring

This subsection helps you capture any requirements for customer management and monitoring needs - e.g. system monitoring, systems management, log analysis, etc.

When you move or start an OCI project, you have a choice to use the tools you are familiar with (should they support modern application architectures), replace them with OCI native Observability services, or use a combination to improve your visibility. When contemplating how to proceed, here are some general questions that will guide you:

- *Does the tool manage across hybrid and multi-cloud environments?*
- *What is the cost of integrating the existing tool with OCI?*
- *Is my current monitor tool enabling you to prevent issues versus reacting to them?*
- *Does the tool tell you how much impact there has been on users or just that there was an impact like something is down or unavailable?*
- *Does the tool provide the full vision of applications and their infrastructure or just a piece of them or specific technology?*

Example:

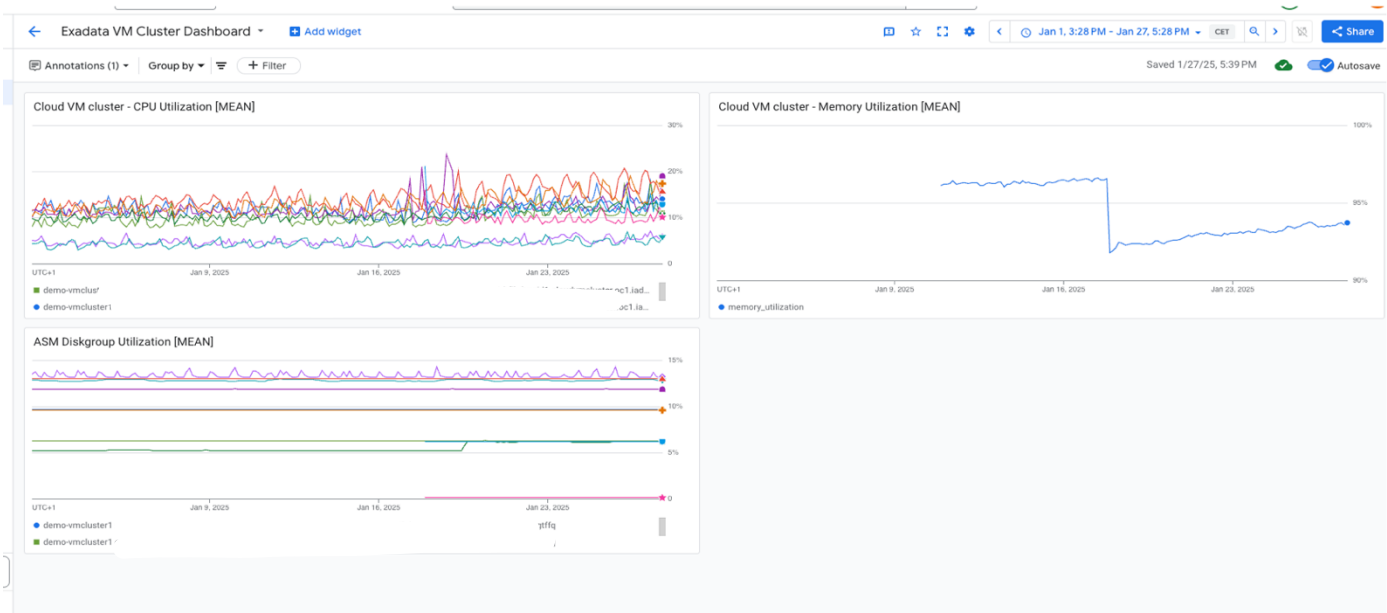
Task	Target	Location	New	Notes
Application Monitoring	All targets	On-Prem and OCI	No	
Monitoring	All targets	OCI (Migration)	No	
Log Management	All targets	OCI (Migration)	No	
Insight	All Oracle DBs	OCI (Migration)	No	

For the above section you can replace it accordingly with your requirements for Database@Google project.

Example:

Copyright @2024, Oracle and/or its affiliates

When you move or start an Oracle Database@Google Cloud project, you have a choice to use the monitoring tools you are familiar with (should they support modern application architectures), including Google Cloud or 3rd party tools. Because Oracle Database@Google Cloud runs within an OCI tenancy, Oracle's recommended approach is to leverage native OCI observability services to ensure optimal performance and management.*



All the logs and monitoring metrics would be available through OCI, and Google Cloud.

Oracle Database@Google Observability within Google

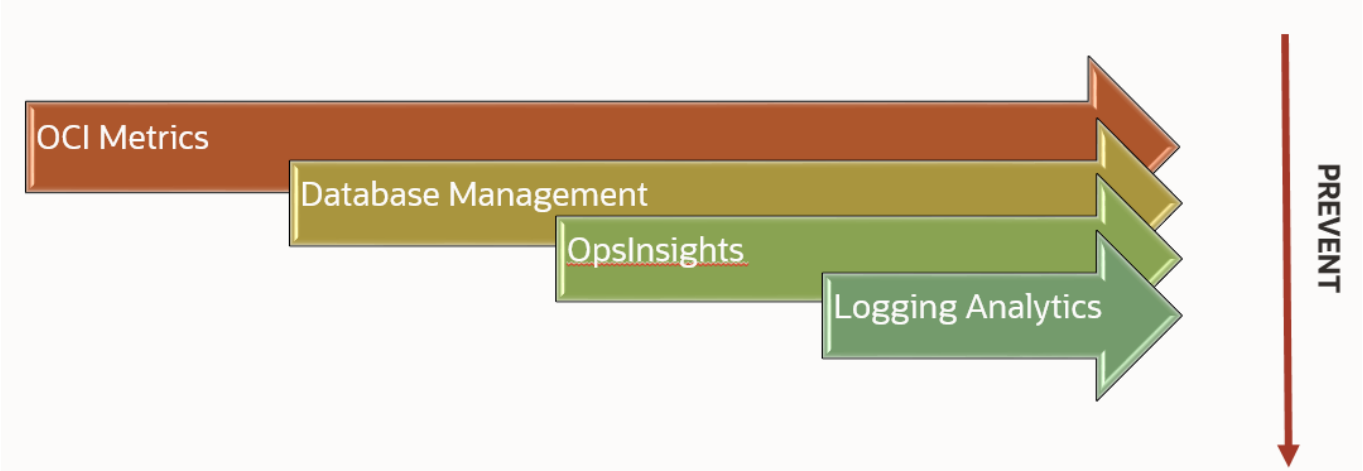
OCI native Observability services for Oracle Database@Google Cloud:

Tool	Service	Tool Location(ADB-S)	Tool Location (ExaDB)	OCI Subscription	Notes
OCI Metrics	basic monitoring	OCI	OCI/Google Cloud	not required	Available by default
Database Management*	advance monitoring & admin	OCI	OCI/Google Cloud	required	To be enabled - DBM Admin features only available in OCI
Ops Insights	Forecast & Capacity planning	OCI	OCI	required	To be enabled
Logging Analytics	Log analysis	OCI	OCI	required	OOTB Parsers/dashboards for Oracle DB

Oracle Database@Google Cloud natively expose logs and maps basic metrics. To enable Administration and advanced analytics capabilities like Resource Forecast, OCI subscription is needed as the relevant services cannot be consumed against Oracle DB@Google Commitment. Once the Oracle Universal credit is available it is possible to activate OCI native services as described here. OOTB dashboard and metrics are available on OCI tenant.

Oracle Enterprise Manager provides Database Management capabilities for customers who do not have an OCI subscription, offering a comprehensive solution for managing Oracle database.

Copyright @2024, Oracle and/or its affiliates



Observability Tools for DB@Google

Example:

MYTestCustomer wants to use Google Cloud Monitor for Metrics, and OCI Database Management, and Splunk for log analysis.

Tool	Task	Target	Location	New	Notes
OCI Database Management	Manage DB Instances + Monitoring and troubleshooting	All targets	OCI	Yes	
Google Cloud Monitoring	Basic metric monitoring	All VM Clusters and DBs	Google Cloud	Yes	
Splunk	Log Analytics	All targets	Splunk	No	

4.2.9 Automation & Integration (IaC)

Guide:

This subsection captures any requirements for integration into the customer's existing automation tools and practices - e.g. terraform, API, SDK requirements. Also, if the customer requires integration into automation platforms e.g. Jenkins, Ansible, GitHub, CD/CI Google Cloud pipelines etc. these should be recorded.

Example:

At the time of this document creation, no Automation requirements have been specified. MYTestCustomer can leverage Google Cloud and OCI Cloud Native automation tools to provision end to end Exadata Infrastructure, Cluster VM and the database. Also for the Base Database and ADB-S native automation tools can be used. Both providers are declared and you can use one Terraform recipe to orchestrate Exadata Infrastructure, VM Cluster and the PDB and CDB provisioning and management.

Official documentation is available here.

Example Autonomous DB:

MYTestCustomer wants to automate the provisioning of Autonomous AI database using Terraform . MYTestCustomer can provision an Autonomous AI database in Google Cloud using Google Cloud Terraform provider and modify the same using OCI Terraform provider.

Copyright @2024, Oracle and/or its affiliates

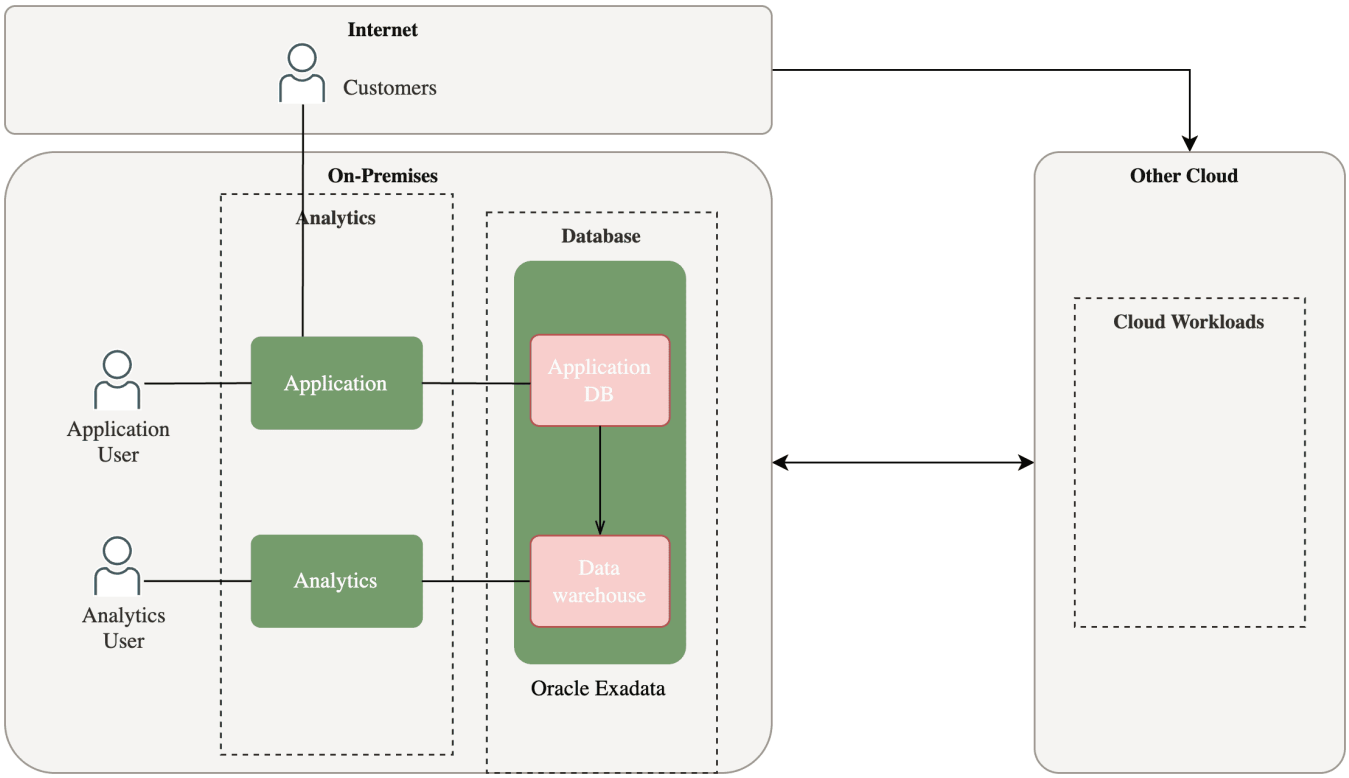
Official documentation is available here.

4.3 Current State Architecture

Guide: Try to capture as much information as possible and suitable for the context of this project. The logical diagram below can be extended or modified for the actual customer requirement. E.g. there can be partners instead of just customer, there can be other cloud vendors already in the picture and so on. Below diagrams draw.io file is available in the diagrams repository for further editing.You can go as broader as you like but capture as much details as possible for the workloads in consideration.

Example 1:

The current implementation of this workload runs fully in MYTestCustomer's own data center. 1 x Exadata Machine contains all database workloads, and both the application and the BI environment are running in the same network. Internet-based customers have access to the self-service part of the application.



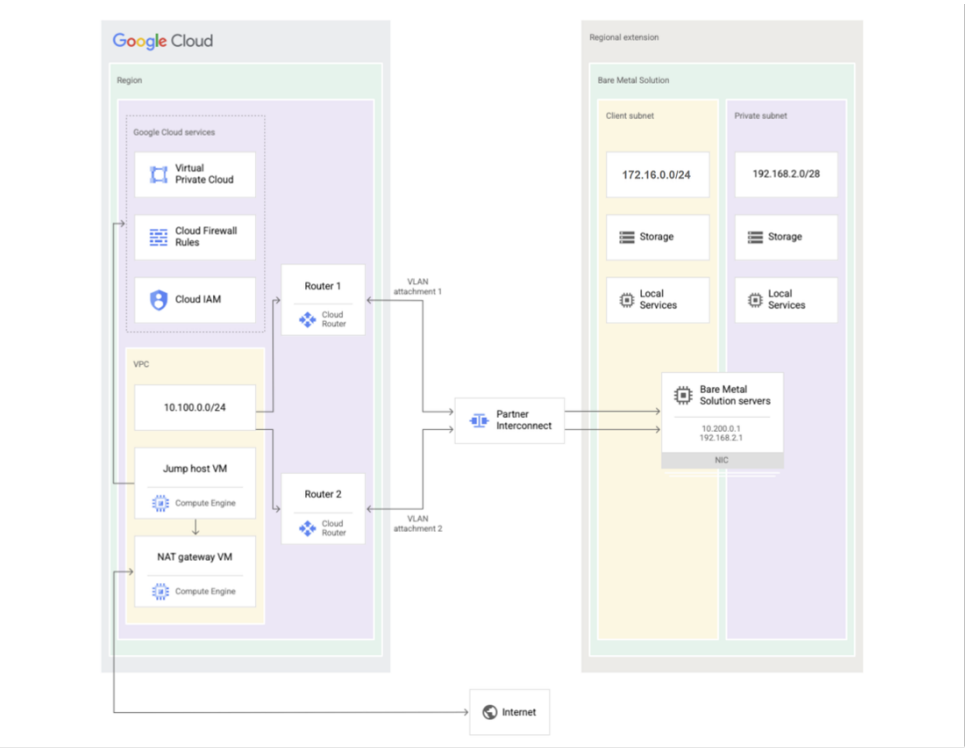
Current State Logical Architecture

Example 2:

Oracle Database workloads currently run on Google Cloud Bare Metal Solution within a dedicated Google Cloud region. The databases are accessed by application tiers in Google Cloud and by on-premises systems through Partner Interconnect, providing private and secure connectivity via a dedicated VPC.

This architecture introduces key limitations. High availability and disaster recovery rely on manual processes, resulting in higher operational risk and recovery times. Database lifecycle management, scaling, and backups are fully customer-managed, increasing operational complexity and limiting agility. In addition, advanced security capabilities such as backup immutability and ransomware protection require custom implementations.

Copyright @2024, Oracle and/or its affiliates

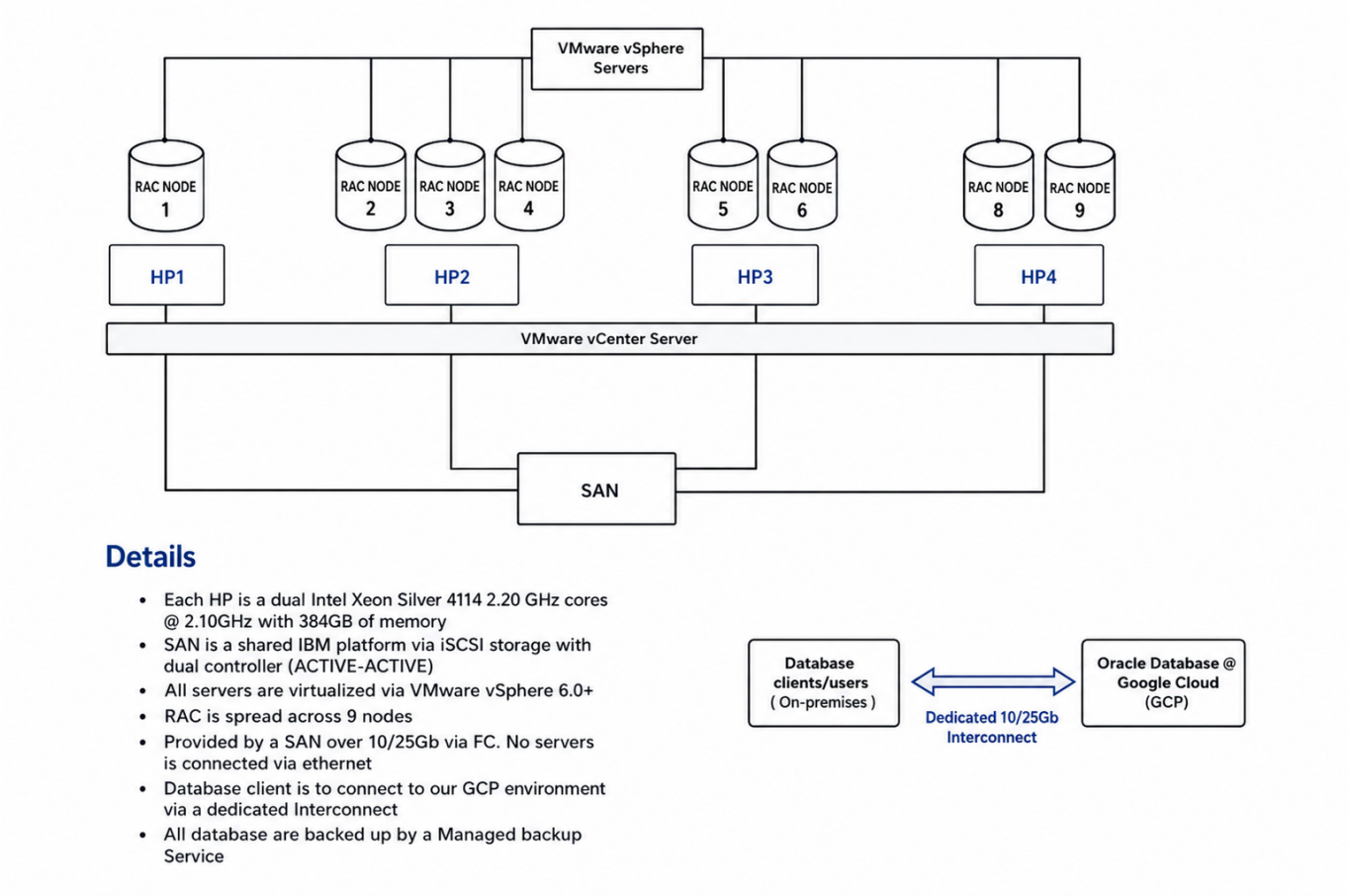


Current State Logical Architecture

Example 3 (ADB):

The current implementation of MYTestCustomer includes databases on VMware on-premise and applications hosted on Google Kubernetes engines . There is a redundant partner interconnect between customers on premise and Google Cloud.

Copyright @2024, Oracle and/or its affiliates



Current State Logical Architecture

4.4 Future State Architecture

Guide:

The Future State Architecture can be described in various forms. In the easiest case, we describe a Logical Architecture, possibly with a System Context Diagram. A high-level physical architecture is mandatory as a description of your solution.

This should be the final architecture as part of the pre-sales solution, not an intermediate or draft version

Additional architectures, in the subsections, can be used to describe needs for specific solution.

4.4.1 Solution Best Practices

Guide:

Oracle highly recommends following the solution best practices for Google as well for OCI. More details on planning your solution at Oracle Database@Google Cloud can be found here

Oracle highly recommends following best practices to protect your Database@Google solution on OCI:

Mandatory Security Best Practices:

Guide:

This chapter only requires to replace the customer name placeholder. Do not change anything else.

Oracle Database@Google Cloud is deployed within an Google Cloud framework, and therefore any Google Cloud security best practices apply to the whole solution / workload. Those best practices are not discussed further in this document.

Oracle Database@Google Cloud is also part of an OCI tenancy, and as such OCI Security best practices also apply and are described here:

The safety of the MYTestCustomer's Oracle Cloud Infrastructure (OCI) environment and data is the MYTestCustomer's priority.

The following table of OCI Security Best Practices lists the recommended topics to provide a secure foundation for every OCI implementation. It applies to new and existing tenancies and should be implemented before the Workload defined in this document will be implemented.

Workload-related security requirements and settings like tenancy structure, groups, and permissions are defined in the respective chapters.

Any deviations from these recommendations needed for the scope of this document will be documented in the chapters below. They must be approved by MYTestCustomer.

MYTestCustomer is responsible for implementing, managing, and maintaining all listed topics.

CATEGORY	TOPIC	DETAILS
User Management	IAM Default Domain	Multi-factor Authentication (MFA) should be enabled and enforced for every non-federated OCI user account. For configuration details see Managing Multi-Factor Authentication. In addition to enforcing MFA for local users, Adaptive Security will be enabled to track the Risk Score of each user of the Default Domain. For configuration details see Managing Adaptive Security and Risk Providers.
User Management	OCI Emergency Users	A maximum of **three** non-federated OCI user accounts should be present with the following requirements: Username does not match any username in the Customer's Enterprise Identity Management System. Are real humans. Have a recovery email address that differs from the primary email address. User capabilities have Local Password enabled only. Has MFA enabled and enforced (see IAM Default Domain). Consider using FIDO security keys as the MFA factor, stored securely in a known location accessible during emergencies.
User Management	OCI Administrators	Daily business OCI Administrators are managed by the Customer's Enterprise Identity Management System. This system is federated with the IAM Default Domain following these configuration steps: Federation Setup, User Provisioning. For configuration guidance for major Identity Providers see the OCI IAM Identity Domain tutorials.
User Management	Application Users	Application users like OS users, Database users, or PaaS users are not managed in the IAM Default Domain but either directly or in dedicated identity domains. These identity domains and users are covered in the Workload design. For additional information see Design Guidance for IAM Security Structure.
Cloud Posture Management	OCI Cloud Guard	OCI Cloud Guard will be enabled at the root compartment of the tenancy. The reporting region should be carefully selected as it cannot be changed without disabling and re-enabling Cloud Guard. This way it covers all future extensions, like new regions or new compartments, of your tenancy automatically. It will use the Oracle Managed Detector and Responder recipes at the beginning and can be customized by the Customer to fulfill the Customer's security requirements. For configuration details see Getting Started with Cloud Guard. Customization of the Cloud Guard Detector and Responder recipes to fit the Customer's requirements is highly recommended. This step requires thorough planning and decisions to make. For configuration details see Customizing Cloud Guard Configuration.

Copyright @2024, Oracle and/or its affiliates

CATEGORY	TOPIC	DETAILS
Cloud Posture Management	OCI Vulnerability Scanning Service	In addition to OCI Cloud Guard, the OCI Vulnerability Scanning Service will be enabled at the root compartment. VSS is regional and needs configuration in each region where you have Compute instances. This service provides vulnerability scanning of all Compute instances once they are created. For configuration details see Vulnerability Scanning.
Monitoring	SIEM Integration	Continuous monitoring of OCI resources is key for maintaining the required security level (see Regulations and Compliance for specific requirements). See Design Guidance for SIEM Integration to implement integration with the existing SIEM system.
Additional Services	Budget Control	OCI Budget Control provides an easy-to-use and quick notification on changes in the tenancy's budget consumption. It will be configured to quickly identify unexpected usage of the tenancy. For configuration details see Managing Budgets.

Google Cloud Security Best Practices:

Guide:

Describe any Google Cloud best practices, security it critical with data encryption, VPC Service Controls. Network design should use subnets, firewall rules and secure communications such as VPC peering.

Naming Conventions:

Guide:

For Oracle Database@Google Cloud workloads without any additional OCI components, it is acceptable to refer to existing Google Cloud naming conventions, rather than describing Google Cloud naming conventions here.

This chapter describes naming convention best practices and usually does not require any changes. If changes are required, please refer to Landing Zone GitHub. The naming convention zone needs to be described in the Solution Design by the service provider.

Use this template ONLY for new cloud deployments and remove it for brownfield deployments. A naming convention is an important part of any deployment to ensure consistency, governance, and security within your tenancy. Find here Oracle's recommended best practices.

OCI Landing Zones:

Guide:

This chapter describes landing zone best practices and usually does not require any changes. If changes are required please refer to Landing Zone GitHub. The full landing zone needs to be described in the Solution Design by the service provider.

Use this template ONLY for new cloud deployments and remove it for brownfield deployments. When Oracle Database@Google Cloud is implemented, it is always linked to an OCI tenancy.

An OCI Landing Zone provides the foundational cloud environment on which workloads are deployed. It defines standardized patterns for identity and access management, network design, compartment structure, security controls, logging, monitoring, and governance, while organizing cloud adoption across operating entities, environments, platforms, and projects.

This foundation enables organizations to onboard and run OCI securely, consistently, and at scale. By establishing shared guardrails, governance boundaries, and reusable design patterns, a Landing Zone reduces risk, supports segregation of duties, improves operational efficiency, and makes it easier to deploy new workloads without rebuilding core controls each time.

Copyright @2024, Oracle and/or its affiliates

In practice, a Landing Zone provides the baseline for tenancy and compartment design, policies, connectivity, observability, security services, tagging, and shared services. This supports stronger governance, repeatable deployments, and clearer ownership across platform, security, network, and workload teams.

Oracle highly recommends the use of an OCI Landing Zone for any deployment. For more up-to-date and relevant information, use these guidelines to define or assess your OCI Landing Zone, including design considerations, reference approaches, and recommended solutions. Additional practical guidance is also available in the OCI Landing Zone Operating Entities repository, which provides blueprint-based designs for onboarding one or multiple operating entities in a single or multipe tenancies. The default minimum recommended baseline is the One-OE model which meets the requirements of most customers and can be deployed with a few clicks.

Note also that there are 2 types of Oracle Database@Google Cloud environment. Those environments where the OCI tenancy is used for other services should design an OCI Landing Zone according to the normal considerations for those workloads. For those environments where the OCI tenancy is only used to support the Oracle Database @ Google Cloud, a minimal landing zone can be used. In that case we still need to consider items such as:

- *Compartments (automatically created by the Oracle Database@Google Cloud service)*
- *IAM (groups and policies created as part of the Oracle Database@Google Cloud service)*
- *Security posture (are services like Cloud Guard, Security Zones, Vulnerability Scanning needed on OCI)*
- *Network Structure (VCNs automatically created by the Oracle Database@Google Cloud service)*
- *Network Security*
- *Network Connectivity*
- *DNS*

Naming conventions:

A naming convention is an important part of any deployment to ensure consistency, governance, and security within your tenancy. Find here Oracle's recommended best practices.

4.4.2 Logical Architecture

Guide:

Provide a high-level logical Oracle solution for the complete solution. Indicate Oracle products as abstract groups, and not as physical detailed instances. Create an architecture diagram following the latest notation and describe the solution.

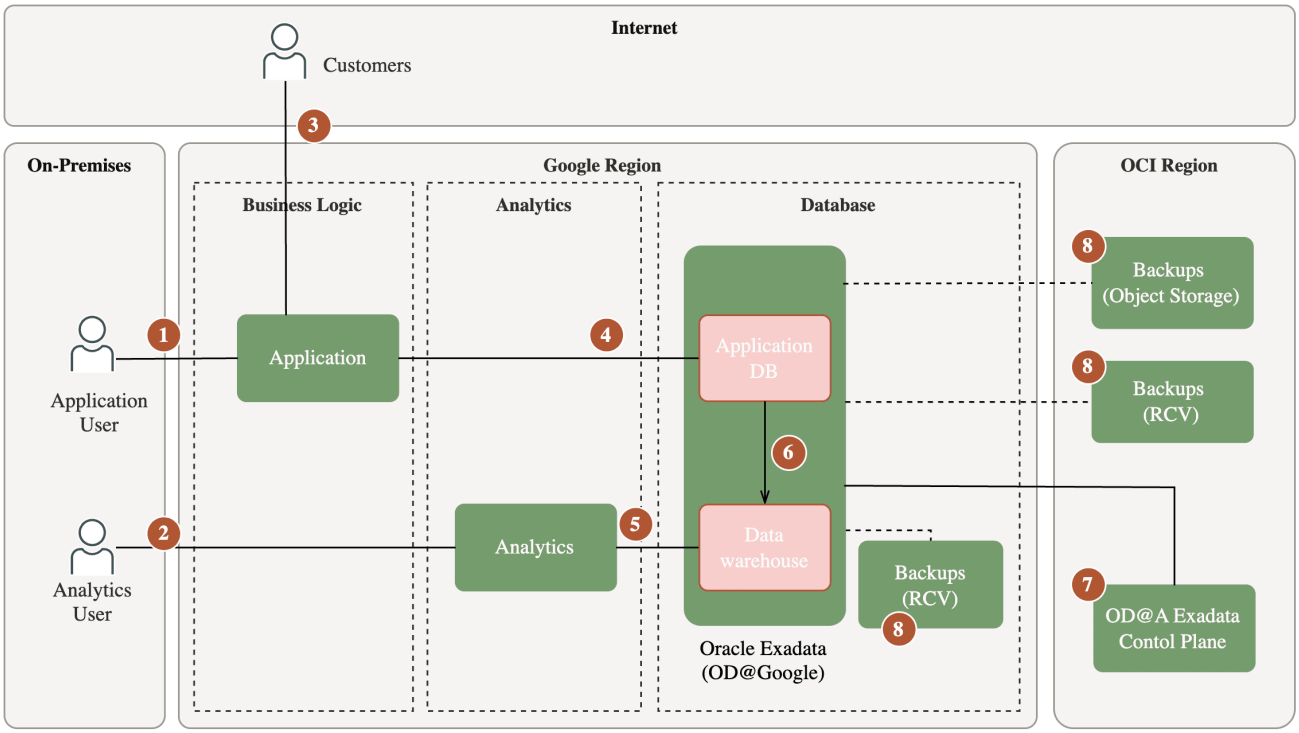
It is expected to provide a full Multicloud architecture in this section, including all Google Cloud elements which have direct or indirect access to Oracle Database@Google Cloud.

To implement a solution the Physical Architecture is needed in the next chapter. The physical notation can show individual components with physical attributes such as IP addresses, hostnames, or sizes.

The Oracle Cloud Notation, OCI Architecture Diagram Toolkits

All the diagrams and relevant resources can be downloaded from the Database@Hyperscalers Design Confluence page

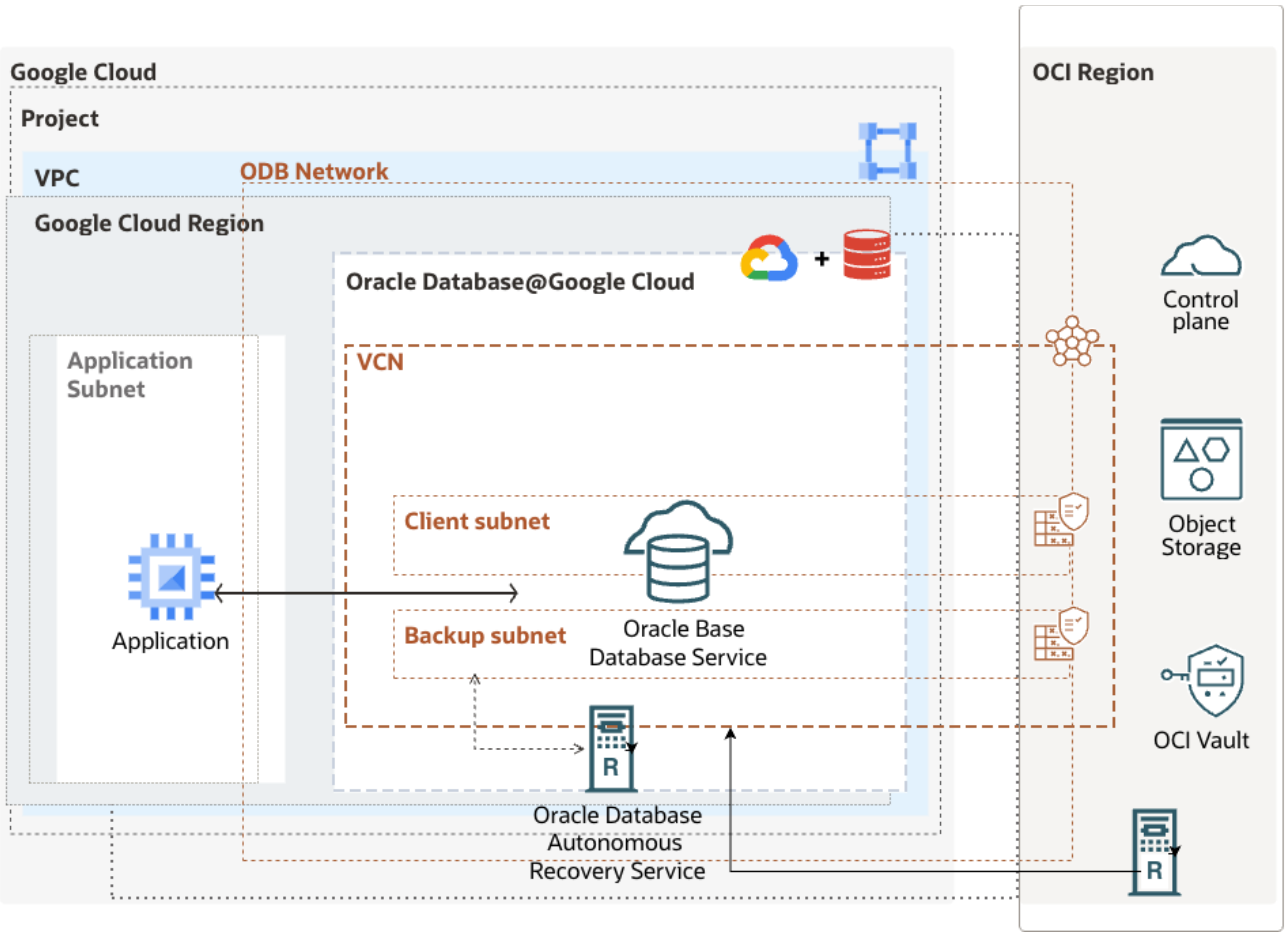
Example: ExaDB



1/2. Application and Analytics users have access to their respecitve applications in Google.
3. Customers have access to the self-service portion of the application.
4/5. Application and Analytics have access to their respective databases.
6. DWH is periodically kept updated with new data from the application DB.
7. OCI is used for Exadata and ADB-S Control Plane.
8. ExaDB-D@Google backups can be stored on one of the three: Object Storage on OCI, RCV@OCI, RCV@Google

DB@Google Logical High Level

Example: BaseDB Deployment Highlevel



DB@Google Logical High Level

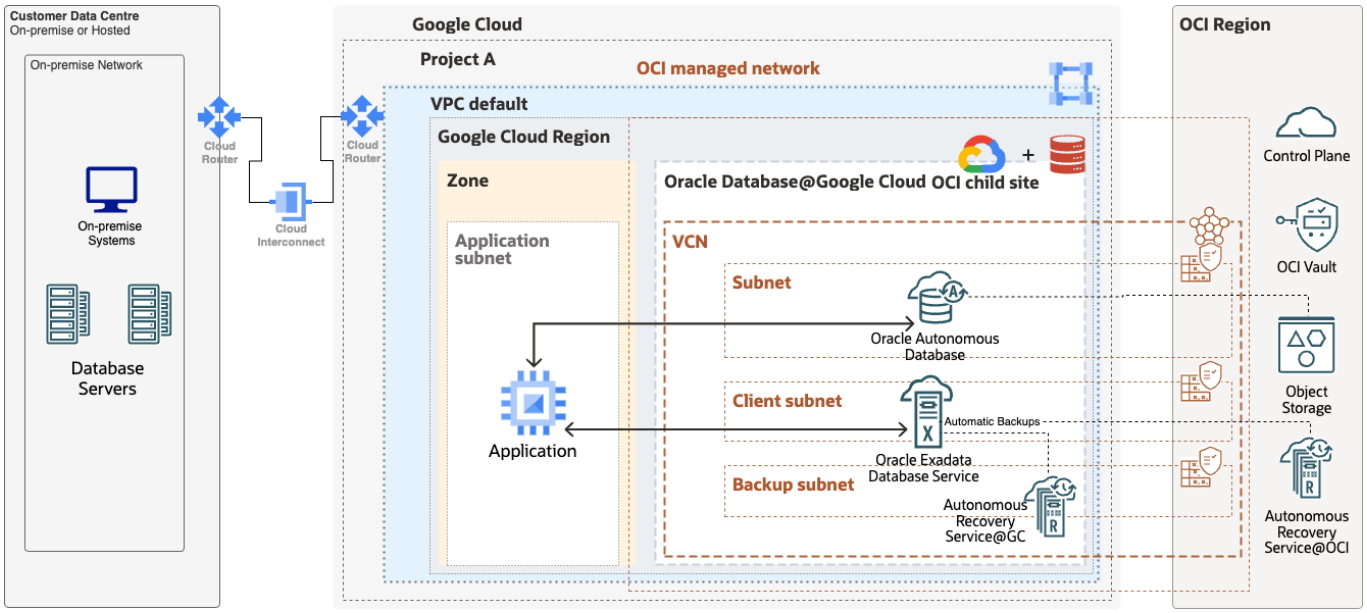
Additional Examples

4.4.2.1 Database Consolidation with Multiple Service Levels (only for ExaDB/ExaScale)

Based on requirements for data residency and local application performance this solution delivers Database service in Google Cloud data centers using ExaDB. Considering Oracle Maximum Availability Architecture (MAA) multiple service levels have been defined in the logical solution architecture below. Also note that data databases with similar requirements i.e. security posture, performance attributes, DB version etc. can be combined into a DB VM Cluster under ExaDB@Google.

Use the below diagram has as a baseline to document the deployment specific details. This diagram can be edited to incorporate other components, systems and applications hosted on Google Cloud or OCI to cover. Also, we are listing here the ExaDB and ADB-S but you can keep either or both as per customer requirements.

Copyright @2024, Oracle and/or its affiliates



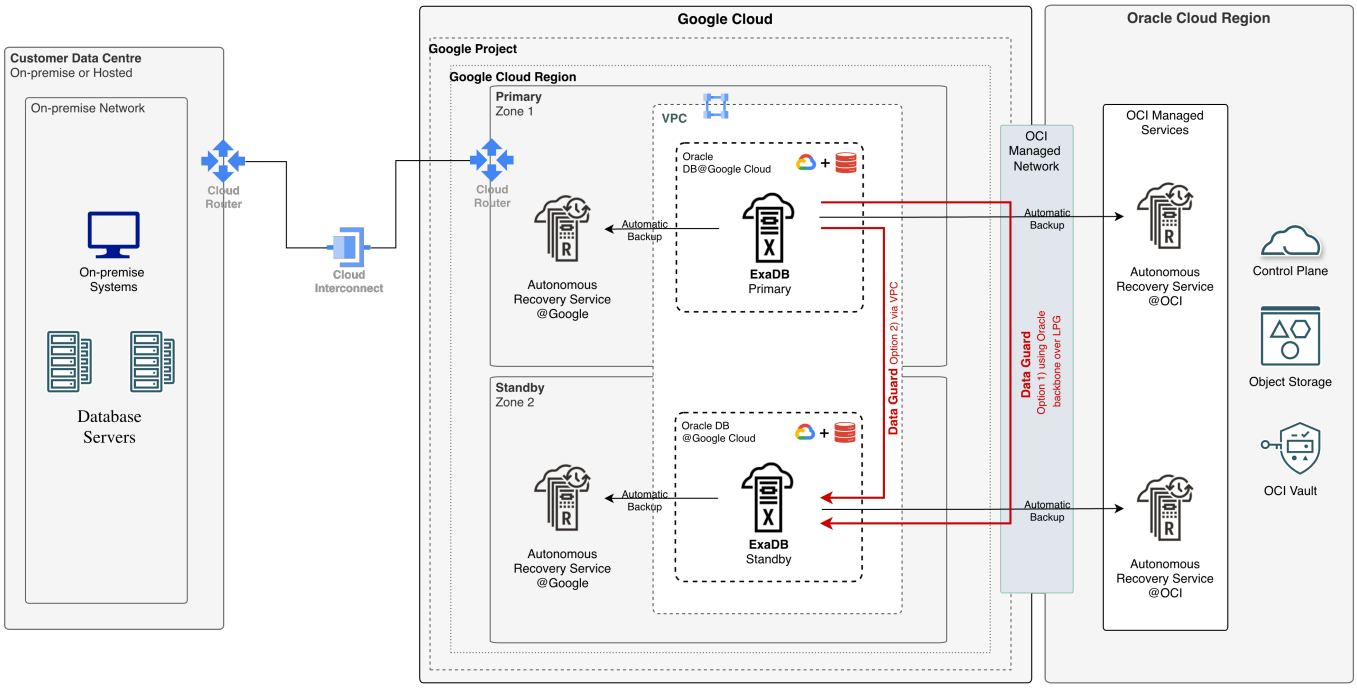
DB@Google High Level Deployment

The physical architectures can have multiple service levels for *Production Database Service A (Standby in same Google Cloud region), and Production Database service B (Standby across Google Cloud regions)

Please note that standby in same Google Cloud region, for ADB-S@Google, is a work in progress at the moment.

4.4.2.2 Service Level with High Availability, Disaster Recovery and Data Protection – within region (ExaDB-D and ExaScale)

Production Database Service A Using MAA Reference Architecture "Gold" for Production Database Service A which has High Availability with Oracle RAC, Disaster Recovery with Oracle Data Guard and Data Protection with copies in both regions with Oracle Zero Data Loss Recovery Service.



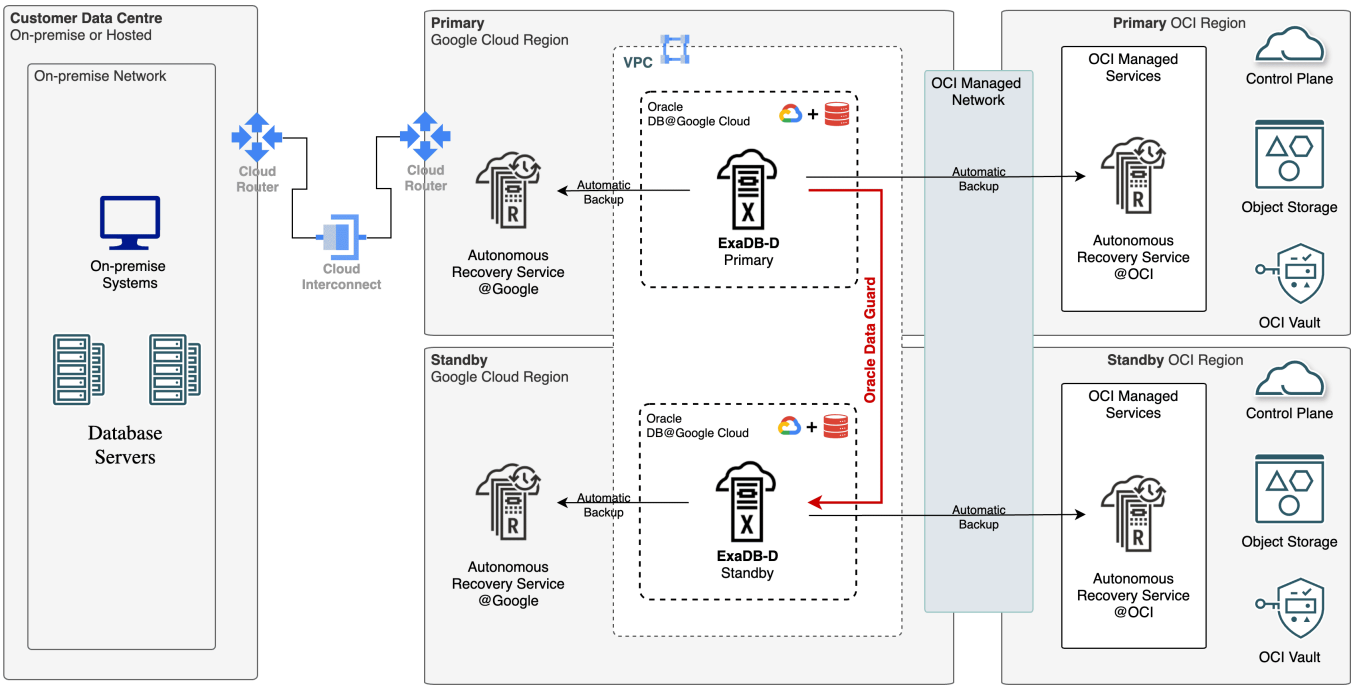
DB@Google MAA Gold Same Region

4.4.2.3 Service Level with High Availability, Disaster Recovery and Data Protection – across regions (ExaDB-D and ExaScale)

Production Database Service B

Using MAA Reference Architecture "Silver" for B and C since they are identical but split across two data centers for efficient use of available resources. Non-Production Database Service B and C has High Availability with Oracle RAC and Data Protection with copies in both data centers with Oracle Zero Data Loss Recovery Appliance (ZDLRA) and ZDLRA Replication.

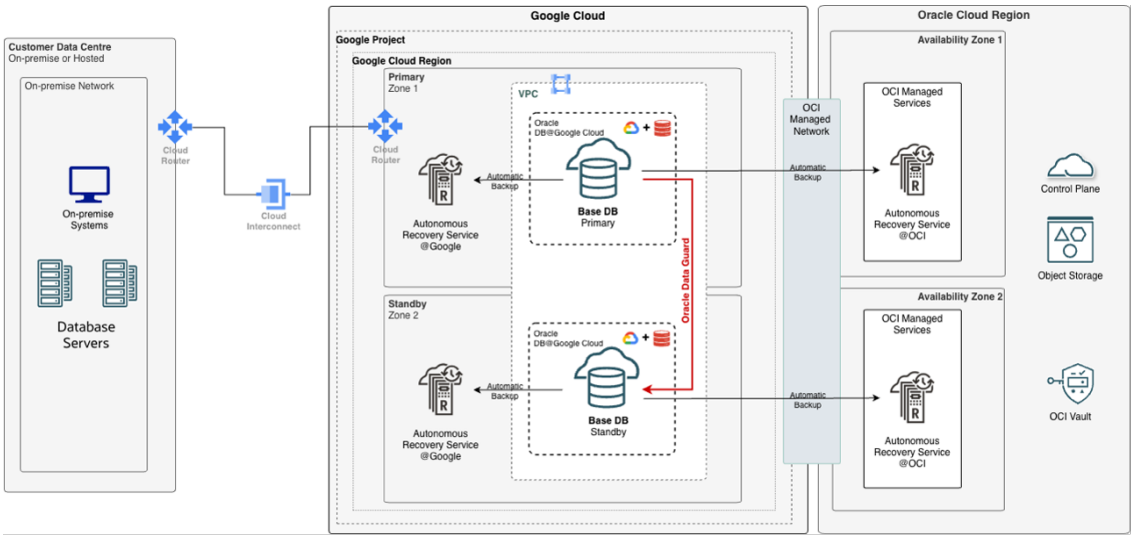
Additional information on MAA Reference Architectures can be found here: Oracle MAA For Oracle Database@Google Cloud



Details of Database Service B based on MAA Reference Architecture "Gold" across regions

4.4.2.4 Service Level with High Availability, Disaster Recovery and Data Protection – within region (BaseDB)

Production Database Service A Using MAA Reference Architecture "Gold" for Production Database Service A, Disaster Recovery with Oracle Data Guard/Autonomous Data Guard and Data Protection with copies in both zones within same region.



DB@Google MAA Gold Same Region

High availability is provided at the infrastructure and availability zone level, with the database deployed in a single Google Cloud region. Database resilience relies on Oracle Database features and Google Cloud zonal availability. Disaster recovery within the region is implemented using Oracle Data Guard between primary and standby databases deployed in different Google Cloud availability zones. Data protection is ensured through Oracle-managed automatic backups to Autonomous Recovery Service, with retention policies aligned to business and compliance requirements.

Copyright @2024, Oracle and/or its affiliates

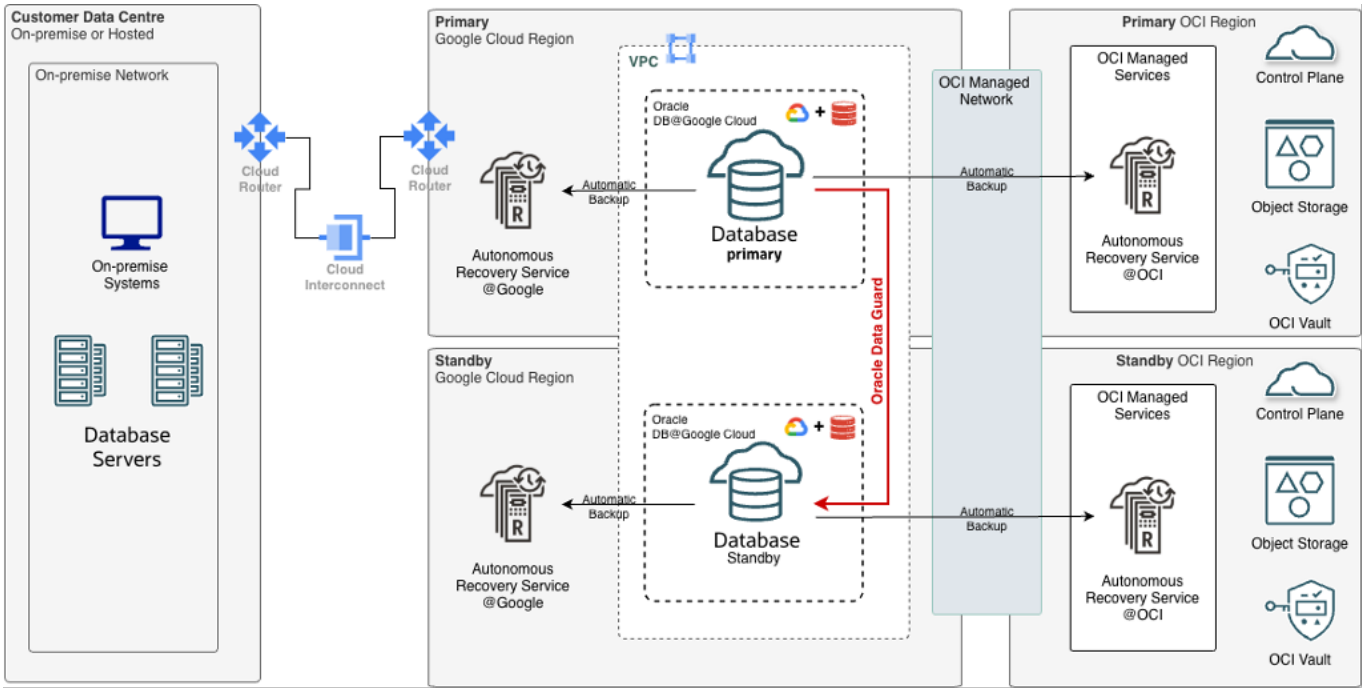
Note: Oracle Data Guard (physical standby) requires Oracle Database Enterprise Edition (EE) or Enterprise Edition – High Performance (EE-HP).

4.4.2.5 Service Level with High Availability, Disaster Recovery and Data Protection – across regions (BaseDB)

Production Database Service B

Using MAA Reference Architecture "Silver" for B and C since they are identical but split across two data centers for efficient use of available resources. Non-Production Database Service B and C has High Availability with Oracle RAC and Data Protection with copies in both data centers with Oracle Zero Data Loss Recovery Appliance (ZDLRA) and ZDLRA Replication.

Additional information on MAA Reference Architectures can be found here: Oracle MAA For Oracle Database@Google Cloud



Details of Database Service B based on MAA Reference Architecture "Gold" across regions

Production Database Service B extends the Base Database Service deployment across two Google Cloud regions to enhance business continuity. Disaster recovery is implemented using Oracle Data Guard for inter-region replication, supporting defined RPO and RTO objectives. Data protection is provided through Oracle-managed automatic backups to Autonomous Recovery Service with backup frequency and retention defined according to business requirements.

Note: Oracle Data Guard (physical standby) requires Oracle Database Enterprise Edition (EE) or Enterprise Edition – High Performance (EE-HP).

4.4.3 Physical Architecture

Guide:

The solution architecture is typically described in a physical form. This should include all solution components. You do not have to provide solution build or deployment details such as IP addresses.

It is expected to provide a full Multicloud architecture in this section, including all Google Cloud elements which have direct or indirect access to Oracle Database@Google Cloud.

Please describe the solution with an architecture image plus a written text. If you have certain specifics you like to explain, you can also use the Solution Consideration chapter to describe the details there.

The Oracle Cloud Notation, OCI Architecture Diagram Toolkits

Reference:

StarterPacks (use the search)

Example:

Physical Architecture of Production and DR/Standby – same region

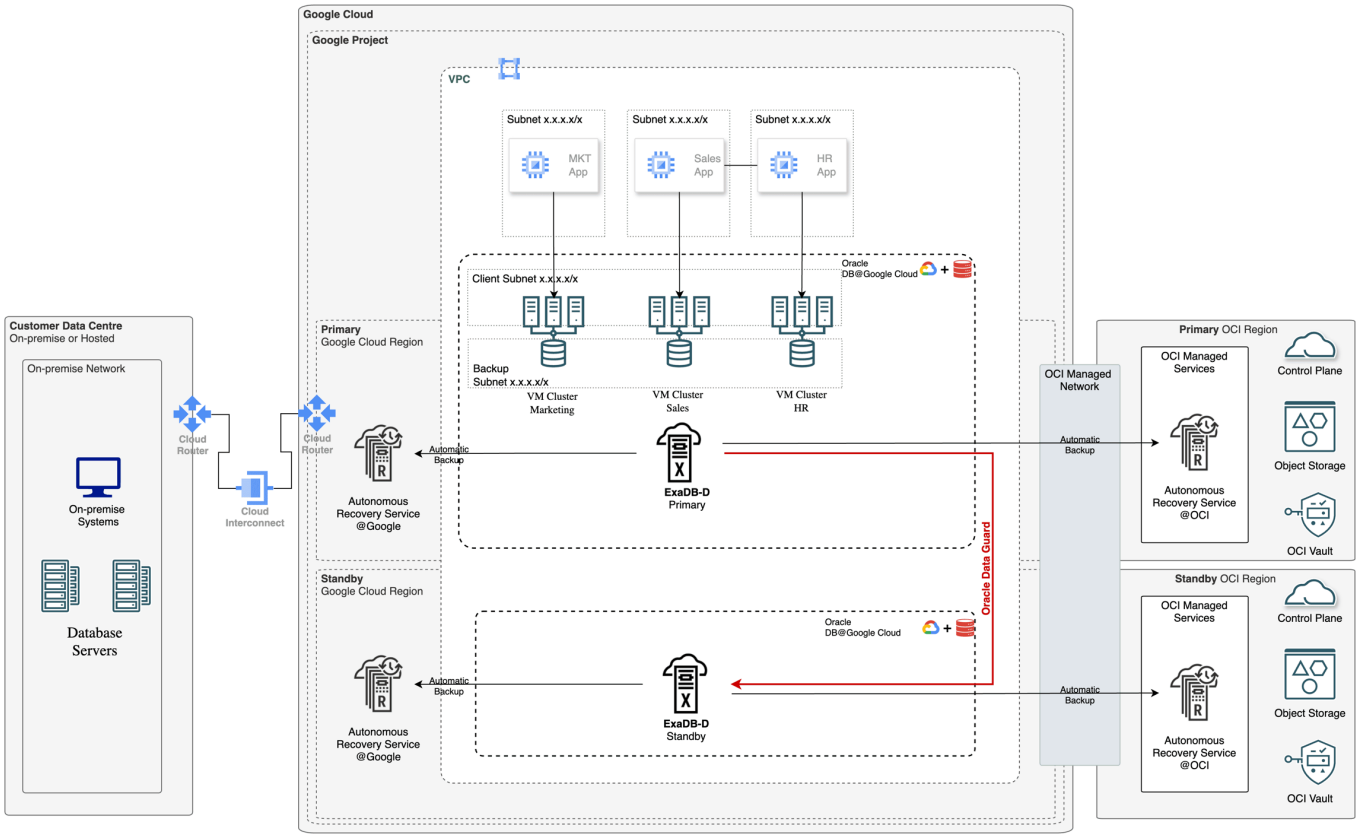
(this feature is not GA yet. Physical architecture will be created and shared later)

---------- Diagram to be mentioned here once the specifics of Single Region DR are clear----------

Physical Architecture of Production and DR/Standby – across regions (ExaDB-D/ExaScale)

Guide:

Please use below diagram and provided example text to write further according to your customer requirements.



DB@Google Physical Across Regions

In this example there are only 3 VM clusters in use to represent three different application DBs. VM Cluster segregation can be based on environment, DB versions, licensing type, security requirements or other attributes as well. When there are multiple workloads across multiple VM clusters, then additionally notes can be made on VM Clusters fulfilling the following requirements:

- Network segmentation due to security:

Each VM Cluster can be placed in its own Google Cloud VPC or OCI Subnet. However this is not mandatory and multiple VM Clusters can co-exist within single VPC and Subnet as long as enough IP Addresses are available. This is what above diagram shows but this can be further enriched with multiple client and backup subnets.

- Workload isolation

  Each VM Cluster have its own dedicated resources in CPU, Memory and Storage Capacity.

- Application / User separation

  Each VM Cluster can have its own users and groups as defined in the Identity Service.

- Required Service Level Objectives (for example MAA Gold, Silver)

  Each VM Cluster is designed against a given MAA Reference Architecture.

High Availability will be granted with Oracle RAC features.

Information on Oracle RAC Best Practices for DB 19c is here: Overview of Oracle RAC and Clusterware Best Practices

Additional information on RAC can be found in the MAA Reference Architectures here: Oracle MAA Reference Architectures

Disaster Recovery capabilities will be granted with Oracle Data Guard. Information on Oracle Data Guard Best Practices for DB 19c is here: Oracle Data Guard Best Practices

Additional information on Data Guard can be found in the MAA Reference Architectures here: Oracle MAA Reference Architectures

In case of unplanned/planned downtime of the production site, an automated or manual mechanism will allow failover/switchover to the other production platform.

Oracle Transparent Data Encryption (TDE) will be used. This is mandatory with ExaDB-D@Google Cloud

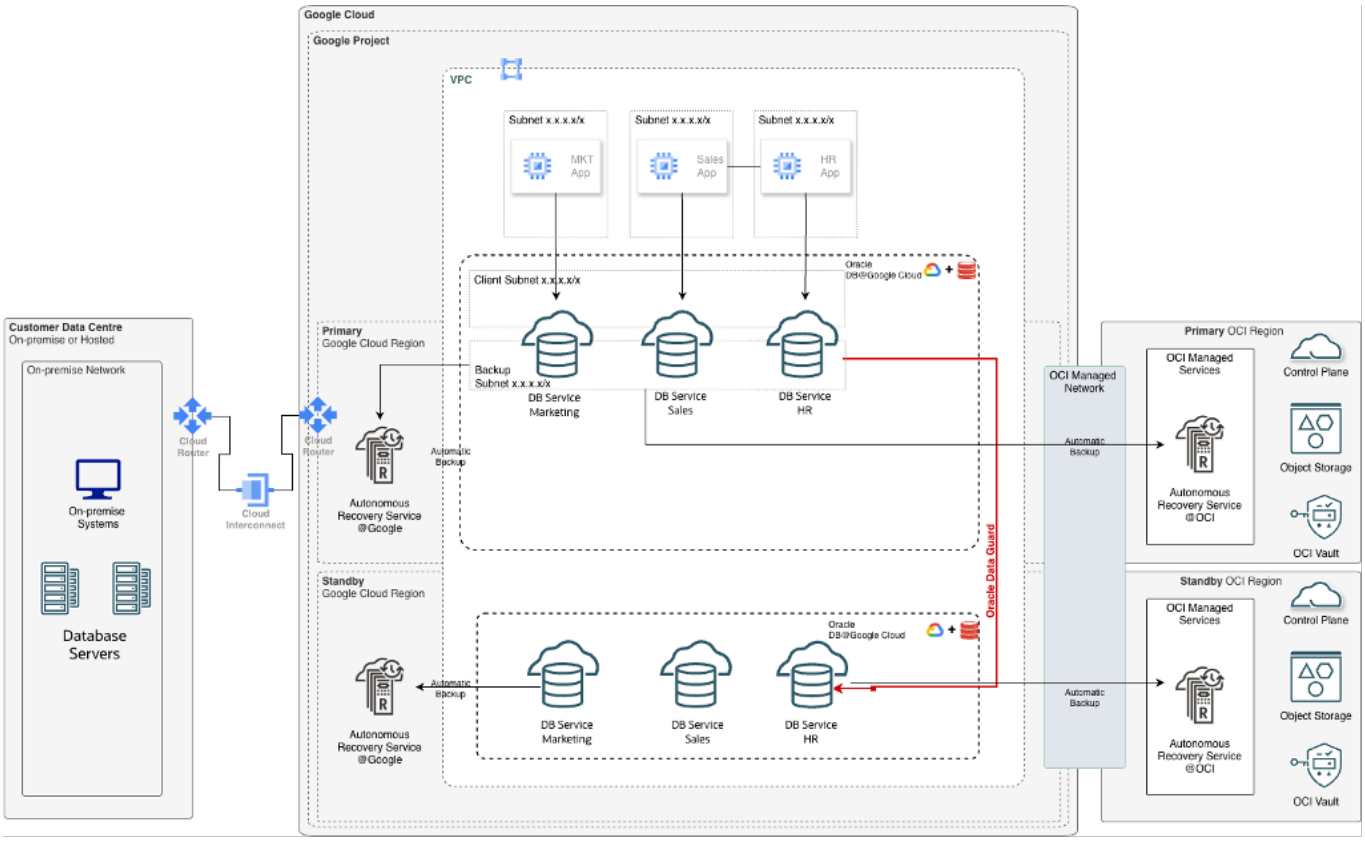
The Control Plane of this ExaDB@Google Cloud is in the local OCI Public Cloud region. The control plane is a sophisticated cloud software suite for order management, subscription billing, identity management, UI and REST API services, network connectivity, security controls, infrastructure and lifecycle management. Oracle Identity and Access Management (optionally federated with Google Cloud IAM), lets you control who has access to your Exadata resources. One can control what type of access a group of users have and to which specific resources.

For data protection all VM Clusters on the same Exadata Infrastructure share the same Backup Subnet.

Physical Architecture of Production and DR/Standby – across regions (BaseDB)

Guide:

Please use below diagram and provided example text to write further according to your customer requirements.



BaseDB@Google Physical Across Regions

In this example, three **Base Database Service** instances are deployed to support three different application databases across two Google Cloud regions (Primary and DR). Each database is deployed as an independent database system with dedicated compute and storage resources.

- Network segmentation due to security:

Each Base Database Service instance is deployed into a **subnet**. Multiple database instances can **coexist within the same subnet**, provided sufficient IP address capacity is available. Separate subnets per environment (e.g., Prod / Non-Prod) are recommended for stronger isolation and simplified firewall policy management. Backup traffic will use a dedicated backup subnet when Autonomous Recovery Service is configured as the backup destination.

- Workload isolation Each Base DB has its own dedicated resources in CPU, Memory and Storage Capacity.
- Application / User separation Each Base DB can have its own users and groups as defined in the Identity Service.

Disaster Recovery capabilities will be granted with Oracle Data Guard. Information on Oracle Data Guard Best Practices for DB 19c is here: Oracle Data Guard Best Practices Additional information on Data Guard can be found in the MAA Reference Architectures here: Oracle MAA Reference Architectures In case of unplanned/planned downtime of the production site, an automated or manual mechanism will allow failover/switchover to the other production platform. The Control Plane of this Base Database Service@Google Cloud is in the local OCI Public Cloud region. The control plane is a sophisticated cloud software suite for order management, subscription billing, identity management, UI and REST API services, network connectivity, security controls, infrastructure and lifecycle management. Oracle Identity and Access Management (optionally federated with Google Cloud IAM), lets you control who has access to your Exadata resources. One can control what type of access a group of users have and to which specific resources.

4.4.4 Key Solution Proposal Components

Example:

Our proposal is based on the following main technical components:

4.4.4.1 Exadata Database Service @Google Cloud (ExaDB@Google Cloud)

Oracle ExaDB@Google Cloud brings the performance, automation, and economics of Exadata Database Service and Autonomous Database fully managed by Oracle to data centers in Google Cloud. This is the easiest way for MYTestCustomer to start using cloud database resources within Google Cloud while continuing their deployment of Google Cloud. ExaDB incorporates unique optimizations that enable databases to run faster with less management and at lower costs, to better leverage MYTestCustomer data.

Value Proposition

Oracle's value proposition to support MYTestCustomer's needs is built around the Oracle ExaDB-D cloud platform:

Resilience and Availability

- Modern, highly available, and secure data architecture by design
- Simplified patch maintenance and proactive threat management
- Through ExaDB@Google Cloud, these services can be used inside an Google Cloud datacenter, natively part of the Google Cloud network.

Performance, agility, and flexibility

- Low latency to keep data as close as possible to applications and choose the timeline for modernizing these databases as needed
- Ability to scale the platform as needs change without increasing complexity
- Maximum availability architecture (e.g. PRA with fast RTO and RPO, service continuity, etc.)
- Obsolescence and risks
- Simplify and standardize to enhance security
- Automation to achieve more predictable service levels and address a wide range of security vulnerabilities Security
- Encryption of all data at rest and in transit.

Speed of implementation / Time to Market

- Time to Market optimization is made possible thanks to the comprehensive ”Infrastructure as Code” approach, which allows all environments to be managed through a DevOps methodology to ensure repeatability.
- Implementation of applications directly and without the need for infrastructure teams, greatly accelerating their implementation and simplifying their maintenance.

Environmental Impact

- Achieving carbon neutrality in 2025
- Reduce CO2 production by 50% in 2030
- Reaching Net Zero in 2050
- Efficiency of Hardware Oracle OCI ExaDB-C@C solutions: 4d eco-design program, certifications, etc.
- Renewable energy use for all global operations by 2025
- End-to-end infrastructure reuse by our engineers: 4d eco-design program, supply chain redesign for delivery and recovery with 99.9% reuse/recycling rate in 2022
- Reduction in the average measured carbon footprint (CSR audit firm) of our customers migrating to our cloud solutions in Europe: 40%
- Align with Sustainable Development Goals
- Aware of climate issues, Oracle has set targets to reduce CO2 production, both internally at the group level and for al of its partners.

Copyright @2024, Oracle and/or its affiliates

4.4.4.2 Exadata Database Service @Google Cloud (BaseDB@Google Cloud)

Oracle Base Database Service is an excellent choice to run single instance Oracle Databases using low-cost general-purpose infrastructure to provide VM compute and network attached storage and running customer's choice of Database editions.

Value Proposition

Oracle's value proposition to support MYTestCustomer's needs is built around the Base DB solution

Performance, agility, and flexibility

Offers consistent and predictable performance for general purpose, business critical enterprise level workloads.

Speed of implementation / Time to Market

- Time to Market optimization is made possible thanks to the comprehensive "Infrastructure as Code" approach, which allows all environments to be managed through a DevOps methodology to ensure repeatability.
- Implementation of applications directly and without the need for infrastructure teams, greatly accelerating their implementation and simplifying their maintenance.

4.5 Solution Considerations

Guide:

Describe certain aspects of your solution in detail. What are the security, resilience, networking, and operations decisions you have taken that are important for your customer?

Typical key considerations are:

- *High Availability and Disaster Recovery*
- *Security*
- *Networking*
- *Manageability and Observability*

Feel free to describe other aspects and important requirements for your customer, and how your solution addresses them in this chapter.

4.5.1 Oracle Database@Google Cloud High Availability and Disaster Recovery

Guide:

Proposed to be HA/DR/MAA design and details

- *Resilience on OCI*
- *Workload Related Content*
- *What happens when site 1 is down?*
- *What happens when XYZ happens?*
- *How is HA achieved?*

Due to the Multicloud nature of the Oracle Database@Google Cloud solution, there can be considerable traffic between Google Cloud and OCI datacenters in Disaster Recovery scenarios. For example:

By default, Oracle Data Guard redo logs are shipped from the primary database to the standby database via the managed Dynamic Routing Gateway (DRG), directing traffic through Google Cloud's network infrastructure.

- *If the standby database is hosted in the same Oracle Database@Google Cloud region:*
    - *Traffic can be routed over Google VPC or through OCI Local Peering Gateway (LPG).*

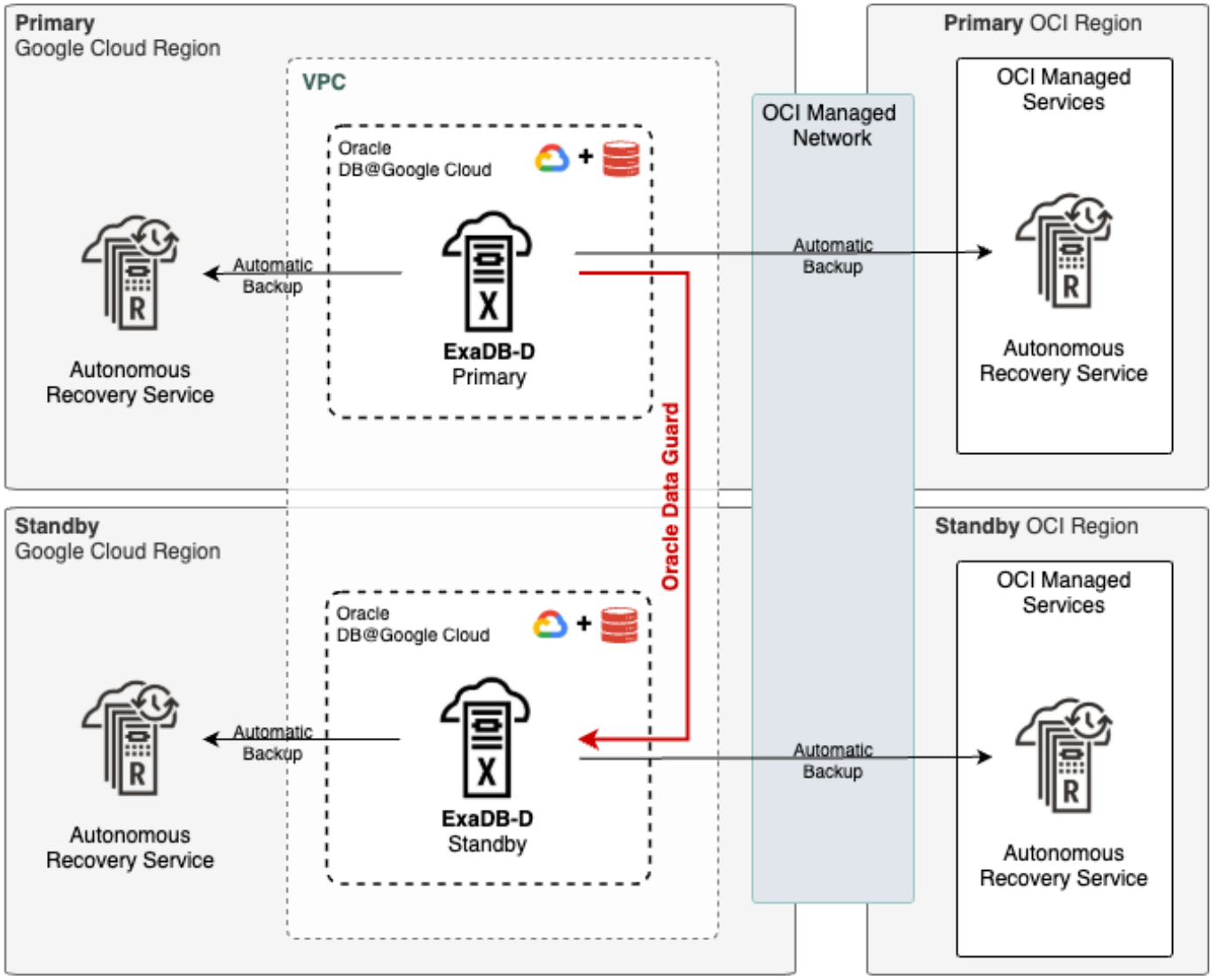
- *If the standby database is hosted in a different Oracle Database@Google Cloud region:*
    - *The preferred path for Data Guard traffic is via Google Cloud's VPC, but can also be routed via Oracle Cloud backbone using the following architecture: https://docs.oracle.com/en/solutions/exadb-dr-on-db-google-cloud/index.html#GUID-041B1ED9-43B8-41C3-90A6-1695668F7DB6 (both options incur cross-region data transfer cost)*

Example:

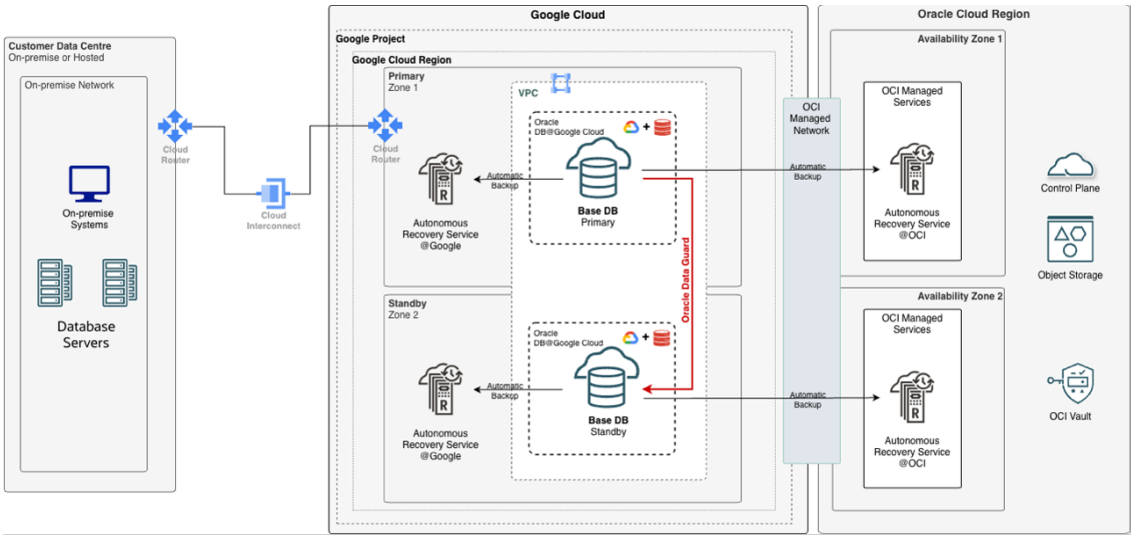
MYTestCustomer requires have a standby in a separate region.

Following has been decided

- Production Databases:
    - Database Service A
    - Full RAC (Only applicable to ExaDB-D/ExaScale)
    - DataGuard with region 1 as primary and region 2 as standby
    - Backups will be done from the local instance to the local backup environment



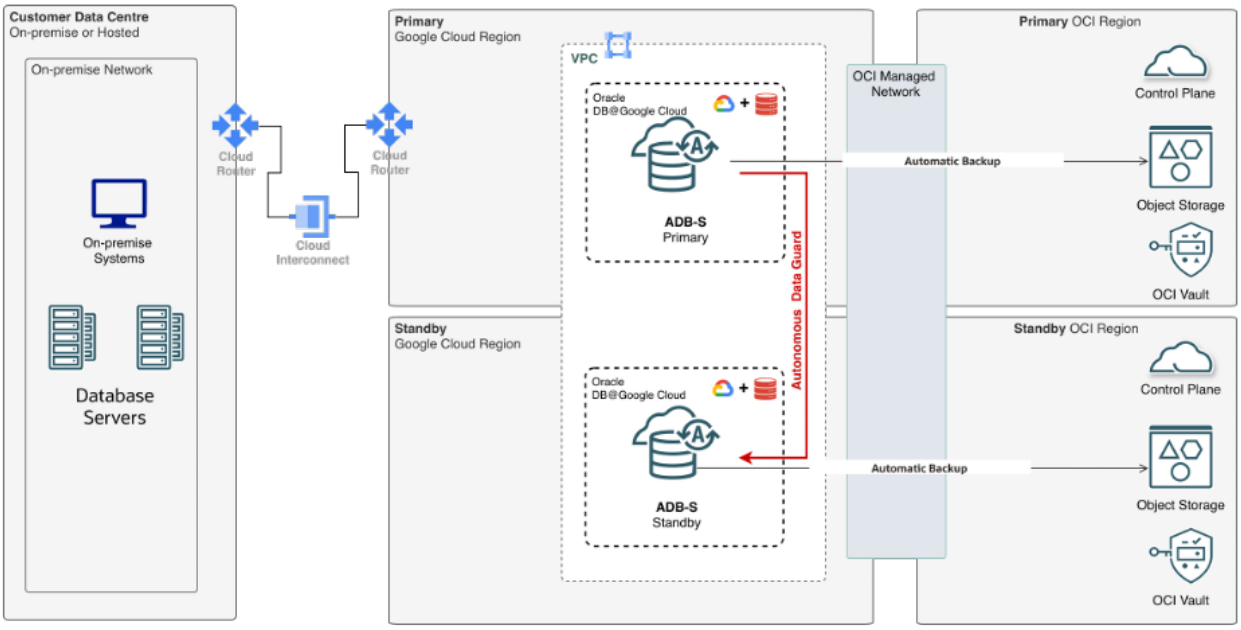
Oracle ExaDB-D@Google Cloud Multi-Region DR with Oracle Data Guard



Oracle BaseDB@Google Cloud Multi-Region DR with Oracle Data Guard

Example Autonomous AI Database:

MYTestCustomer has a requirement for cross region DR using Autonomous Dataguard. Following is the architectural diagram for the same .



Oracle ADB-S@Google Multi-region Autonomous DataGuard

4.5.2 Transparent Application Continuity

Guide:

Please describe the customer specific application continuity requirements in this section. Consider expanding on below mentioned text

Example

Oracle Database@Google fully supports high availability capabilities, including features that enable transparent application continuity such as Fast Application Notification (FAN) and session draining.

- **Fast Application Notification (FAN)** is a high availability mechanism that proactively informs client applications about changes in the status of database services.
- **Draining** allows sessions to be gracefully migrated from one node to another, enabling maintenance activities on the original node without disrupting active workloads.

When these features are properly implemented, along with the necessary configuration adjustments on both the application and client connection side, they can help MYTestCustomer achieve seamless application continuity during planned maintenance operations. It is important to note that while these capabilities are provided at the database level, effective use of draining requires the applications themselves to be correctly configured and parameterized.

In addition, Oracle provides mechanisms to handle unplanned outages through features such as Transparent Application Continuity (TAC) and Application Continuity (AC). These capabilities allow applications to automatically replay in-flight transactions and continue processing without exposing errors to end users. The specific application changes required to leverage these features are outside the direct scope of Oracle support; however, we are available to assist through dedicated awareness sessions.

4.5.3 Security

Guide:

Please describe your solution from a security point of view. Generic security guidelines are in the Annex

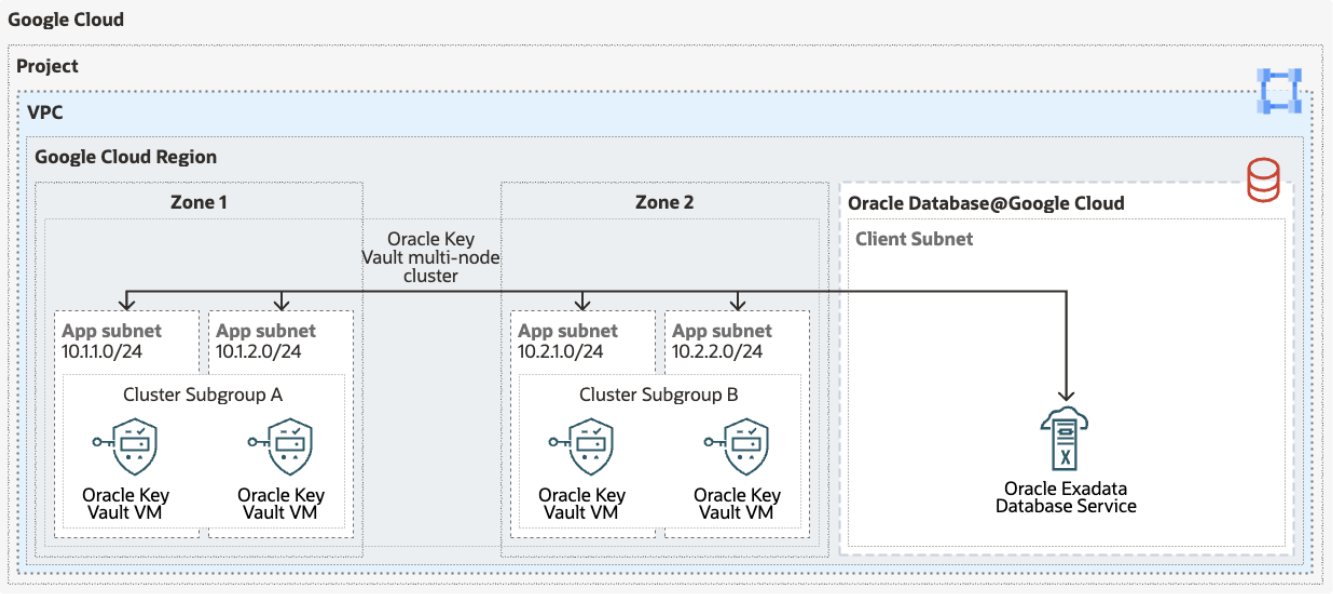
Note that Key Management is always something that needs to be thought of clearly for Oracle Database@Google Cloud Exadata deployments. As per section Security Requirements, if customer-managed keys are required, then Oracle Key Vault is usually the default correct choice. However, if for example keys need to be held in hardware, then OCI Vault should be used.

Example:

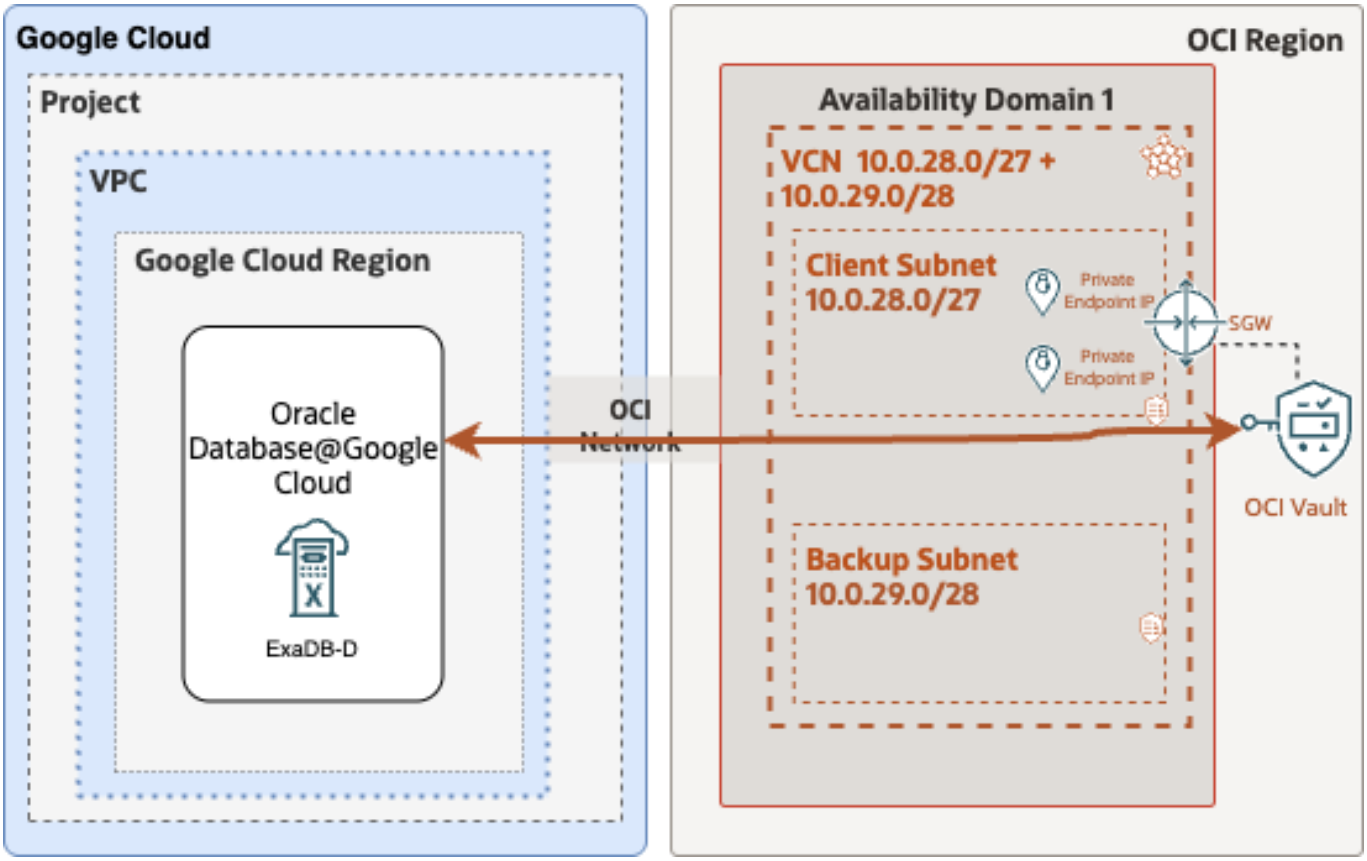
Key management options for Oracle Database@Google Cloud can be based on following options.

Key Management Option	Service	Type	Further Information
Oracle Managed Keys	Oracle managed vault	Default in Exadata Cloud Infrastructure and Autonomous DB	Oracle manages the encryption keys
Customer Managed Keys	OCI Vault (service in OCI, UCM credits needed)	Virtual Vault Multitenant partition	HSM Keys - A master encryption key protected by an HSM is stored on an HSM and cannot be exported from the HSM. All cryptographic operations involving the key also happen on the HSM. These keys are FIPS Level 3 compliant.
Customer Managed Keys	OCI Vault (service in OCI, UCM credits needed)	Private Vault Own partition in HSM, Better and consistent transactions per second for cryptographic operations. Cross Region Replication. Cross Region Back/Restore of Keys	Software Keys - A master encryption key protected by software is stored on a server and can be exported from the server to perform cryptographic operations on the client instead of on the server. While at rest, the software-protected key is encrypted by a root key on the HSM. These keys are FIPS Level 1 compliant.
Customer Managed Keys	Oracle Key Vault (license needed)	Oracle Key Vault running on OCI, Customer on-premise or in Google Cloud VME.	Software on VM, manual installation. Located on Google Cloud, “local” to the database.

Copyright @2024, Oracle and/or its affiliates



Oracle Database@Google Cloud with OKV on Google Cloud VMs



Oracle Database@Google Cloud with OCI Vault

4.5.4 Networking

Example:

Below are standard OCI guidelines and examples for networking. This section also has Database@Google specification to be considered

If your customers have any or one of the needs described in Network Requirements Guidance, then the OCI Network Firewall (OCI NFW) is the cloud native solution that provides all of it.

OCI Network Firewall is based on the industry-leading Nextgen firewall solution by Palo Alto (VM-Series).

Refer to the Annex for more best practices around deployment models.

Networking Example

The OCI Network Firewall can be deployed as a Distributed Network Firewall Model or Transit Network Firewall Model, where the firewall is hosted in the Hub VCN. In general, the OCI Network Firewall can be used to protect North-South traffic (Internet traffic) and/or East-West traffic (internal traffic).

As a best practice, we do recommend using one dedicated OCI Network Firewall instance per type of traffic (North-South and East-West) in separated VCNs. This way performance will be maximized as well as ensuring the network isolation between the types of traffic.

For more information please follow this link.

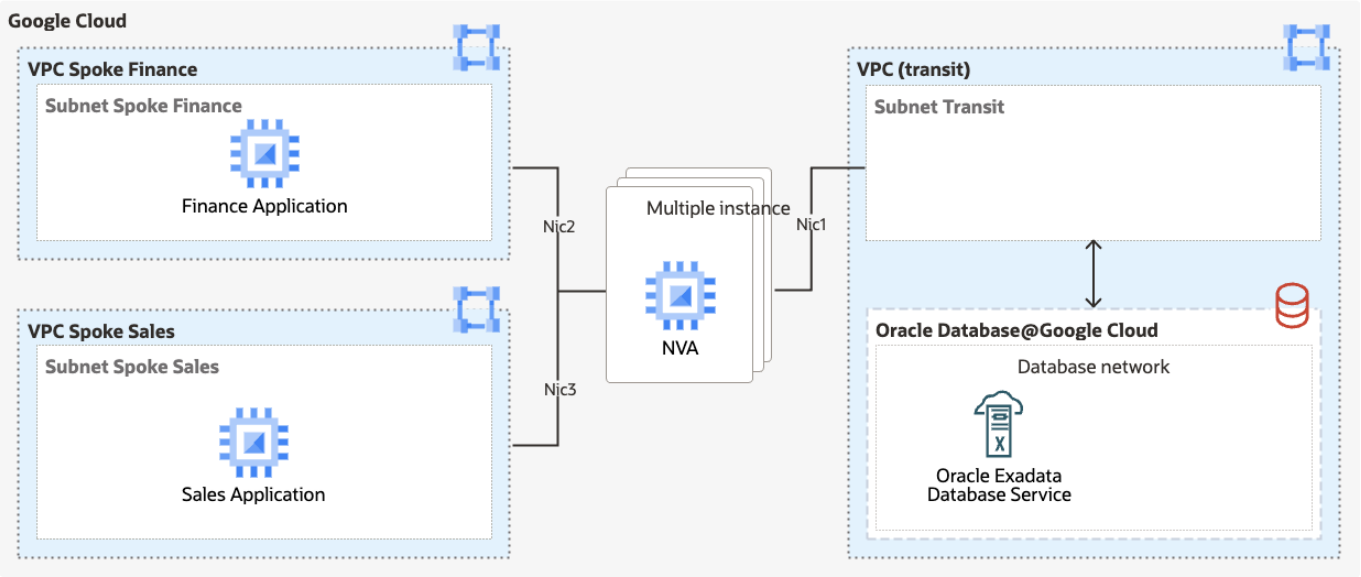
Detailed information about the OCI NFW capabilities with examples can be found in the PDF document below:
Learn OCI Network Firewall in Oracle Cloud Infrastructure with Examples

Guide: Please describe your solution from an Oracle Database@Google networking design point of view.

Example 1:

Hub and Spoke Topology

MYTestCustomer would like to use their existing Hub and Spoke network topology to route all the traffic through their Network Virtual Appliance/Firewall. Applications and DB@Google resources can reside in separate VPCs for increase network isolation and security.

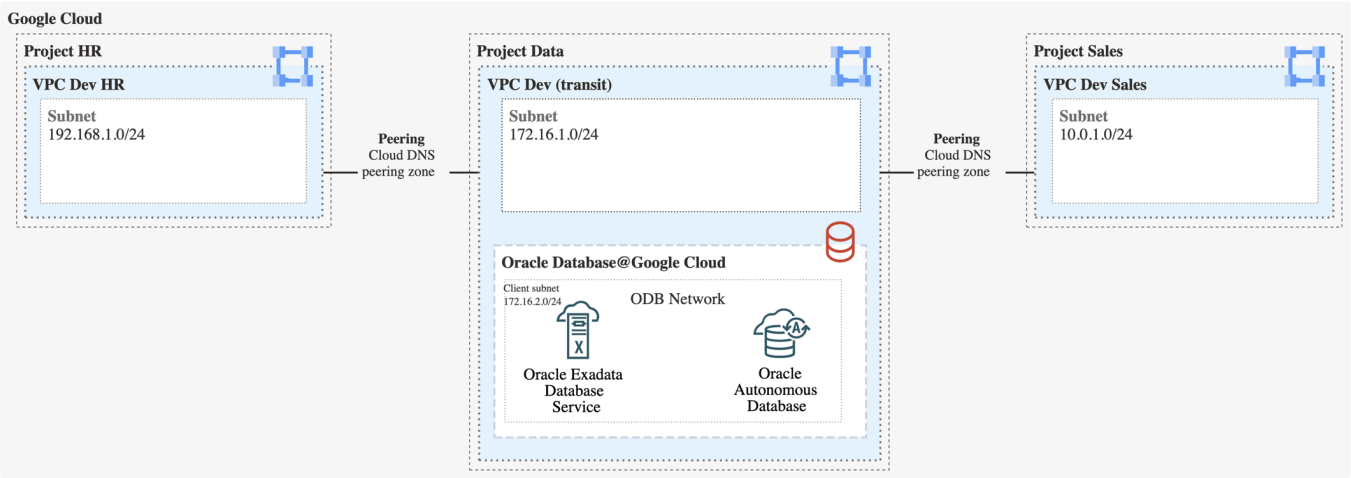


Oracle Database@Google Hub and Spoke Network Topology

Example 2:

Network Peering Topology

VPC peering topology connects your applications in one VPC to the database in another VPC. VPC peering connects two VPCs so that resources in each network can communicate with each other in the same project, a different project of the same organization, or even different projects of different organizations.



Oracle Database@Google Network Peering Topology

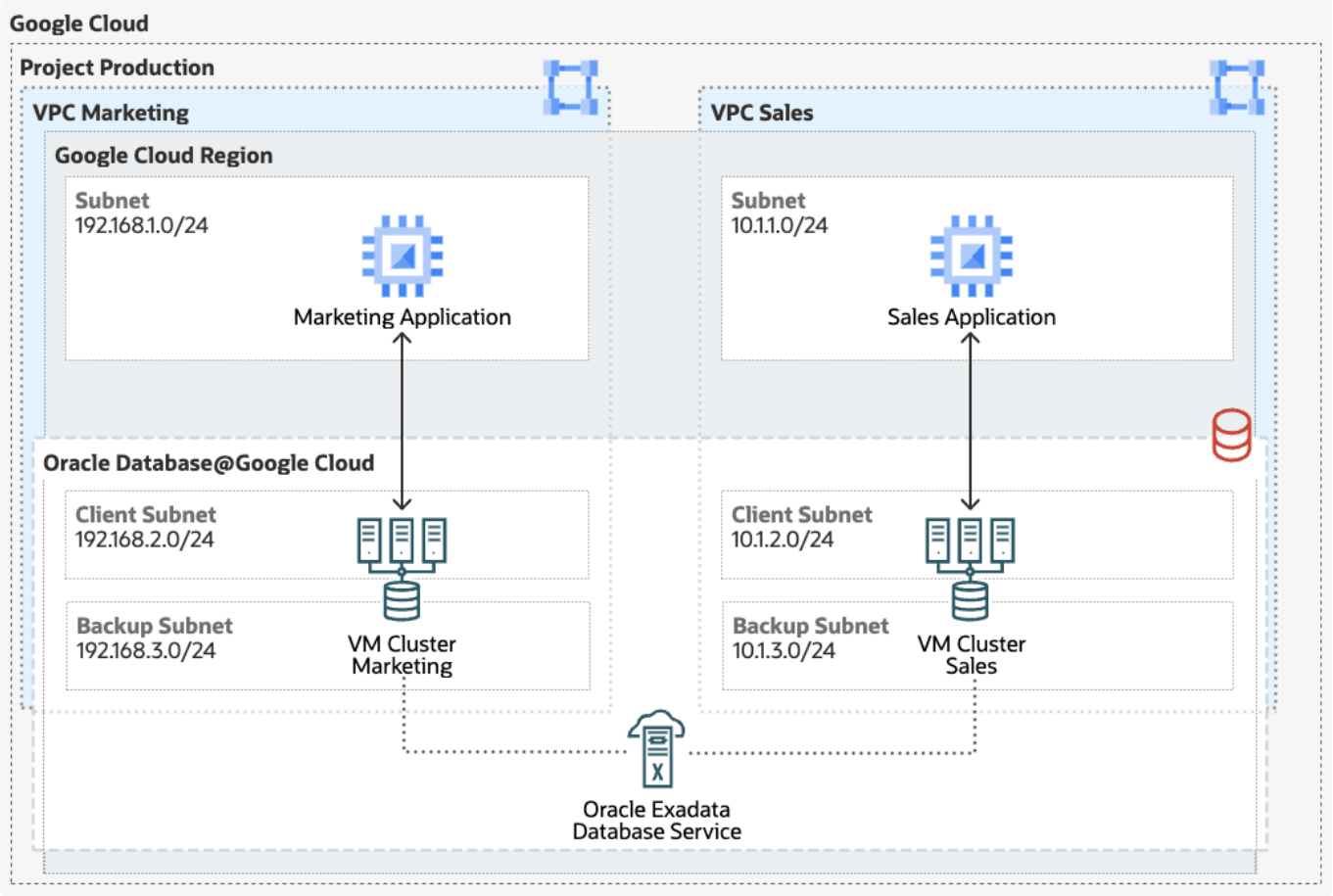
Example 3:

Multiple VPC Topology

If you want to isolate database workloads between two lines of businesses, use the multiple VPC topology. A Sales and Marketing team can have their own VPC and subnets for their databases in a VM Cluster inside an Oracle Exadata Database Service infrastructure.

To isolate workloads on Oracle Exadata Database Service at the VM Cluster level, deploy multiple clusters in isolated VPCs.

Copyright @2024, Oracle and/or its affiliates

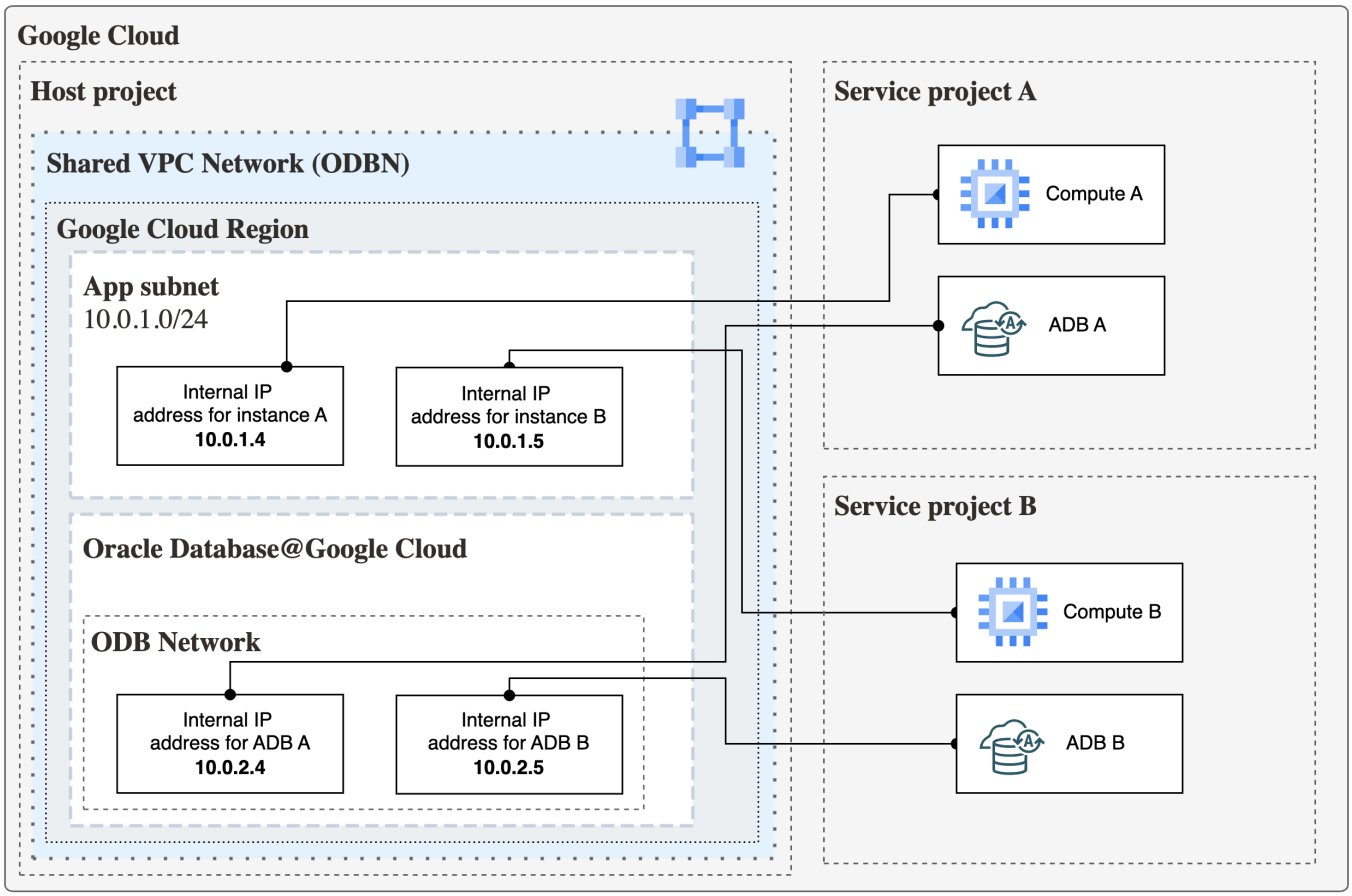


Oracle Database@Google Multiple Networks

Shared VPC Topology

Oracle Database@Google Cloud Network supports Google Cloud's Shared VPC capability. Shared VPCs allow organizations to connect resources from multiple projects to a common Virtual Private Cloud (VPC) network in a Host project. Organization administrators can delegate management of applications to Service Project Administrators while maintaining centralized control over network resources. This simplifies the configuration and allows these resources to communicate securely and efficiently with each other using an internal IP address from the Shared VPC network. Service owners, like database users, use the network configuration defined by their network teams, instead of manually configuring the networks between different resources. It reduces the need to enable and configure VPC Peering and associated configurations.

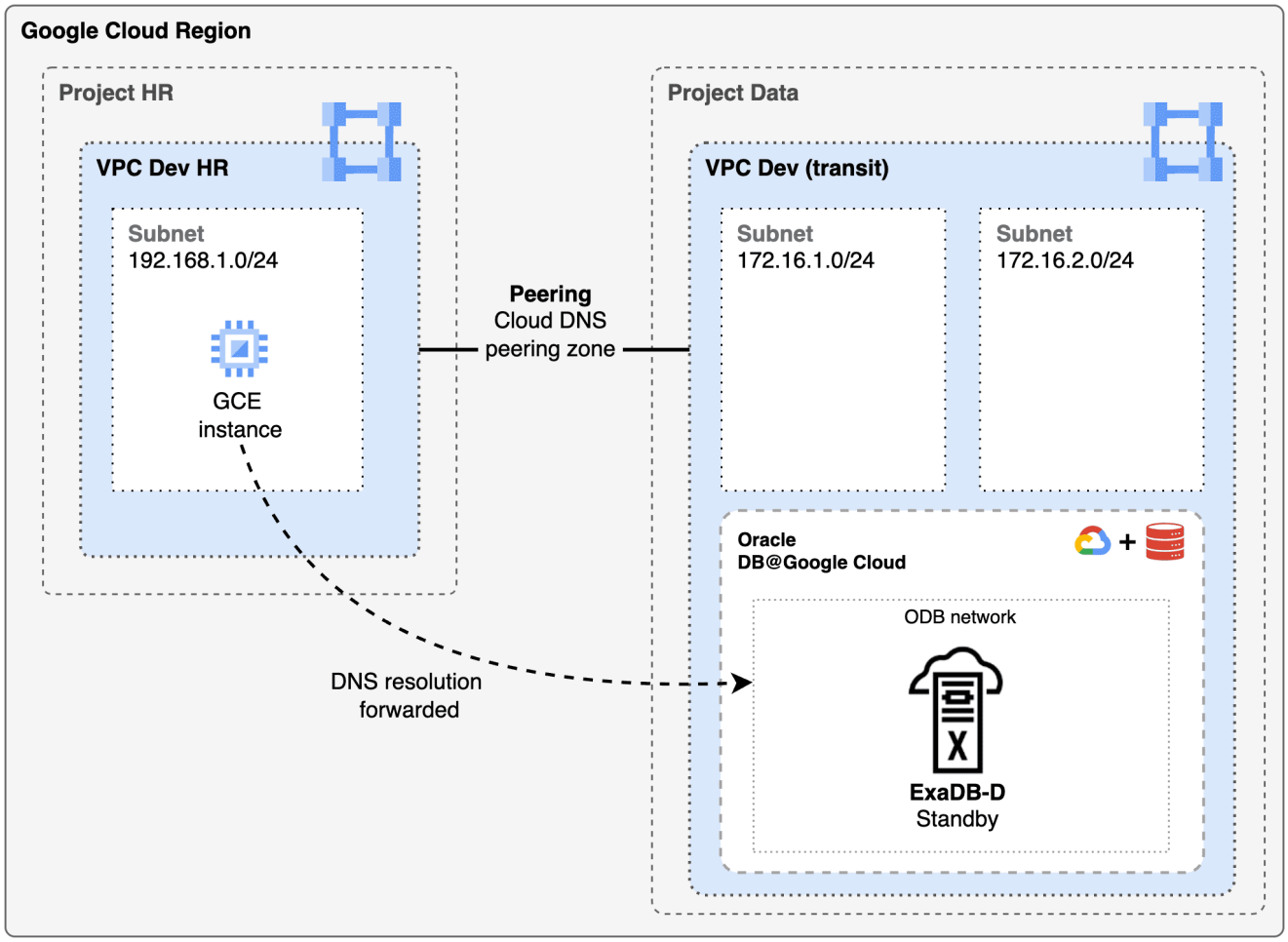
Copyright @2024, Oracle and/or its affiliates



Oracle Database@Google Shared VPC architecture

DNS resolution

In addition to network toplogy for resource placement, describe any requirements with regards to DNS:



Oracle Database@Google DNS

DNS resolution in Google VPC is forwarded to OCI DNS Private Resolver. Configure DNS zone peering to resolve DNS entries in other VPCs.

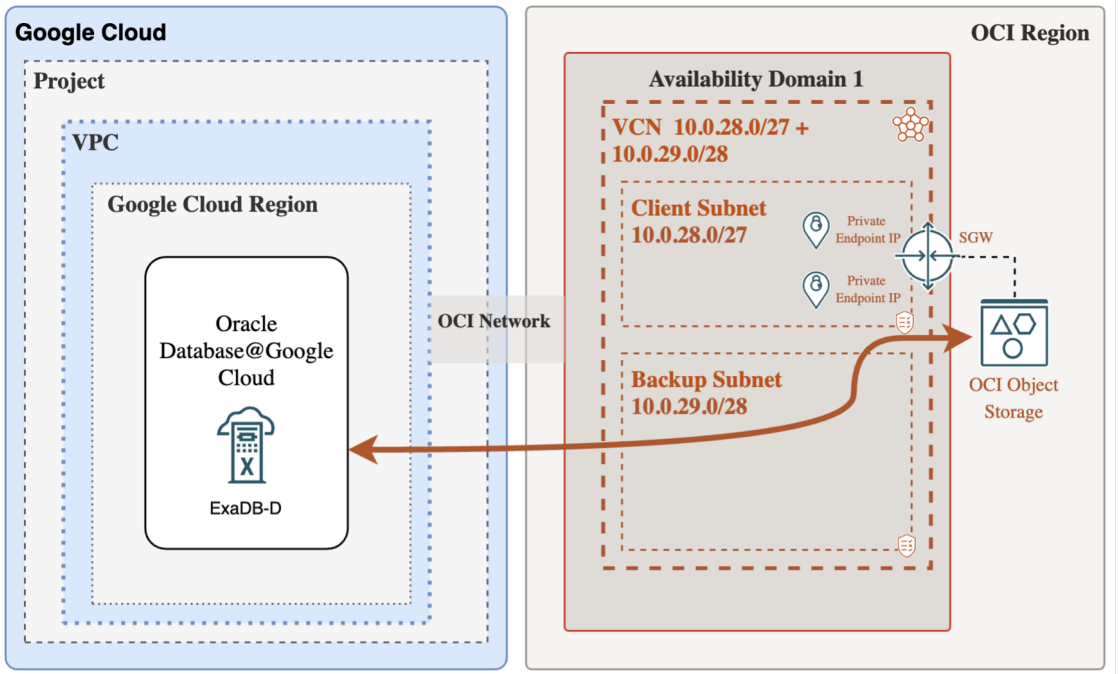
4.5.5 Reliability and Resilience / Backup and Recovery

Some useful links for this topic:

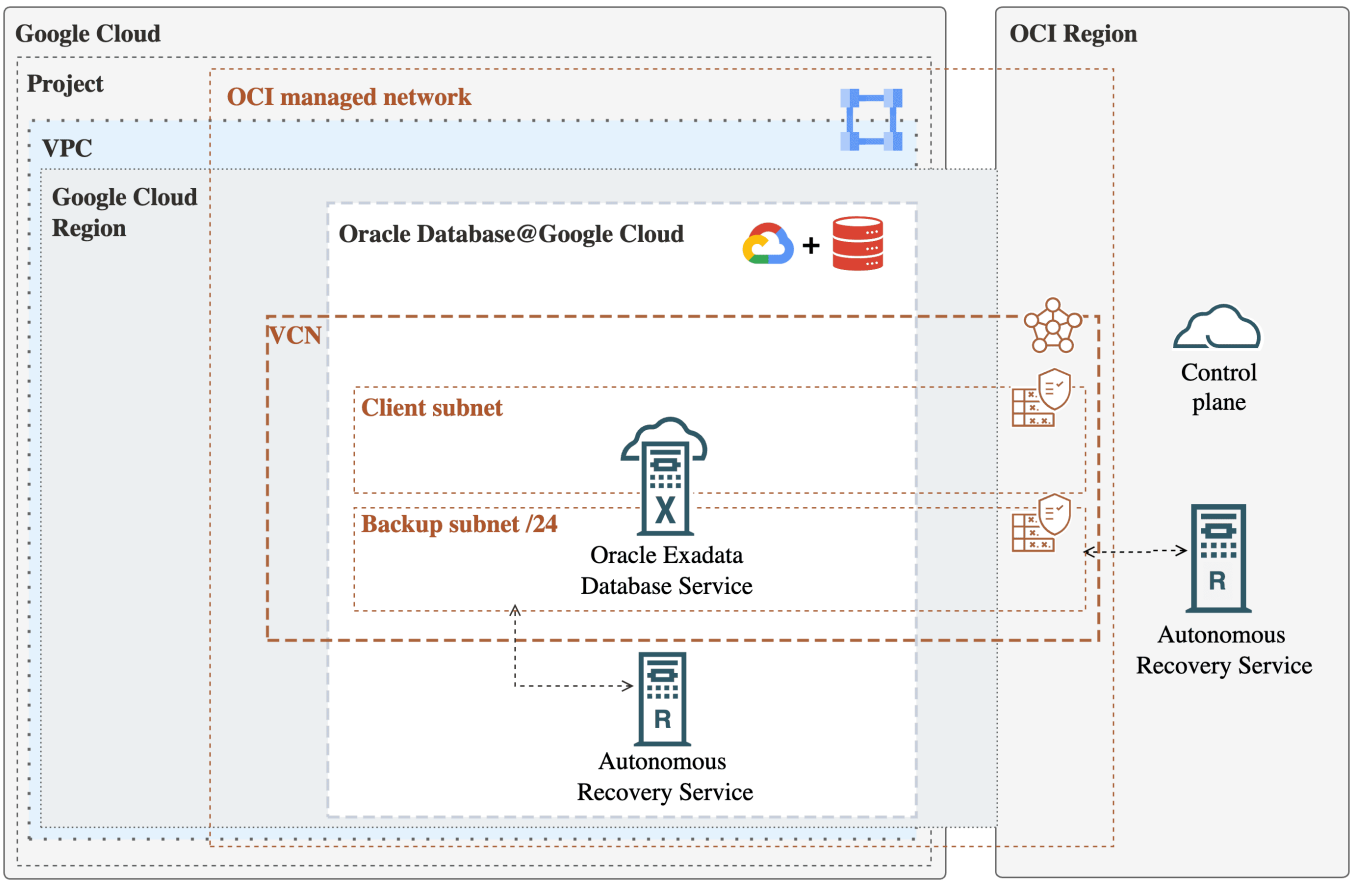
- *Resilience on OCI*
- *Solution Related Content*

Please describe your solution from a backup and recovery design point of view. What should be the backup destination storage – OCI Object Storage or Google Cloud Blob Storage or Any other target Automatic vs Manual backups. The Oracle-recommended backup solution is Zero Data Loss Recovery Service.

Copyright @2024, Oracle and/or its affiliates



Automatic Backup to OCI Object Storage



Automatic Backup to Autonomous Recovery Service (located within OCI region or Google Cloud region)

Copyright @2024, Oracle and/or its affiliates

Backup Option	Info	Retention Period	Backup Destination
Oracle managed backup	Default and recommended		
From OCI cloud tooling	Automatic backup Max 60 days retention		
Standalone backup = until deleted	OCI Object storage (Oracle Managed) Charged from Google Cloud credits		
User configured backup	Configure backups from the host using the dbaascli database backup and dbaascli database recover commands.	Defined by customer	OCI Object storage (Customer managed)
Charged from OCI credits			
Autonomous Recovery Service (recommended)	Recovery Service is the recommended option for backups with ExaDB	Retention period can be defined by customer. Long-term backups are available for up to 10 years	OCI region or Google Cloud region
Manual setup	RMAN (Recovery Manager) or other backup tools can be configured to do backup to Google Cloud Blob Storage or OCI Object storage	Defined by customer	To Google Cloud Blob storage or OCI Object storage
Charged from respective CSP			

4.5.6 Monitoring

Guide:

Please describe your solution for monitoring options

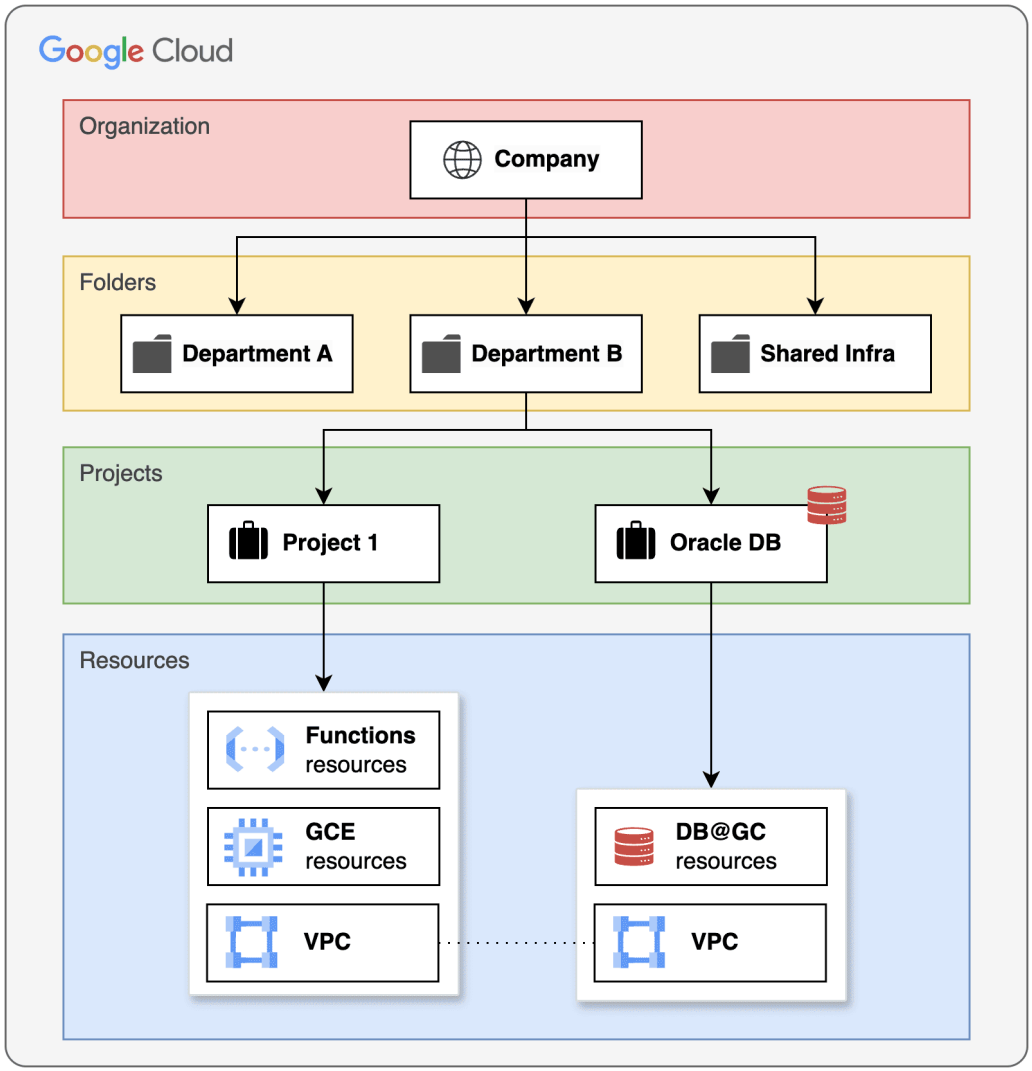
- *Google Cloud Log Analytics*
- *Google Cloud Application Insight*
- *Oracle Enterprise Manager*
- *OCI Database Management Service*
- *OCI Observability*
- *3rd party tools (Splunk etc)*

4.5.7 Governance

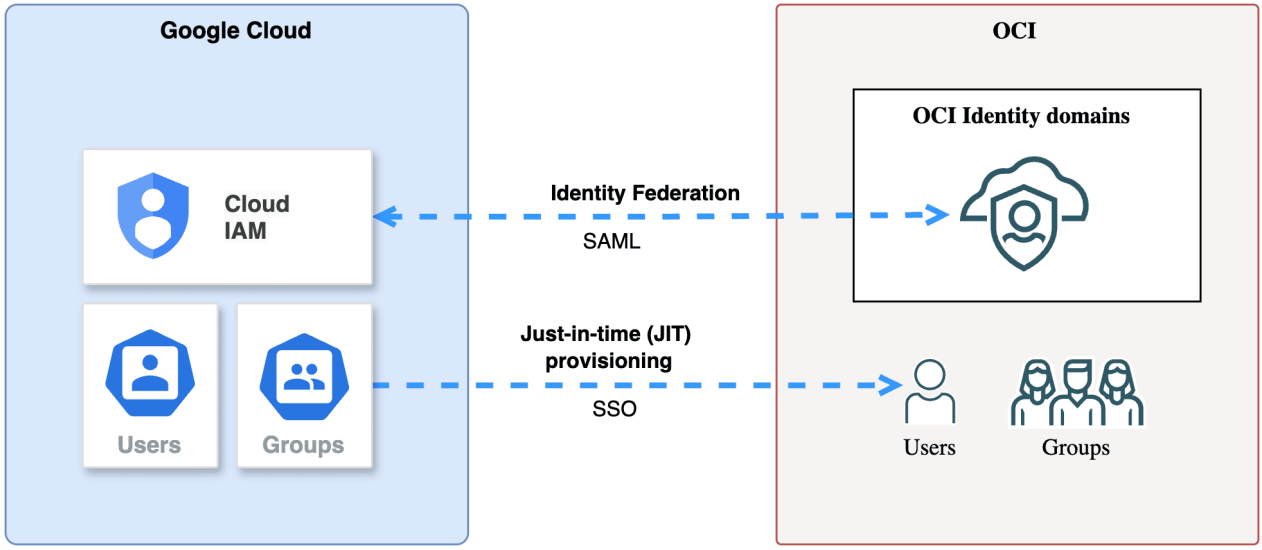
Guide:

Please describe your Oracle Database@Google solutions' governance model

Copyright @2024, Oracle and/or its affiliates



Oracle Database@Google Governance Model



Oracle Database@Google Cloud Identity Federation

4.5.8 Manageability and Observability

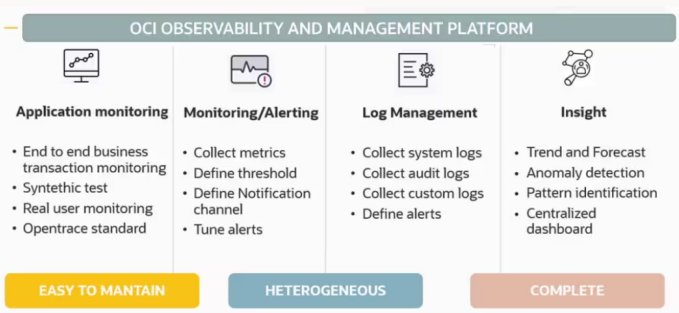
The example below is the original OCI SDD Template text. For Oracle Database@Google Cloud customers who want to leverage (parts of) OCI Observability and Monitoring, use the relevant sections of that text. For Oracle Database@Google Cloud customers who want to include other forms of monitoring, describe those here if relevant.

Example:

Observability is a technology advancement focused on getting insights from a vast array of data, logs, and events generated within an IT environment. By implementing an Observability strategy, organizations gain the capability to anticipate system disruptions, prevent resource overconsumption, and enhance the overall application user satisfaction. That means being proactive, which is a must, especially in a distributed environment.

Gone are the days when the IT landscape remained a mysterious black box. The company's digitalization and the Cloud model compel C-level executives to gain comprehensive insights into asset utilization. The efficient allocation of resources directly influences budgetary considerations.

Observability helps organizations examine how well their infrastructure is working, predict future needs, and help take proactive steps to improve efficiency and protect investments. Therefore, Observability tools are needed to cover these important areas.

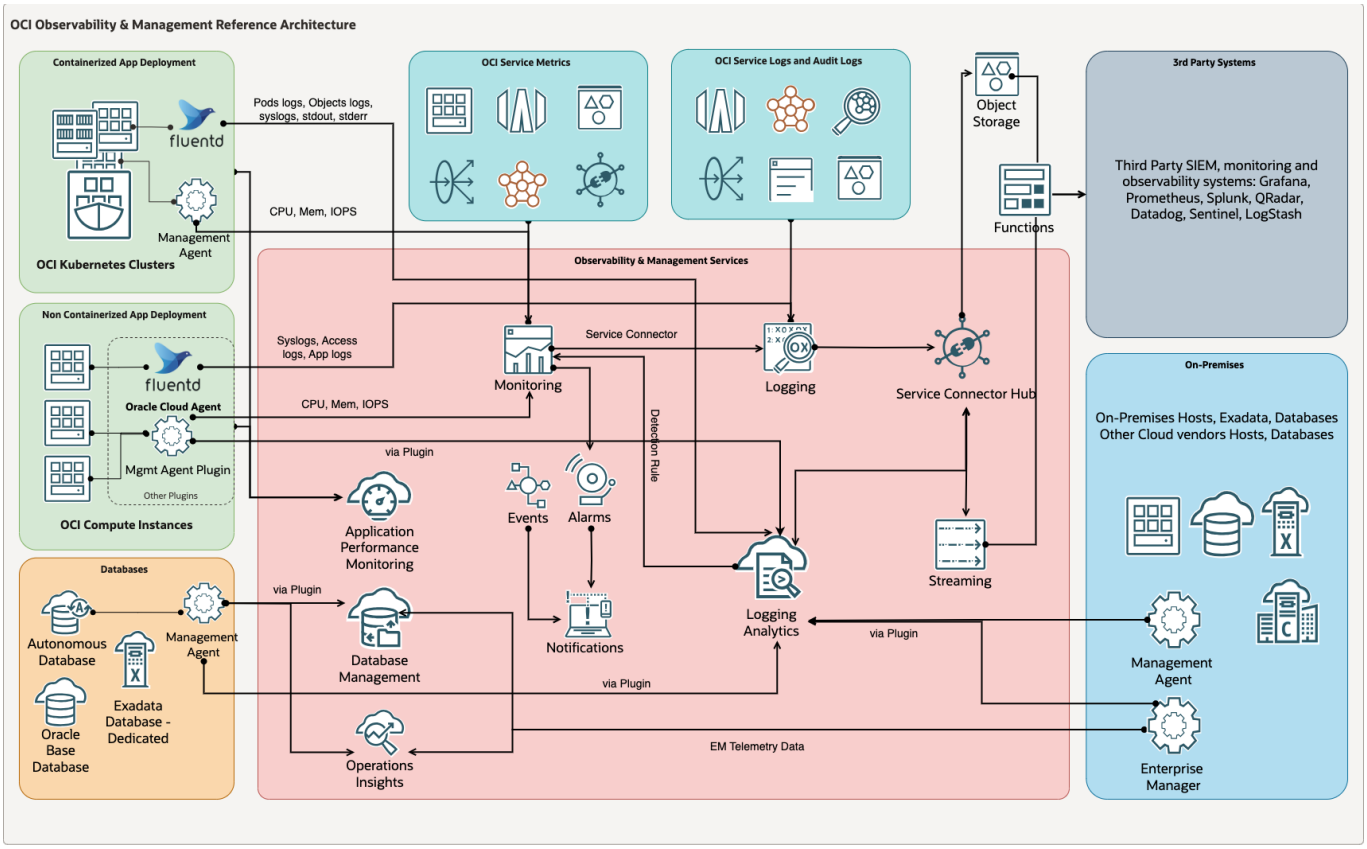


Observability and Manageability

4.5.8.1 Observability Architecture

The basic monitoring OCI services collect the data and send logs and metrics to OCI Monitoring and Logging services. If you want to apply machine-learning capabilities and perform analysis, you can send the data to the Logging Analytics service. If you want to use OCI Logging Analytics to collect logs coming from both on-premises and cloud sources to analyze them for auditing, security purposes, or to integrate data with an external SIEM solution, the Connector Hub serves as the solution.

It's advisable to plan your monitoring strategy by considering both the O&M (Observability and Management) native service of OCI and its integration with third-party tools, as O&M is flexible and a highly customizable solution.



OCI Architecture

4.5.8.2 Real-Time Monitoring

Real-time monitoring is the delivery of continuously updated data about systems, processes, or events. Such monitoring provides information streaming at zero or low latency, so there is minimal delay between data collection and analysis. It enables quick detection of anomalies, performance issues, and critical events.

Please find all references for this chapter in the Annex.

4.5.8.3 Performance and Tuning

Performance tuning is the improvement of system performance. It can be done proactively to prevent issues or reactively in response to increased workload, which is crucial for avoiding system outages.

Please find all references for this chapter in the Annex.

4.5.8.4 Administration

Administrator tasks involve upholding a data management policy and ensuring essential equipment functionality, such as instance management, backup & restore operations, key management, and allocating resources from the database to the storage.

Please find all references for this chapter in the Annex.

4.5.8.5 Troubleshooting

Issues can happen on several levels. To identify the root cause, it is important to be able to correlate resources, drill down into the issues, and analyze trends in the systems. It's crucial to consider that the application itself might be the root cause of the issue. Therefore, it's essential to gather information about the application's behavior and performance to fully understand the problem and resolve it effectively. Troubleshooting also allows you to avoid an outage which is why it is important to notice issues as early as possible.

Please find all references for this chapter in the Annex.

4.5.8.6 Cost Control and Chargeback

Cost control is the practice of identifying and reducing business expenses to increase profits. It starts with the budgeting process. Cost control is an important factor in maintaining and growing profitability.

IT chargeback can provide greater visibility into the costs of IT services and infrastructure usage. It enables organizations to identify opportunities for cost optimization and reduce wasteful spending.

Cost control and chargeback are critical concerns, especially for companies transitioning to the cloud, presenting new financial operational challenges (FinOps). In this context, reducing consumption directly impacts the company's business.

Please find all references for this chapter in the Annex.

4.5.9 Oracle Database@Google Cloud Operating Model

Guide:

This section captures requirements on how the system will be managed after implementation and migration. Reference can be made to the normal "Explanation of Cloud Operations Service" for ExaDB in MOS Note 2875973.1. The split between Oracle and customer responsibility is the same for ExaDB running within Google Cloud as it is for ExaDB in OCI.

Example:

MYTestCustomer's full Google Cloud estate, including Oracle Database@Google Cloud is managed fully by . For the management of the Exadata Database Service on Dedicated Infrastructure there is a split between Oracle responsibility and Customer/Partner responsibility, as described in "Explanation of Cloud Operations Service" for ExaDB in MOS Note 2875973.1.

In short Oracle owns and is responsible for managing the infrastructure layer, and the customer/partner manages the layers on top of that (VMs, Databases, including access to these).

For an overview of responsibilities between Google Cloud, Oracle and the end customer, see section "Roles and Responsibilities for Oracle Database@Google Cloud" of the document Exadata Database Service on Dedicated Infrastructure Security Controls.

For incident management, Oracle Cloud Support is the first line of support for all Oracle Database@Google Cloud and questions. Detailed information on Oracle and Google Cloud support responsibilities are available here.

4.6 Sizing and Bill of Materials

Guide:

Estimate and size the physically needed resources of the solution. The information can be collected and is based upon previously gathered capacities, business user numbers, integration points, or translated existing on-premises resources. The sizing is possibly done with or even without a Physical Architecture. It is okay to make assumptions and to clearly state them!

Clarify with sales your assumptions and your sizing. Get your sales to finalize the BoM with discounts or other sales calculations. Review the final BoM and ensure the sales are using the correct product SKUs / Part Number.

Even if the BoM and sizing were done with the help of Excel between the different teams, ensure that this chapter includes or links to the final BoM as well.

Example:

4.6.1 Bill of Materials scope

This section covers only the Oracle Database@Google Cloud elements, and any additional OCI elements. It does not contain any Google Cloud services or components.

4.6.2 Collected Data for Sizing

Guide:

With OCCA Oracle Cloud Capacity Analytics the data collection comes from Oracle Enterprise Manager, AWR (Automatic Workload Repository) and/or is manually added.

Customer data is gathered with a script provided by Oracle with clear instructions on how to execute. It's customer responsibility to run the extract script and optionally obfuscate the data and then upload the output to Oracle using secure methods.

The output needs a first validation, where any anomalies in the data collection, such as errors, missing data, unrealistic outliers/deviations or unexpected growth can be identified.

This data is then grouped in Cohorts which are in the context of sizing grouping of databases together for the purpose of being deployed in VM Clusters. In the sizing process customer define Cohorts/VM Clusters for each database taking the following into consideration:

- *Network segmentation due to security*
- *Workload isolation*
- *Application / User separation*
- *Required Service levels (for example MAA Gold, Silver, Bronze)*
- *Size of the workload*
- *Physical Location*

Copyright @2024, Oracle and/or its affiliates

	Cohort	Database Name	Allocated Database Size (GB)	Total Database Size (GB)	Use Values from Database No
2	non-Prod B	oracle_database-00000			
3	non-Prod C	oracle_database-00001			
4		oracle_database-00002			
5	Prod A Primary	oracle_database-00003			
6	Prod A Standby	oracle_database-00004			
7	Prod A Primary	oracle_database-00005			
8	Prod A Standby	oracle_database-00006			
9	Prod A Standby	oracle_database-00007			
46	non-Prod B	oracle_database-00044			
47	non-Prod B	oracle_database-00045			
48	non-Prod C	oracle_database-00046			
49	non-Prod B	oracle_database-00047			
50	non-Prod C	oracle_database-00048			
51	Misc D	oracle_database-00049			
52	Misc D	oracle_database-00050			
53	Misc D	oracle_database-00051			

Oracle Database@Google Sizing Scope

Document the scope, manual additions, corrections and/or assumptions made related to the anomalies.

Example:

The scope that has been studied considers all the Oracle databases within the customer. This scope includes both Oracle Databases hosted on on-premise Exadata Infrastructures and Oracle Databases on legacy infrastructure (VMWare).

To complete the study, Oracle provided customer with scripts to capture the activity of the Oracle databases included in this scope. However, the activity of a number of databases could not be recovered. For these databases, we relied on assumptions shared by customer.

Oracle Database@Google Sizing Graph

The data collection showed vCPU growth from August 2024 to September 2024 was higher than expected and because of that checked with and confirmed by customer. This will result in adjusted sizing values for OCPU.

4.6.3 Defined VM Clusters for Sizing

Guide:

Cohorts in the context of sizing are grouping databases together for the purpose of being deployed in VM Clusters. In the sizing process customer define Cohorts/VM Clusters for each database taking the following into consideration:

- *Network segmentation due to security*
- *Workload isolation*
- *Application / User separation*
- *Required Service levels (for example MAA Gold, Silver, Bronze)*
- *Size of the workload*
- *Physical Location*

Document the VM Clusters that has been agreed with the customer and any assumptions made. If you have a more complex VM Cluster layout with VM Cluster Node Subsetting, then consider visualizing it.

Example:

Based on the customers' different requirements for Production and non-Production environments which include different service levels as well as separate Client network segments for the environments, the following Cohorts (VM Clusters) have been defined.

Each VM cluster runs a single version of the Oracle Grid infrastructure (GI) to be chosen by the customer among the most recent. Each cluster can run different versions of Oracle Homes. Each independent VM cluster has OCPU assigned during the deploy phase of the VM cluster, so, we can assign different number of OCPU to different VM clusters and environments.

VM Clusters to be deployed are listed in the following tables together with the criteria that define why separate VM Clusters are deployed.

VM Clusters	Environment	VNet	MAA Service Level
Production A Primary	Production	DBVNetProd	Gold
Non-Production B	Test	DBVNetNonProd	Silver
Miscellaneus D	Test	DBVNetMisc	Silver

An ExaDB-D@OCI X9M Quarter Rack (with two DB Servers) can host up to X independent VM Clusters, the maximum number of VM Clusters is Y for X9M systems with more than 2 database servers. The maximum number of VMs per database server is Z regardless of the number of database servers in the system.

Documentation on in ExaDB@Google Cloud is available here

4.6.4 Sizing Analysis

Guide:

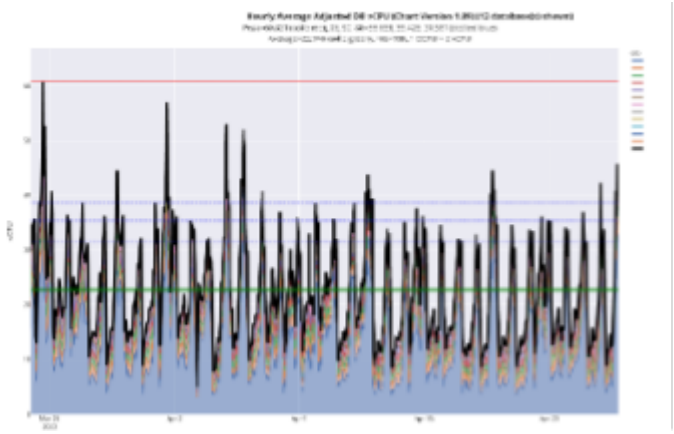
Each VM Cluster is sized independently using Time-Aligned Peak Sizing with adjustments made for historical deviations and finally all VM Clusters are combined per ExaDB-D rack.

Values of interest include:

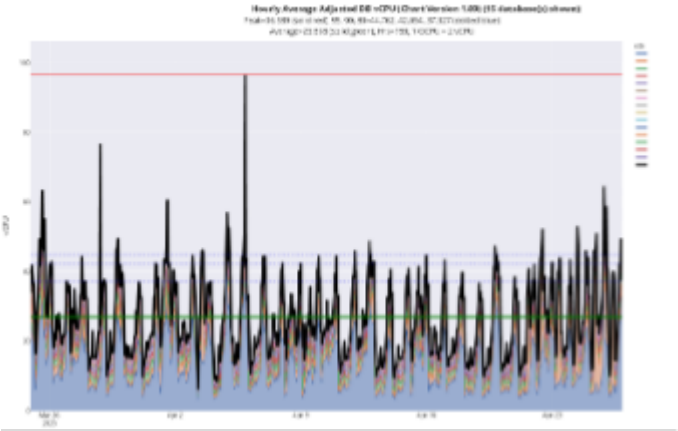
- *OCPU Peak*
- *OCPU 95th Percentile*
- *DB Memory*
- *Allocated and Uses Storage*
- *IOPS Read and Write*

Copyright @2024, Oracle and/or its affiliates

Document the summary from the Sizing Summary for customer reference. Example: These are the time aligned plots for the two production VM Clusters of Database Service A (Primary + Standby).



Oracle Database@Google Sizing Graph



Oracle Database@Google Sizing Graph

4.6.5 Sizing Assumptions

Guide:

Document the customer requirements that is included in the sizing as well as assumptions made for the sizing.

Example:

The following customer requirements and general assumptions have been used in the sizing.

- All analyses are based on previous resource consumption and does not necessarily predict the future workload behavior.
- The defined cohorts (VM Clusters) and databases can differ from the current deployment.
- The sizing computations are based on the hourly average resource consumption of databases in each cohort.
- Cohort metrics are aligned by time and then the sum of peaks is computed for each hour.
- Hourly data is adjusted based on peaks found in the daily data over the past year (valid for EM data case).
- Using in-memory or other database options may reduce/increase the required processing power.
- Using different execution plans will influence the required processing power.

Copyright @2024, Oracle and/or its affiliates

- All Prod DBs will have DR. 5% YoY growth was considered for a period of 4 years (corresponding system shape was selected).
- 10% additional overhead has been considered for converting standalone DBs to RAC.
- For each VM Cluster, an additional 4 OCPUs were added for OS+GI. Metrics for DR DBs were considered as 20% of the corresponding Primary DBs

4.6.6 Proposed Hardware Shapes

Guide:

Document the proposed hardware shape and any additions, corrections or customer requested changes made.

Example:

The sizing shows that ExaDB@Google Cloud X9M Quarter Rack will fulfill requirements, but due to heavy use of CLOB in some Production Databases the customer requests to add an additional ExaDB@Google Cloud X9M Storage Server to each system. This is referred to as an Elastic Configuration.

4.6.7 Licensing models and Elastic Expansion of Exadata on Oracle Database@Google Cloud

Guide:

Fully elastic expansion of Exadata on Oracle Database@Google Cloud, allows customers to provision the database compute and storage resources for any workload and provides the scale for any size database DB Systems.

Exadata on Oracle Database@Google Cloud provides Multi-VM-Clustering and Node-Subsetting capabilities to provide workload segregation and resource isolation on a single Oracle Database@Google Cloud infrastructure. The features are as follows:

- *Provision VM-cluster on a Subset of DB servers
- *Expand an Existing VM Cluster by Adding VMs
- *Shrink an Existing VM Cluster by Removing VMs

Oracle Database@Google Cloud offers elastic infrastructure shapes to support workloads of different sizes. Customers can deploy flexible shapes that range from a Quarter Rack, 2 database and 3 storage servers, up to 32 database and 64 storage servers to meet a variety of CPU processing and storage requirements. Hence making it a perfect solution to consolidate on.

There are two licensing models:

1. Bring your own license (BYOL). Customer is only allowed to use the existing option licensed for.
2. License included. This includes all RDBMS options.

The available editions for BaseDB@Google are

- Oracle Database Standard Edition 2
- Oracle Database Enterprise Edition (EE)
- Oracle Database Enterprise Edition – High Performance (EE-HP)

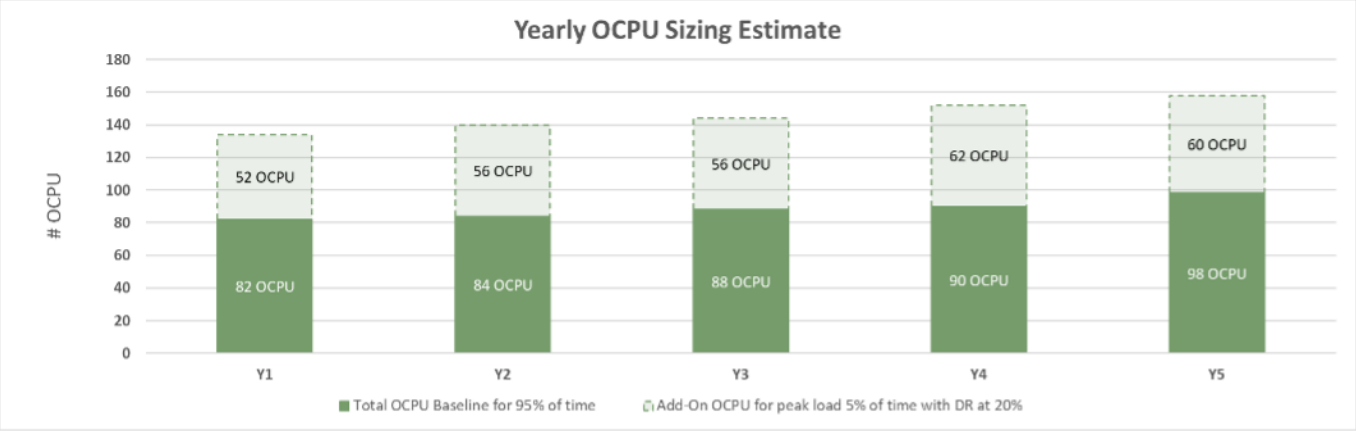
License Included pricing incorporates the database license cost into the hourly ECPU rate.

The licensing model is set at Virtual Cluster level and can be changes at any point during the duration of the subscription. This is very effective in scenarios where more licenses are required due to the scope growth of the project and/or customer has a desire not to maintain on-premises licenses.

Example:

This is the proposed Consumption Plan over five years based on the sizing, growth and other assumptions.

Copyright @2024, Oracle and/or its affiliates



Oracle Database@Google Sizing Estimate

4.6.8 Exadata Database@Google Cloud Bill of Materials

Product	Metric	Qty
B93380 - Exadata Cloud Infrastructure - Quarter Rack - X9M	N/A	2
B88592 – OCI - Database Exadata OCPU	OCPU BYOL	152
B91627 - Object Storage - Requests#[0-5]	10,000 Requests per Month (first 50,000 free)	1
B91628 - Object Storage - Storage#[10-999999999]	Gigabyte Storage Capacity Per Month	1000

4.6.9 Base Database@Google Cloud Bill of Materials

Product	Metric	Qty
B111584 – Oracle Base Database Service - Database Storage	Gigabyte (GB) Storage Capacity Per Month	152
B111586- Oracle Base Database Service - Enterprise	ECPU—ECPU Per Hour	8
B91627 - Object Storage - Requests#[0-5]	10,000 Requests per Month (first 50,000 free)	1
B91628 - Object Storage - Storage#[10-999999999]	Gigabyte Storage Capacity Per Month	1000

4.6.10 Autonomous AI Database@Google Cloud Bill of Materials

Part number	Description	Metric	Qty	Comments
B95702	Oracle Autonomous AI Transaction Processing - ECPU	ECPU Per Hour	40	
B95754	Oracle Autonomous AI Database Storage (Gigabyte Storage Capacity Per Month)	Gigabyte Storage Capacity Per Month	40960	
B95706	Oracle Autonomous AI Database Storage for Transaction Processing	Gigabyte Storage Capacity Per Month	14336	14 TB according to sizing spreadsheet

Copyright @2024, Oracle and/or its affiliates