ORACLE

ACME
Example Oracle Database Consolidation to ExaDB-CC

Solution Definition

3 July, 2023 | Version 1.0

Contents

Document Control 3
1.1 Version Control 3
1.2 Team 3
1.3 Document Purpose 3
Business Context 3
1.4 Executive Summary 3
1.5 Workload Business Value 3
Workload Requirements and Architecture 4
2.1 Overview 4
2.2 Functional Requirements 4
2.3 Non-Functional Requirements 5
2.3.1 Environments 5
2.3.2 High Availability and Disaster Recovery Requirements 5
2.3.3 Security Requirements 5
2.4 Future State Architecture 5
2.4.1 Mandatory Security Best Practices 5
2.4.2 OCI Secure Landing Zone Architecture 7
2.4.3 Physical Architecture 12
2.4.4 Database Consolidation 14
Annex 20
3.1 Security Guidelines 20
3.1.1 Oracle Security, Identity, and Compliance 20
3.1.2 Compliance and Regulations 20
3.2 Additional Resources 20

Document Control

1.1 Version Control

Guide:

Version	Authors	Date	Comments
1.0			Initial publication

1.2 Team

Name	Email	Role	Company
<name>	<name>@acme.com	Cloud Architect	ACME

1.3 Document Purpose

This document provides a high-level solution definition for the Oracle solution and aims at describing the current state, and to-be state for ACME's Consolidation to ExaDB-CC project.

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

Business Context

ACME, A Company Making Everything, is a manufacturing company with customers all over the world.

1.4 Executive Summary

ACME has three mission critical applications with Oracle database on aging Exadata that is running out of support and needs to be upgraded or replaced. It has decided to consolidate the Oracle databases to ExaDB-CC.

1.5 Workload Business Value

By consolidating the Oracle databases to the ExaDB-CC platform, ACME aims to achieve the following benefits:

- Reduced Costs
- Improved Security
- Ensured Availability
- Assured Performance
- Simplified Administration

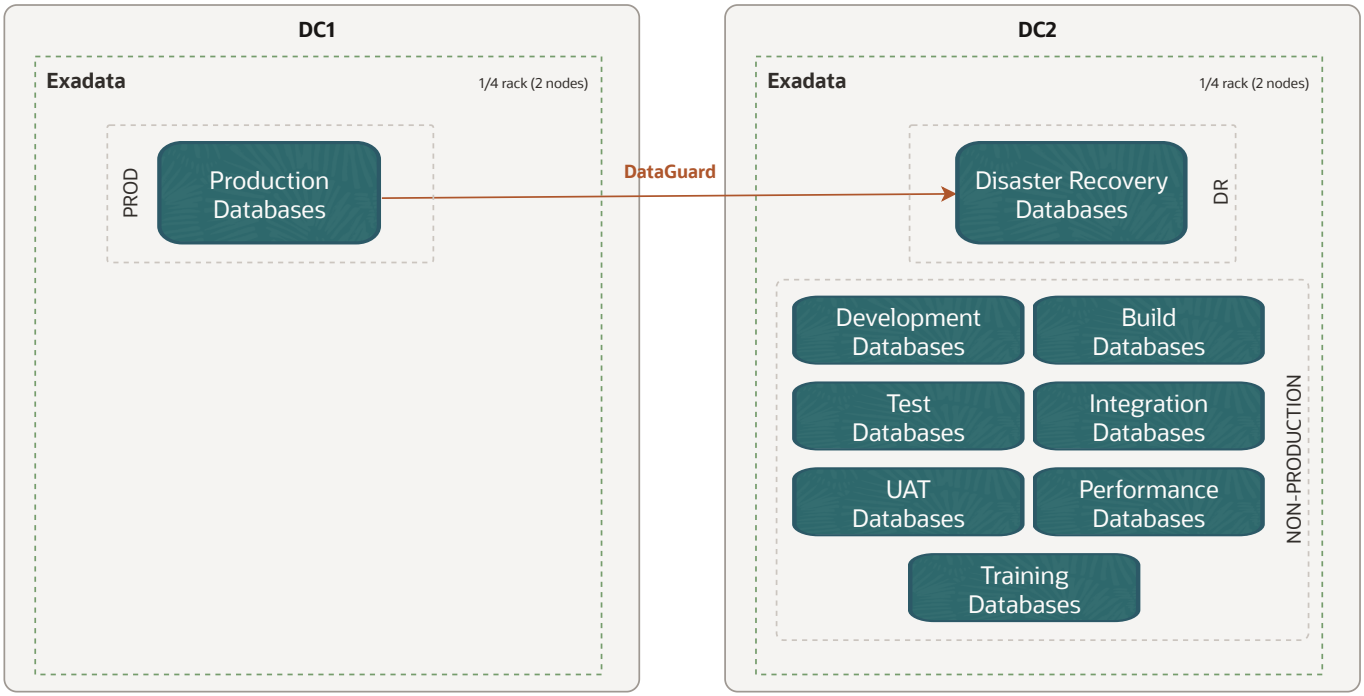
Workload Requirements and Architecture

2.1 Overview

The workload described in this document consists in migrating Oracle databases running in two separate ACME data centers on Exadata machines to two new ExaDB-CC quarter rack systems also distributed in this fashion.

The environments include Production, Disaster Recovery or Standby and other non-Production databases.

The following diagram show the current on-premises Exadata deployment:



2.2 Functional Requirements

The workload is database only therefore functionally the platform only provides the services to accommodate Oracle Databases and their associated complementary functions like clustering, storage, networking and compute.

The solution implemented with ExaDB-CC allows ACME to meet advanced requirements in the following areas:

- Higher data availability for business continuity
- Consolidation of more than 40 Databases
- Increased resource management to match SLO (service level objective)

All the applications are typical multi-tier web application made of three main layers: Presentation, Application and Data Layers. Applications are Java Based running on top of Weblogic application servers. High availability is ensured by a load balancer that distributes the load over several Weblogic servers.

Presentation and Application layers are not part of this migration and will stay as-is, only the Database layer is addressed in this document.

2.3 Non-Functional Requirements

2.3.1 Environments

Name	Size of Prod	Location	DR	Scope
Production	100%	DC1	Yes	Workload
DR	100%	DC2	No	Workload
NonProd	100%	DC1,2	No	Workload

2.3.2 High Availability and Disaster Recovery Requirements

2.3.2.1 High Availability

Service Name	KPI	Unit	Value
Production DB	Uptime	percent	99.95
NonProduction DB	Uptime	percent	95

2.3.2.2 Disaster Recovery

Service Name	KPI	Unit	Value
Production DB	RTO	minutes	30
Production DB	RPO	minutes	10

2.3.2.3 Backup and Restore

Service Name	KPI	Unit	Value
Production DB	Frequency	/day	2
Production DB	BckpTime (F)	hours	4
Production DB	BckpTime (I)	hours	1
Production DB	Retention	days	60

2.3.3 Security Requirements

The solution provided must address the following security requirements expressed by ACME :

- Data encryption must be implemented using customer provided keys
- Use of a Key Management System (KMS) to store the encryption keys

2.4 Future State Architecture

2.4.1 Mandatory Security Best Practices

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

To 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 chapters below. They must be approved by ACME.

ACME 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 enforce 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.
	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 has Local Password enabled only. • Has MFA enabled and enforced (see IAM Default Domain).
	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.
	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 home region. 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 fulfil 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 with the Customer's requirements is highly recommended. This step requires thorough planning and decisions to make. • For configuration details see Customizing Cloud Guard Configuration
	OCI Vulnerability Scanning Service	In addition to OCI Cloud Guard, the OCI Vulnerability Scanning Service will be enabled at the root compartment in the home region. This service provides vulnerability scanning of all Compute instances once they are created. • For configuration details see Vulnerability Scanning.

CATEGORY	TOPIC	DETAILS
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 of the tenancy's budget consumption. It will be configured to quickly identify unexpected usage of the tenancy. • For configuration details see Managing Budgets

2.4.2 OCI Secure Landing Zone Architecture

The design considerations for an OCI Cloud Landing Zone have to do with OCI and industry architecture best practices, along with ACME specific architecture requirements that reflect the Cloud Strategy (hybrid, multi-cloud, etc). An OCI Cloud Landing zone involves a variety of fundamental aspects that have a broad level of sophistication. A good summary of a Cloud Landing Zone has been published in the OCI User Guide.

2.4.2.1 Naming Convention

A naming convention is an important part of any deployment to ensure consistency as well as security within your tenancy. Hence we jointly agree on a naming convention, matching Oracle's best practices and ACME requirements.

Oracle recommends the following Resource Naming Convention:

- The name segments are separated by "-"
- Within a name segment avoid using and "."
- Where possible intuitive/standard abbreviations should be considered (e.g. "shared" compared to "shared.cloud.team")
- When referring to the compartment full path, use ":" as a separator, e.g. cmp-shared:cmp-security

Some examples of naming are given below:

- cmp-shared
- cmp-<workload>
- cmp-networking

The patterns used are these:

- <resource-type>-<environment>-<location>-<purpose>
- <resource-type>-<environment>-<source-location>-<destination-location>-<purpose>
- <resource-type>-<entity/sub-entity>-<environment>-<function/department>-<project>-<custom>
- <resource-type>-<environment>-<location>-<purpose>

Abbreviations per resource type are listed below. This list may not be complete.

Resource Type	Abbreviation	Example
Bastion Service	bst	bst-<location>-<network>
Block Volume	blk	blk-<location>-<project>-<purpose>
Compartment	cmp	cmp-shared, cmp-shared-security
Customer Premise Equipment	cpe	cpe-<location>-<destination>
DNS Endpoint Forwarder	dnsepf	dnsepf-<location>
DNS Endpoint Listener	dnsepl	dnsepl-<location>

Resource Type	Abbreviation	Example
Dynamic Group	dgp	dpg-security-functions
Dynamic Routing Gateway	drg	drg-prod-<location>
Dynamic Routing Gateway Attachment	drgatt	drgatt-prod-<location>-<source_vcn>-<destination_vcn>
Fast Connect	fc# <# := 1...n>	fc0-<location>-<destination>
File Storage	fss	fss-prod-<location>-<project>
Internet Gateway	igw	igw-dev-<location>-<project>
Jump Server	js	js-<location>-xxxxx
Load Balancer	lb	lb-prod-<location>-<project>
Local Peering Gateway	lpg	lpg-prod-<source_vcn>-<destination_vcn>
NAT Gateway	nat	nat-prod-<location>-<project>
Network Security Group	nsg	nsg-prod-<location>-waf
Managed key	key	key-prod-<location>-<project>-database01
OCI Function Application	fn	fn-security-logs
Object Storage Bucket	bkt	bkt-audit-logs
Policy	pcy	pcy-services, pcy-tc-security-administration
Region Code, Location	xxx	fra, ams, zch # three letter region code
Routing Table	rt	rt-prod-<location>-network
Secret	sec	sec-prod-wls-admin
Security List	sl	sl-<location>
Service Connector Hub	sch	sch-<location>
Service Gateway	sgw	sgw-<location>
Subnet	sn	sn-<location>
Tenancy	tc	tc
Vault	vlt	vlt-<location>
Virtual Cloud Network	vcn	vcn-<location>
Virtual Machine	vm	vm-xxxx

2.4.2.2 Security and Identity Management

This chapter covers the Security and Identity Management definitions and resources which will be implemented for ACME.

2.4.2.2.1 Universal Security and Identity and Access Management Principles

- Groups will be configured at the tenancy level and access will be governed by policies configured in OCI.
- Any new project deployment in OCI will start with the creation of a new compartment. Compartments follow a hierarchy, and the compartment structure will be decided as per the application requirements.
- It is also proposed to keep any shared resources, such as Object Storage, Networks, etc. in a shared services compartment. This will allow the various resources in different compartments to access and use the resources deployed in the shared services compartment and user access can be controlled by policies related to specific resource types and user roles.
- Policies will be configured in OCI to maintain the level of access/control that should exist between resources in different compartments. These will also control user access to the various resources deployed in the tenancy.
- The tenancy will include a pre-provisioned Identity Cloud Service (IDCS) instance (the primary IDCS instance) or, where applicable, the Default Identity Domain. Both provide access management across all Oracle cloud services for IaaS, PaaS, and SaaS cloud offerings.

- The primary IDCS or the Default Identity Domain will be used as the access management system for all users administrating (OCI Administrators) the OCI tenant.

2.4.2.2.2 Authentication and Authorization for OCI

The provisioning of respective OCI administration users will be handled by ACME.

2.4.2.2.2.1 User Management

Only OCI Administrators are granted access to the OCI Infrastructure. As a good practice, these users are managed within the pre-provisioned and pre-integrated Oracle Identity Cloud Service (primary IDCS) or, where applicable, the OCI Default Identity Domain, of OCI tenancy. These users are members of groups. IDCS Groups can be mapped to OCI groups while Identity Domains groups do not require any mapping. Each mapped group membership will be considered during login.

Local Users

The usage of OCI Local Users is not recommended for the majority of users and is restricted to a few users only. These users include the initial OCI Administrator created during the tenancy setup and additional emergency administrators.

Local Users are considered Emergency Administrators and should not be used for daily administration activities!

No additional users are to be, nor should be, configured as local users.

ACME is responsible to manage and maintain local users for emergency use cases.

Federated Users

Unlike Local Users, Federated Users are managed in the Federated or Enterprise User Management system. In the OCI User list Federated Users may be distinguished by a prefix that consists of the name of the federated service in lower case, a '/' character followed by the user name of the federated user, for example:

```
oracleidentityservicecloud/user@example.com
```

Providing the same attributes (OCI API Keys, Auth Tokens, Customer Secret Keys, OAuth 2.0 Client Credentials, and SMTP Credentials) for Local and *Federated Users* federation with third-party Identity Providers should only be done in the pre-configured primary IDCS or the Default Identity Domain where applicable.

All users have the same OCI-specific attributes (OCI API Keys, Auth Tokens, Customer Secret Keys, OAuth 2.0 Client Credentials, and SMTP Credentials).

OCI Administration users should only be configured in the pre-configured primary IDCS or the Default Identity Domain where applicable.

Note: Any federated user can be a member of 100 groups only. The OCI Console limits the number of groups in a SAML assertion to 100 groups. User Management in the Enterprise Identity Management system will be handled by ACME.

Authorization

In general, policies hold permissions granted to groups. Policy and Group naming follows the Resource Naming Conventions.

Tenant Level Authorization

The policies and groups defined at the tenant level will provide access to administrators and authorized users, to manage or view resources across the entire tenancy. The tenant-level authorization will be granted to tenant administrators only.

These policies follow the recommendations of the CIS Oracle Cloud Infrastructure Foundations Benchmark v1.2.0, recommendations 1.1, 1.2, 1.3.

Service Policy

A Service Policy is used to enable services at the tenancy level. It is not assigned to any group.

Shared Compartment Authorization

Compartment-level authorization for the cmp-shared compartment structure uses the following specific policies and groups.

Apart from tenant-level authorization, authorization for the cmp-shared compartment provides specific policies and groups. In general, policies will be designed so that lower-level compartments are not able to modify the resources of higher-level compartments.

Policies for the cmp-shared compartment follow the recommendations of the CIS Oracle Cloud Infrastructure Foundations Benchmark v1.2.0, recommendations 1.1, 1.2, 1.3.

Compartment Level Authorization

Apart from tenant-level authorization, compartment-level authorization provides compartment structure-specific policies and groups. In general, policies will be designed so that lower-level compartments are not able to modify the resources of higher-level compartments.

Authentication and Authorization for Applications and Databases

Application (including Compute Instances) and Database User management are completely separate and done outside of the primary IDCS or Default Identity Domain. The management of these users is the sole responsibility of ACME using the application, compute instance, and database-specific authorization.

2.4.2.2.3 Security Posture Management

Oracle Cloud Guard

Oracle Cloud Guard Service will be enabled using the pcy-service policy and with the following default configuration. Customization of the Detector and Responder Recipes will result in clones of the default (Oracle Managed) recipes.

Cloud Guard default configuration provides a number of good settings. It is expected that these settings may not match ACME's requirements.

Targets

In accordance with the CIS Oracle Cloud Infrastructure Foundations Benchmark, v1.2.0, Chapter 3.15, Cloud Guard will be enabled in the root compartment.

Detectors

The Oracle Default Configuration Detector Recipes and Oracle Default Activity Detector Recipes are implemented. To better meet the requirements, the default detectors must be cloned and configured by ACME.

Responder Rules

The default Cloud Guard Responders will be implemented. To better meet the requirements, the default detectors must be cloned and configured by ACME.

Vulnerability Scanning Service

In accordance with the CIS Oracle Cloud Infrastructure Foundations Benchmark, v1.2.0, OCI Vulnerability Scanning will be enabled using the pcy-service policy.

Compute instances that should be scanned *must* implement the *Oracle Cloud Agent* and enable the *Vulnerability Scanning plugin*.

OCI OS Management Service

Required policy statements for OCI OS Management Service are included in the pcy-service policy.

By default, the *OS Management Service Agent plugin* of the *Oracle Cloud Agent* is enabled and running on current Oracle Linux 6, 7, 8, and 9 platform images.

2.4.2.2.4 Monitoring, Auditing, and Logging

In accordance with the CIS Oracle Cloud Infrastructure Foundations Benchmark, v1.2.0, Chapter 3 Logging and Monitoring the following configurations will be made:

- OCI Audit log retention period set to 365 days.
- At least one notification topic and subscription to receive monitoring alerts.
- Notification for Identity Provider changes.
- Notification for IdP group mapping changes.
- Notification for IAM policy changes.
- Notification for IAM group changes.
- Notification for user changes.
- Notification for VCN changes.
- Notification for changes to route tables.
- Notification for security list changes.
- Notification for network security group changes.
- Notification for changes to network gateways.
- VCN flow logging for all subnets.
- Write level logging for all Object Storage Buckets.
- Notification for Cloud Guard detected problems.
- Notification for Cloud Guard remedied problems.

For IDCS or OCI Identity Domain Auditing events, the respective Auditing API can be used to retrieve all required information.

2.4.2.2.5 Data Encryption

All data will be encrypted at rest and in transit. Encryption keys can be managed by Oracle or the customer and will be implemented for identified resources.

2.4.2.2.5.1 Key Management

All keys for **OCI Block Volume**, **OCI Container Engine for Kubernetes**, **OCI Database**, **OCI File Storage**, **OCI Object Storage**, and **OCI Streaming** are centrally managed in a shared or a private virtual vault will be implemented and placed in the compartment cmp-security.

Object Storage Security

For Object Storage security the following guidelines are considered.

- **Access to Buckets** -- Assign least privileged access for IAM users and groups to resource types in the object-family (Object Storage Buckets & Object)
- **Encryption at rest** -- All data in the Object Storage is encrypted at rest using AES-256 and is on by default. This cannot be turned off and objects are encrypted with a master encryption key.

Data Residency

It is expected that data will be held in the respective region and additional steps will be taken when exporting the data to other regions to comply with the applicable laws and regulations. This should be reviewed for every project onboard into the tenancy.

2.4.2.2.6 Operational Security

Security Zones

Whenever possible OCI Security Zones will be used to implement a security compartment for Compute instances or Database resources. For more information on Security Zones refer to the *Oracle Cloud Infrastructure User Guide* chapter on Security Zones.

Remote Access to Compute Instances or Private Database Endpoints

To allow remote access to Compute Instances or Private Database Endpoints, the OCI Bastion will be implemented for defined compartments.

To be able to use OCI services for OS management, Vulnerability Scanning, Bastion Service, etc. it is highly recommended to implement the Oracle Cloud Agent as documented in the *Oracle Cloud Infrastructure User Guide* chapter Managing Plugins with Oracle Cloud Agent.

2.4.2.2.7 Network Time Protocol Configuration for Compute Instance

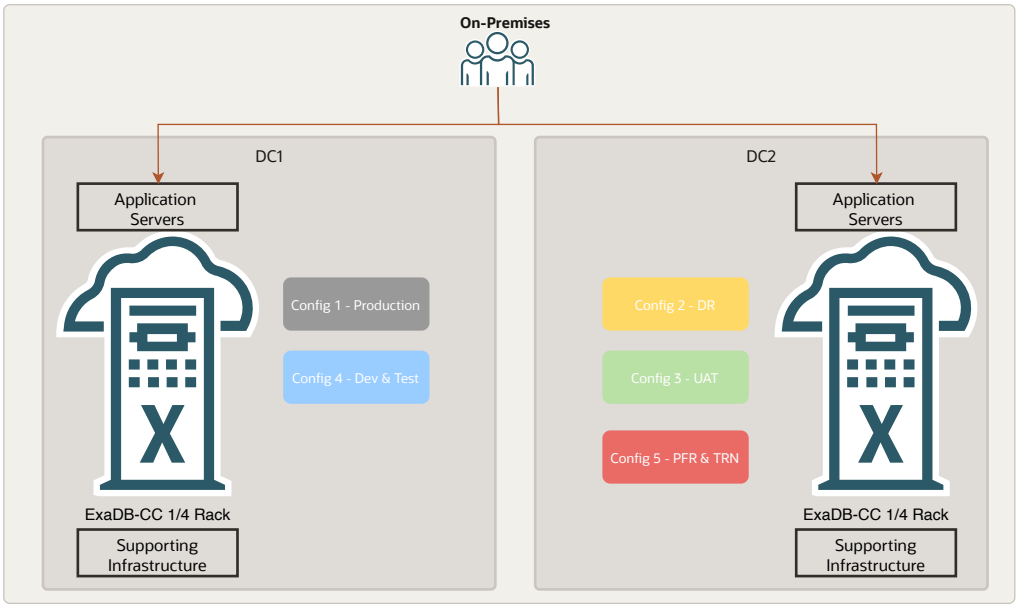
Synchronized clocks are a necessity for securely operating environments. OCI provides a Network Time Protocol (NTP) server using the OCI global IP number 169.254.169.254. All compute instances should be configured to use this NTP service.

2.4.2.2.8 Regulations and Compliance

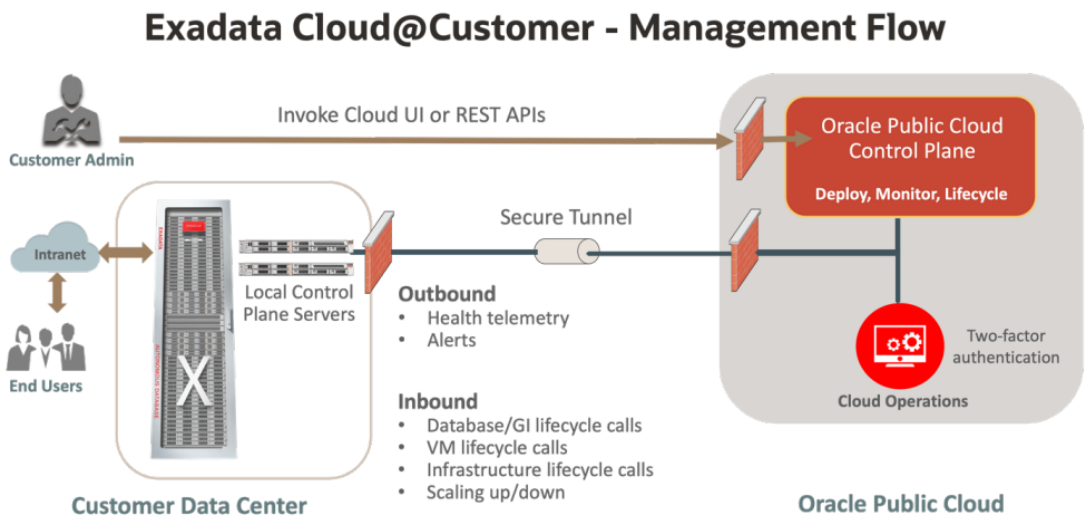
ACME is responsible for setting the access rules to services and environments that require stakeholders' integration into the tenancy to comply with all applicable regulations. Oracle will support in accomplishing this task.

2.4.3 Physical Architecture

Two Exadata Cloud at Customer X9M-2 (ExaDB-CC) quarter racks will be deployed in the two customer data centers, as shown below:



The Control Plane of this Exadata Cloud at Customer is in the OCI Public Cloud (home 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.



2.4.4 Database Consolidation

2.4.4.1 Oracle Database Consolidation Planning Process

- Use Database consolidation questionnaire to collect database information.
- Example: Oracle database version, source OS, NLS characterset, database life cycle (production, test, dev), database security zone (PCI vs non-PCI), Business Criticality, etc.
- Size the target ExaDB-CC platform based on source databases' utilization information.
- Design RAC VM cluster, RDBMS homes, CDBs.
- Create PDB to CDB mapping for all source databases to be consolidated.

2.4.4.2 Source DB Inventory

Data Center	DB Name	APP Name	Environment	Source DB Version	Target DB Charset	DB Size (GB)	DB CPU (cpu_count)	Memory (GB)	RAC [Y/N]	DR [Y/N]	PCI (Y/N)	Criticality	Target MT
DC1	DC1C1AP1DB11	AP1	PRD	19.6.0.0.0	AL32UTF8	15,385	24	112.0	Y	Y	N	5	Y
	DC1C1AP2DB11	AP2	PRD	19.6.0.0.0	AL32UTF8	4,326	12	8.0	Y	Y	N	5	Y
	DC1C1AP3DB11	AP3	PRD	12.1.0.0.0	AL32UTF8	1,807	12	54.0	Y	Y	N	5	Y
DC2	DC2C1AP1DB21	AP1	DR	19.6.0.0.0	AL32UTF8	15,385	24	112.0	Y	N	N	5	Y
	DC2C1AP2DB21	AP2	DR	19.6.0.0.0	AL32UTF8	4,326	12	8.0	Y	N	N	5	Y
	DC2C1AP3DB21	AP3	DR	12.1.0.0.0	AL32UTF8	1,807	12	54.0	Y	N	N	5	Y
	DC2C3AP1DB31	AP1	UAT	19.6.0.0.0	AL32UTF8	4,350	8	77.8	Y	N	N	4	Y
	DC2C3AP1DB32	AP1	UAT	19.6.0.0.0	AL32UTF8	3,927	8	78.0	Y	N	N	4	Y
	DC2C3AP1DB33	AP1	UAT	19.6.0.0.0	AL32UTF8	3,951	24	71.2	Y	N	N	4	Y
	DC2C3AP1DB34	AP1	UAT	19.6.0.0.0	AL32UTF8	1,115	8	71.0	Y	N	N	4	Y
	DC2C3AP1DB38	AP1	UAT	19.6.0.0.0	AL32UTF8	3,001	24	82.0	Y	N	N	4	Y
	DC2C3AP1DB39	AP1	UAT	19.6.0.0.0	AL32UTF8	5,454	12	37.2	Y	N	N	4	Y
	DC2C3AP2DB31	AP2	UAT	19.6.0.0.0	AL32UTF8	1,137	8	5.0	Y	N	N	4	Y
	DC2C3AP2DB32	AP2	UAT	19.6.0.0.0	AL32UTF8	508	8	5.0	Y	N	N	4	Y
	DC2C3AP2DB33	AP2	UAT	19.6.0.0.0	AL32UTF8	944	12	8.0	Y	N	N	4	Y
	DC2C3AP2DB34	AP2	UAT	19.6.0.0.0	AL32UTF8	711	8	5.0	Y	N	N	4	Y
	DC2C3AP2DB38	AP2	UAT	19.6.0.0.0	AL32UTF8	358	4	6.2	Y	N	N	4	Y
	DC2C3AP2DB39	AP2	UAT	19.6.0.0.0	AL32UTF8	150	8	5.0	Y	N	N	4	Y
	DC2C3AP3DB31	AP3	UAT	12.1.0.0.0	AL32UTF8	453	8	7.0	Y	N	N	4	Y
	DC2C3AP3DB32	AP3	UAT	12.1.0.0.0	AL32UTF8	266	8	7.0	Y	N	N	4	Y
	DC2C3AP3DB33	AP3	UAT	12.1.0.0.0	AL32UTF8	199	8	8.0	Y	N	N	4	Y
	DC2C3AP3DB34	AP3	UAT	12.1.0.0.0	AL32UTF8	106	8	7.0	Y	N	N	4	Y
	DC2C3AP3DB38	AP3	UAT	12.1.0.0.0	AL32UTF8	1,350	8	7.0	Y	N	N	4	Y
	DC2C3AP3DB39	AP3	UAT	12.1.0.0.0	AL32UTF8	705	8	7.0	Y	N	N	4	Y
	DC2C4AP1DB41	AP1	DEV	19.8.0.0.0	AL32UTF8	1,559	4	13.0	Y	N	N	4	Y
	DC2C4AP2DB41	AP2	DEV	19.8.0.0.0	AL32UTF8	165	4	4.8	Y	N	N	4	Y
	DC2C4AP1DB42	AP1	DEV	19.8.0.0.0	AL32UTF8	344	4	6.3	Y	N	N	4	Y
	DC2C4AP2DB42	AP2	DEV	19.8.0.0.0	AL32UTF8	165	4	4.8	Y	N	N	4	Y
	DC2C4AP1DB43	AP1	TST	19.8.0.0.0	AL32UTF8	703	4	13.0	Y	N	N	4	Y
	DC2C4AP2DB43	AP2	TST	19.8.0.0.0	AL32UTF8	583	4	4.8	Y	N	N	4	Y
	DC2C4AP1DB44	AP1	TST	19.8.0.0.0	AL32UTF8	1,183	4	12.2	Y	N	N	4	Y
	DC2C4AP2DB44	AP2	TST	19.8.0.0.0	AL32UTF8	498	4	5.0	Y	N	N	4	Y
	DC2C4AP1DB45	AP1	INT	19.8.0.0.0	AL32UTF8	337	4	6.2	Y	N	N	4	Y
	DC2C4AP2DB45	AP2	INT	19.8.0.0.0	AL32UTF8	114	4	5.0	Y	N	N	4	Y
	DC2C4AP1DB46	AP1	BLD	19.8.0.0.0	AL32UTF8	354	4	6.3	Y	N	N	4	Y
	DC2C4AP2DB46	AP2	BLD	19.8.0.0.0	AL32UTF8	111	4	4.8	Y	N	N	4	Y
	DC2C4AP1DB47	AP1	DEV	19.8.0.0.0	AL32UTF8	1,397	4	6.3	Y	N	N	4	Y
	DC2C4AP2DB47	AP2	DEV	19.8.0.0.0	AL32UTF8	134	4	5.0	Y	N	N	4	Y
	DC2C4AP1DB48	AP1	TST	19.8.0.0.0	AL32UTF8	3,197	4	13.0	Y	N	N	4	Y
	DC2C4AP2DB48	AP2	TST	19.8.0.0.0	AL32UTF8	364	4	5.0	Y	N	N	4	Y
	DC2C5AP1DB51	AP1	PRF	19.8.0.0.0	AL32UTF8	16,094	24	80.5	Y	N	N	4	Y
	DC2C5AP2DB51	AP2	PRF	19.8.0.0.0	AL32UTF8	7,255	12	8.0	Y	N	N	4	Y
	DC2C5AP3DB51	AP3	PRF	12.1.0.0.0	AL32UTF8	480	8	7.0	Y	N	N	4	Y
	DC2C5AP1DB52	AP1	TRN	19.8.0.0.0	AL32UTF8	5,875	24	71.2	Y	N	N	4	Y
	DC2C5AP2DB52	AP2	TRN	19.8.0.0.0	AL32UTF8	907	12	8.0	Y	N	N	4	Y
	DC2C5AP3DB52	AP3	TRN	12.1.0.0.0	AL32UTF8	1,191	4	11.0	Y	N	N	4	Y

2.4.4.3 Database Consolidation Requirements

- Prefer to separate database of different environments for PDB consolidation. However, BLD and DEV can go together, so does TST and INT (Integration).
- Production environment will be run as MAA Gold (RAC + Data Guard), while other environments will run as MAA Silver.
- Prefer to have different grid clusters for PROD, DR, UAT, DEV + TEST, PRF + TRN

2.4.4.4 Database Consolidation Results

Below is the summary of consolidation result in consideration of the above requirements.

2.4.4.4.1 PDB Consolidation

CDB	DB Vesion	Charset	PDB Name	APP Name	Environment	CDB oCPU	CDB RAM (GB)	CDB Disk (GB)
CPRAP12	19.6.0.0.0	AL32UTF8	DC1C1AP1DB11	AP1	PRD	16	240	19,711
			DC1C1AP2DB11	AP2	PRD			
CPRAP3	12.1.0.0.0	AL32UTF8	DC1C1AP3DB11	AP3	PRD	4	108	1,807
CDTAP1	19.8.0.0.0	AL32UTF8	DC2C4AP1DB41	AP1	DEV	6	107	9,074
			DC2C4AP1DB42	AP1	DEV			
			DC2C4AP1DB43	AP1	TST			
			DC2C4AP1DB44	AP1	TST			
			DC2C4AP1DB45	AP1	INT			
			DC2C4AP1DB46	AP1	BLD			
			DC2C4AP1DB47	AP1	DEV			
			DC2C4AP1DB48	AP1	TST			
CDTAP2	19.8.0.0.0	AL32UTF8	DC2C4AP2DB41	AP2	DEV	4	55	2,133
			DC2C4AP2DB42	AP2	DEV			
			DC2C4AP2DB43	AP2	TST			
			DC2C4AP2DB44	AP2	TST			
			DC2C4AP2DB45	AP2	INT			
			DC2C4AP2DB46	AP2	BLD			
			DC2C4AP2DB47	AP2	DEV			
			DC2C4AP2DB48	AP2	TST			
CPRAP12	19.6.0.0.0	AL32UTF8	DC2C1AP1DB21	AP1	DR	4	240	19,711
			DC2C1AP2DB21	AP2	DR			
CPRAP3	12.1.0.0.0	AL32UTF8	DC2C1AP3DB21	AP3	DR	2	108	1,807
CUAAP1	19.6.0.0.0	AL32UTF8	DC2C3AP1DB31	AP1	UAT	8	584	21,797
			DC2C3AP1DB32	AP1	UAT			
			DC2C3AP1DB33	AP1	UAT			
			DC2C3AP1DB34	AP1	UAT			
			DC2C3AP1DB38	AP1	UAT			
			DC2C3AP1DB39	AP1	UAT			
CUAAP2	19.6.0.0.0	AL32UTF8	DC2C3AP2DB31	AP2	UAT	4	48	3,806
			DC2C3AP2DB32	AP2	UAT			
			DC2C3AP2DB33	AP2	UAT			
			DC2C3AP2DB34	AP2	UAT			
			DC2C3AP2DB38	AP2	UAT			
			DC2C3AP2DB39	AP2	UAT			
CUAAP3	12.1.0.0.0	AL32UTF8	DC2C3AP3DB31	AP3	UAT	4	60	3,078
			DC2C3AP3DB32	AP3	UAT			
			DC2C3AP3DB33	AP3	UAT			
			DC2C3AP3DB34	AP3	UAT			
			DC2C3AP3DB38	AP3	UAT			
			DC2C3AP3DB39	AP3	UAT			
CPFAP12	19.8.0.0.0	AL32UTF8	DC2C5AP1DB51	AP1	PRF	16	177	23,348
			DC2C5AP2DB51	AP2	PRF			
CPFAP3	12.1.0.0.0	AL32UTF8	DC2C5AP3DB51	AP3	PRF	4	14	480
CTRAP12	19.8.0.0.0	AL32UTF8	DC2C5AP1DB52	AP1	TRN	4	111	6,782
			DC2C5AP2DB52	AP2	TRN			
CTRAP3	12.1.0.0.0	AL32UTF8	DC2C5AP3DB52	AP3	TRN	2	22	1,191

2.4.4.4.2 CDB to VM Cluster Consolidation

The following section gives an overview of the CDB list in each VM Cluster with sizing information:

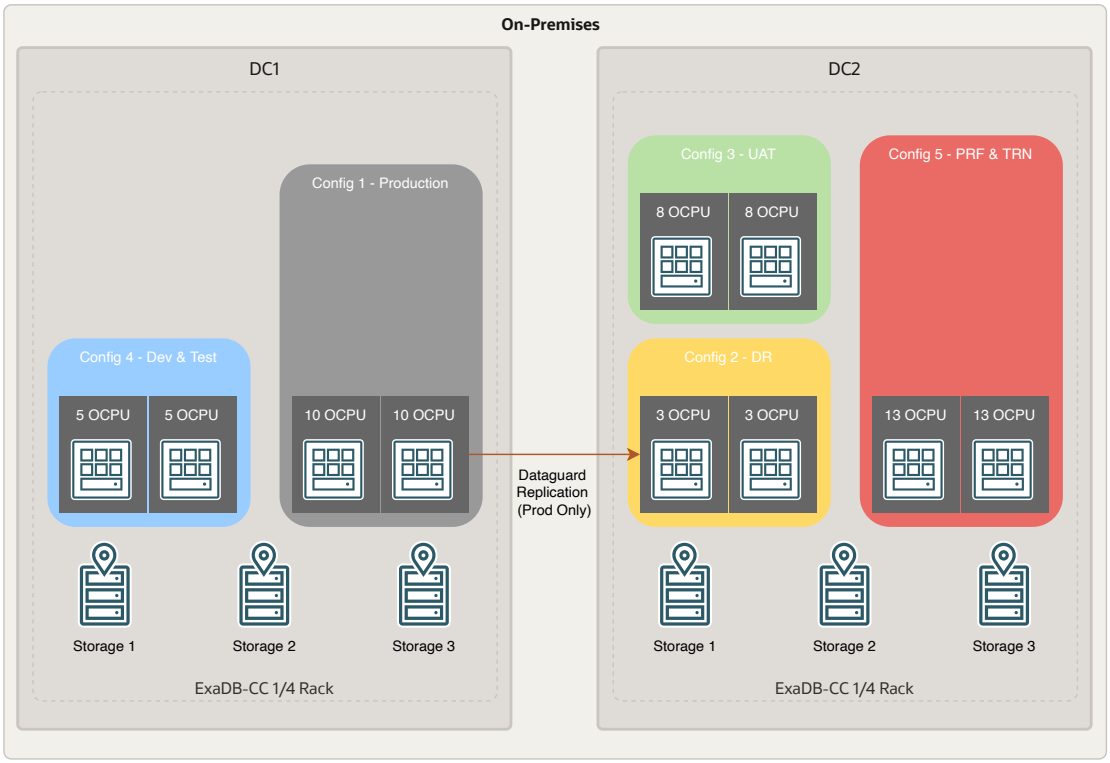
VM Cluster	CDB	Cluster oCPU	Cluster RAM (GB)	Cluster Disk (GB)
vmcls-prod	CPRAP12	20	364	21,518
	CPRAP3			
vmcls-devtst	CDTAP1	10	178	11,207
	CDTAP2			
vmcls-dr	CPRAP12	6	364	21,518
	CPRAP3			
vmcls-uat	CUAAP1	16	780	28,682
	CUAAP2			
	CUAAP3			
vmcls-prf	CPFAP12	26	340	31,802
	CPFAP3			
	CTRAP12			
	CTRAP3			

2.4.4.4.3 VM Clusters

An ExaDB-CC can host up to eight independent VM clusters (for quarter rack and above). One cluster can be considered a domain where the databases will be consolidated based on criteria to be 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 clusters 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. ACME calls his different environments as "Config", for example Production is "Config 1" and it will have assigned 20 OCPU during the provisioning of the virtual cluster and it will be placed in DC 1.

Name	OCPUs	Location	Oracle MAA
Production "Config 1"	20	DC 1	Gold
DR "Config 2"	6	DC 2	Gold
UAT "Config 3"	16	DC 2	Silver
Dev & Test "Config 4"	10	DC 1	Silver
PFR & TRN "Config 5"	26	DC 2	Silver



2.4.4.4.4 VM Cluster to ExaDB-CC Mapping

The following section gives an overview of the VM Cluster list in each ExaDB-CC Infrastructure:

Data Center	ExaDB-CC	VM Cluster	Rack oCPU	Rack RAM (GB)	Rack Disk (GB)
DC1	dc1-exacc01	vmcls-prod	30	542	32,724
		vmcls-devtst			
DC2	dc2-exacc01	vmcls-dr	48	1,412	82,001
		vmcls-uat			
		vmcls-prf			

2.4.4.4.5 Source Database to ExaDB-CC Mapping

The following section gives an overview of the mapping of all resources in both ExaDB-CC with VM cluster and CDB/PDB without sizing information:

Data Center	ExaDB-CC	VM Cluster	CDB	DB Vesion	Charset	PDB Name	APP Name	Environment
DC1	dc1-exacc01	vmcls-prod	CPRAP12	19.6.0.0.0	AL32UTF8	DC1C1AP1DB11	AP1	PRD
						DC1C1AP2DB11	AP2	PRD
			CPRAP3	12.1.0.0.0	AL32UTF8	DC1C1AP3DB11	AP3	PRD
		vmcls-devtst	CDTAP1	19.8.0.0.0	AL32UTF8	DC2C4AP1DB41	AP1	DEV
						DC2C4AP1DB42	AP1	DEV
						DC2C4AP1DB43	AP1	TST
						DC2C4AP1DB44	AP1	TST
						DC2C4AP1DB45	AP1	INT
						DC2C4AP1DB46	AP1	BLD
						DC2C4AP1DB47	AP1	DEV
						DC2C4AP1DB48	AP1	TST
			CDTAP2	19.8.0.0.0	AL32UTF8	DC2C4AP2DB41	AP2	DEV
						DC2C4AP2DB42	AP2	DEV
						DC2C4AP2DB43	AP2	TST
						DC2C4AP2DB44	AP2	TST
						DC2C4AP2DB45	AP2	INT
						DC2C4AP2DB46	AP2	BLD
						DC2C4AP2DB47	AP2	DEV
						DC2C4AP2DB48	AP2	TST
DC2	dc2-exacc01	vmcls-dr	CPRAP12	19.6.0.0.0	AL32UTF8	DC2C1AP1DB21	AP1	DR
						DC2C1AP2DB21	AP2	DR
			CPRAP3	12.1.0.0.0	AL32UTF8	DC2C1AP3DB21	AP3	DR
		vmcls-uat	CUAAP1	19.6.0.0.0	AL32UTF8	DC2C3AP1DB31	AP1	UAT
						DC2C3AP1DB32	AP1	UAT
						DC2C3AP1DB33	AP1	UAT
						DC2C3AP1DB34	AP1	UAT
						DC2C3AP1DB38	AP1	UAT
						DC2C3AP1DB39	AP1	UAT
			CUAAP2	19.6.0.0.0	AL32UTF8	DC2C3AP2DB31	AP2	UAT
						DC2C3AP2DB32	AP2	UAT
						DC2C3AP2DB33	AP2	UAT
						DC2C3AP2DB34	AP2	UAT
						DC2C3AP2DB38	AP2	UAT
						DC2C3AP2DB39	AP2	UAT
			CUAAP3	12.1.0.0.0	AL32UTF8	DC2C3AP3DB31	AP3	UAT
						DC2C3AP3DB32	AP3	UAT
						DC2C3AP3DB33	AP3	UAT
						DC2C3AP3DB34	AP3	UAT
						DC2C3AP3DB38	AP3	UAT
						DC2C3AP3DB39	AP3	UAT
		vmcls-prf	CPFAP12	19.8.0.0.0	AL32UTF8	DC2C5AP1DB51	AP1	PRF
						DC2C5AP2DB51	AP2	PRF
			CPFAP3	12.1.0.0.0	AL32UTF8	DC2C5AP3DB51	AP3	PRF
			CTRAP12	19.8.0.0.0	AL32UTF8	DC2C5AP1DB52	AP1	TRN
						DC2C5AP2DB52	AP2	TRN
			CTRAP3	12.1.0.0.0	AL32UTF8	DC2C5AP3DB52	AP3	TRN

Annex

3.1 Security Guidelines

3.1.1 Oracle Security, Identity, and Compliance

Oracle Cloud Infrastructure (OCI) is designed to protect customer workloads with a security-first approach across compute, network, and storage – down to the hardware. It's complemented by essential security services to provide the required levels of security for your most business-critical workloads.

- Security Strategy – To create a successful security strategy and architecture for your deployments on OCI, it's helpful to understand Oracle's security principles and the OCI security services landscape.
- The security pillar capabilities pillar capabilities reflect fundamental security principles for architecture, deployment, and maintenance. The best practices in the security pillar help your organization to define a secure cloud architecture, identify and implement the right security controls, and monitor and prevent issues such as configuration drift.

3.1.1.1 References

- The Best Practices Framework for OCI provides architectural guidance about how to build OCI services in a secure fashion, based on recommendations in the Best practices framework for Oracle Cloud Infrastructure.
- Learn more about Oracle Cloud Security Practices.
- For detailed information about security responsibilities in Oracle Cloud Infrastructure, see the Oracle Cloud Infrastructure Security Guide.

3.1.2 Compliance and Regulations

Cloud computing is fundamentally different from traditionally on-premises computing. In the traditional model, organizations are typically in full control of their technology infrastructure located on-premises (e.g., physical control of the hardware, and full control over the technology stack in production). In the cloud, organizations leverage resources and practices that are under the control of the cloud service provider, while still retaining some control and responsibility over other components of their IT solution. As a result, managing security and privacy in the cloud is often a shared responsibility between the cloud customer and the cloud service provider. The distribution of responsibilities between the cloud service provider and customer also varies based on the nature of the cloud service (IaaS, PaaS, SaaS).

3.2 Additional Resources

- Oracle Cloud Compliance – Oracle is committed to helping customers operate globally in a fast-changing business environment and address the challenges of an ever more complex regulatory environment. This site is a primary reference for customers on Shared Management Model with Attestations and Advisories.
- Oracle Security Practices – Oracle's security practices are multidimensional, encompassing how the company develops and manages enterprise systems, and cloud and on-premises products and services.
- Oracle Cloud Security Practices documents.
- Contract Documents for Oracle Cloud Services.
- OCI Shared Security Model
- OCI Cloud Adoption Framework Security Strategy
- OCI Security Guide
- OCI Cloud Adoption Framework Security chapter