Document Control

Guide:

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

Version Control

Example:

Version	Author	Date	Comment
0.1	Bart Eygenraam	July, 2023	Initial Draft Sol Def V0.1

Team

Guide:

A section describing the Oracle team.

Example:

Name	Email	Role	Company
Name Surname	name@example.com	Solution Architect	example
Name Surname	name@lexample.com	Account Cloud Engineer	example

Document Purpose

Guide:

Describe the purpose of this document and the Oracle-specific terminology, specifically around 'Workload'.

Example:

This document provides a high-level solution definition for the Oracle solution and aims at describing the current state, current state requirements, and to-be state.

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 Workload 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:

Describe the customer's business and background. What is the context of the customer's industry and LoB? What are the business needs and goals which this Workload 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?

Executive Summary

Guide:

A section describing the background of the Customer and the context of the Workload migration

Example:

- Brief history of the Customer
- Current Solution and Rationale for moving to Oracle Cloud Infrastructure (OCI)

Workload Business Value

Guide:

A section describing the business value of the Application on OCI

Example:

Organizations use on-premises deployments of JD Edwards (JDE) for a wide range of functionalities, including Financial Management, Order Management, Project Management, Agribusiness, Supply Magement, Manufacturing, Logistics etc. These implementations are often customized to seamlessly integrate with other applications to meet business requirements. So it’s counterproductive to re-architect software from scratch. OCI has the flexibility to support everything Organizations are currently doing with JD Edwards.

Most On-Premises JDE deployments can be migrated to run on OCI without requiring significant configuration, integration, or business process changes, and result in an implementation that is more flexible, more reliable, higher performance, and lower cost than either On-Premises or other Cloud vendors. Running JDE on Oracle Cloud enables you to:

- Increase business agility
- Better manage growth
- Reduce time and cost for new projects
- Track and Manage Usage and Cost
- Maximize the productivity of your IT staff

OCI Database service offers Autonomous and Co-managed (Base Database, Exadata Database on Dedicated Infrastructure, and Exadata Database on Cloud@Customer). JDE customers can run their mission-critical business applications with unprecedented performance, scalability, and availability. This is accomplished by leveraging the **best database platforms** available in OCI discussed above. Further note that most JDE systems currently running on OCI host the Database on either Base Database (Oracle Database Cloud Services on Virtual Machines), or on Oracle Exadata Database on Dedicated Infrastructure. Additional JDE Database can also run on Aotonomous, both Shared as Dedicated Autonomous Database System.

Additionally, all the activities mentioned within the scope will ensure the deployment of workload as per Oracle's best practices. As a tried and tested methodology by many customers 'Oracle Lift' brings the speed of deployment resulting in a successful project without any setbacks; thus bringing value to the overall project provisioning for the Application workload.

Workload Requirements and Architecture

Overview

Guide:

A section describing the Current JDE workload of the Customer. Describe the Workload: What applications and environments are part of this Workload, specify their names and details. The implementation will be scoped later and is typically a subset of the Workload. For example, a Workload could exist of multiple 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 late in the chapter. Scope.

Example Architecture for Deploying JD Edwards EnterpriseOne in a Single Region:

One can deploy JD Edwards EnterpriseOne in a single availability domain while ensuring high availability.

You can achieve high availability by placing the application instances inside multiple fault domains. Use this architecture when you want to ensure that your application is available even when an application instance goes down in one fault domain. The other available application instances inside the other fault domain continue to process the requests. You can deploy JD Edwards EnterpriseOne manually or by using the JD Edwards EnterpriseOne automation tools on Oracle Cloud Infrastructure.

The referenced architecture shows that redundant instances are deployed in the presentation tier and middle tier in an availability domain to ensure high availability within the availability domain. All instances in the availability domain are active. This high availability of an application within an availability domain can be achieved by placing application instances in separate fault domains. Fault domains let you distribute your instances so that they are not on the same physical hardware within a single availability domain. A hardware failure or Oracle Cloud Infrastructure Compute hardware maintenance that affects one fault domain does not affect instances in other fault domains. If an instance fails, then the traffic is diverted to other instances in the availability domain that continue to process the requests. However, if your connection to the availability domain fails or the entire availability domain goes down, then the instances are not available to process the requests.

The referenced architecture consists of a virtual cloud network (VCN) with the bastion host, load balancer tier, presentation tier, middle tier, administration tier, and database tier. The tiers are placed in a single subnet of the VCN in a single availability domain.

In the referenced architecture diagram, the bastion host is deployed in a public subnet, and all the other instances are placed in private subnets. Depending on your business requirements, you can place instances in public or private subnets. You can access the instances that are in private subnets over port 22 through the bastion host or the dynamic routing gateway (DRG). To enable communication between the DRG and the customer on-premises equipment, use IPSec VPN or Oracle Cloud Infrastructure FastConnect.

The Server Manager in the Administration tier communicates with Presentation tier, Middle tier, and Database tier to provide code deployment, configuration management, runtime metrics access, and log access. The Deployment Server in the Administration tier communicates with the Middle tier and the Database tier to build and deploy code. The Development Client communicates with the Middle tier and the Database tier. Application Development Framework (ADF) and Oracle Business Intelligence Publisher communicate with the HTML server in the Presentation tier.

Non-Functional Requirements

Guide:

Describe the high-level technical requirements for the Workload. 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.

Regulations and Compliances Requirements

Guide:

This section captures specific regulatory or compliance requirements for the Workload. 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

If there are none, 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 CIS Oracle Cloud Infrastructure Foundation Benchmark, v1.2 will be applied to the Customer tenancy.

Environments

Guide:

A section describing the Current JD Edwards workload of a Customer Example Environment details

Example:

NOT SURE ABOUT THIS SECTION - BEY

Bastion host: The bastion host is an optional component that can be used as a jump server to access instances in the private subnet. A bastion host is an Oracle Cloud Infrastructure Compute instance that uses Linux as its operating system. Place the bastion host in a public subnet and assign it a public IP address to access it from the Internet.

To provide an additional level of security, you can set up security lists to access the bastion host only from the public IP address of your on-premises network. You can access Oracle Cloud Infrastructure instances in the private subnet through the bastion host. To do this, enable ssh-agent forwarding, which allows you to connect to the bastion host, and then access the next server by forwarding the credentials from your computer. You can also access the instances in the private subnet by using dynamic SSH tunneling. SSH tunneling is a way to access a web application or other listening service. The dynamic tunnel provides a SOCKS proxy on the local port, but the connections originate from the remote host.

Load Balancer tier: The load balancer tier contains the Oracle Cloud Infrastructure Load Balancing instances that load balances the traffic to all instances in the presentation tier. The load balancer receives requests from users, and then routes these requests to instances in the presentation tier.

Use Oracle Cloud Infrastructure Load Balancing to distribute traffic to your application instances within a VCN. This service provides a primary and a standby instance of the load balancer to ensure that if the primary load balancer becomes unavailable, the standby load balancer forwards the requests. The load balancer ensures that requests are routed to the healthy application instances. If a problem occurs within an application instance, then the load balancer will route requests to the remaining healthy application instances.
Based on your requirements, you can place load balancers in a public or private subnet.

For internal endpoints, that aren't accessible from the Internet, use a private load balancer. A private load balancer has a private IP address, and it isn't accessible from the Internet. Both the primary and the standby instances of a load balancer reside in the same private subnet. You can access private load balancers in the VCN or in your data center over the IPSec VPN through a DRG. The private load balancer accepts traffic from your data center, and distributes the traffic to underlying application instances.

For Internet-facing endpoints, use a public load balancer. A public load balancer has a public IP address, and it's accessible from the Internet. You can access the public load balancers from the Internet through the Internet gateway.

For accessing internal endpoints and Internet-facing endpoints, set up private load balancers and public load balancers. Set up private load balancers to serve the internal traffic, and set up public load balancers to serve the traffic from the Internet.

Register the public or private IP address of Oracle Cloud Infrastructure Load Balancing instances in your on-premises or public domain name server (DNS) for domain resolution of your application endpoint.

The ports provided in the architecture diagram are only an example. You can use any port that's available.

Administration tier: The administration tier contains a single instance of the following servers. You don't require a redundant instance of these servers to ensure high availability.

Provisioning server: Use this server to automate end-to-end deployment of JD Edwards EnterpriseOne components on Oracle Cloud Infrastructure. It communicates with all the instances in the other tiers, including the instances in the database tier, over port 22. It hosts the JD Edwards EnterpriseOne One-Click Provisioning Console and JD Edwards EnterpriseOne Server Manager Console.

Deployment Server: During the installation process, this server acts as the central repository of all the required files and installation packages. The software is distributed or deployed to all other servers and clients from this server.

Development client: The JD Edwards EnterpriseOne Development client contains components that run as standard Microsoft Windows applications (for example, Active Console, Forms Design Aid (FDA), and Report Design Aid (RDA)) and components that run in a web browser.

Application Development Framework (ADF) server: JD Edwards EnterpriseOne ADF server is a web application that is deployed on an Oracle WebLogic server with ADF runtime. It is used to run JD Edwards EnterpriseOne applications developed with Oracle ADF.
Oracle Business Intelligence Publisher: Oracle Business Intelligence Publisher presents the data collected by JD Edwards EnterpriseOne in the form of reports. Use Oracle Business Intelligence Publisher to present reports using different templates based on your business requirements. You can design and control how the report outputs are presented by using template files.

Presentation tier: The presentation tier contains redundant instances of Application Interface Services and Java Application Servers to provide high availability. These servers communicate with servers in the middle tier. All instances are active and they receive traffic from the load balancer. Each instance is associated with a block storage volume. This tier also contains components that you can use to create integration between JD Edwards EnterpriseOne and an external system. Your implementation can include one or more of these components.

This tier contains the following servers:

Application Interface Services (AIS) Server: Application Interface Service server provides the communication interface between JD Edwards EnterpriseOne mobile enterprise applications and JD Edwards EnterpriseOne.

Standard Java Application Servers (Standard JAS): It receives requests from the load balancer and executes simple business logic. For tasks that require complicated business logic, Standard JAS passes the requests to the logic server. It also passes requests to the AIS server in some cases. However, it's not configured with the AIS server for the AIS runtime.
Dedicated Java Application Servers (Dedicated JAS): It receives requests from the AIS Server. It passes requests to the logic server to execute tasks that require complicated business logic. It is configured with the AIS server for the AIS runtime.

To ensure high availability within an availability domain, deploy redundant instances of every component. All instances are active and they receive traffic from the load balancer and middle tier.

Middle Tier: The middle tier contains logic servers and batch servers. They are not directly load balanced but they have one-to-one mapping with servers in presentation tier. You can host the logic server and the batch server on the same enterprise server instance. However, it is recommended that you set up the logic server and the batch server on separate enterprise server instances.

The middle tier receives requests from the presentation tier. After processing the requests, it forwards the requests to the database servers. All instances of the servers are active and process requests.

This tier contains the following servers:

Logic servers or enterprise servers: These servers contain the business logic or business functions.

Batch servers: These servers are used for batch processing.

Database tier: The database tier contains JD Edwards EnterpriseOne database server instances. For high availability requirements, Oracle recommends that you use two-node, Oracle Real Application Clusters (Oracle RAC) database systems or an Oracle Database Exadata Cloud Service system in Oracle Cloud Infrastructure to set up JD Edwards EnterpriseOne database server instances.

You can set up redundant database instances to provide high availability. For Oracle RAC and Oracle Database Exadata Cloud Service database systems, requests that are received from the application subnet are load balanced across the database servers. If one database instance becomes unavailable, the other database instance processes the requests. You can use Oracle Cloud Infrastructure Object Storage to back up the JD Edwards EnterpriseOne database by using Oracle Recovery Manager (RMAN). To back up or patch the JD Edwards EnterpriseOne database to Oracle Cloud Infrastructure Object Storage, the DB system's VCN must be configured with either a service gateway or an Internet gateway. It is recommended that you use a service gateway rather than an Internet gateway for backup and patching.

Use security lists to restrict access to the database servers only from the bastion host, application tier, and on-premises servers. You can set up security lists to ensure that communication occurs only over port 22, through the bastion host, and over port 1521. Also ensure that the database systems can’t be accessed over the Internet.

Current State Architecture

Current state configuration of a customers JD Edwards architecture with the complete list of all the servers in scope for the migration to Oracle Cloud Infrastructure.

Customer JDE Instance Details

Customer EU Instance

JDE	9.2 Base release (no updates)
Tools Release	**9.2.0.5**
Total Active Users:	**2,500**
Total Concurrent Users:	**1200**
Database Sizes:	
Non Prod Data:	**11 TB**
Prod Data:	**11 TB**
JDE Foundation:	**1.1 TB**
Servers Platform:	
Prod Database and JDE Enterprise Server:	**AS400 V7R3 BSBPD1**
Non-Prod Database and JDE Enterprise Server:	**AS400 V7R3 BSBPD1**
All other servers:	**Windows**
Web-Tier:	**Weblogic**

\pagebreak

Customer AP Instance

JDE	9.2 Update 5
Tools Release	**9.2.4.6**
Total Active Users:	**494**
Total Concurrent Users:	**300**
Database Sizes:	
__Non Prod Data:	**1.5 TB**
Prod Data:	**1 TB**
JDE Foundation:	**150 GB**
Servers Platform	
Prod Database and JDE Enterprise Server:	**AS400 V7R3 BSBPD1**
Non-Prod Database and JDE Enterprise Server:	**AS400 V7R3 BSBPD1**
All other servers:	**Windows**
Web-Tier:	**Weblogic**

\pagebreak

Environment Sizing

Guide:

A section describing the Current JDE workload of the Customer: Sizing Details, Current On-Premise BoM

Example:

Partner will capture current JDE workload sizing here.

High Availability and Disaster Recovery Requirements

Guide:

This section captures the resilience and recovery requirements for the Workload. 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?*
- *What are the backup requirements*

Example:

The recovery time objective (downtime tolerance) and recovery point objective (data loss tolerance) details are very important considerations for the Customer. The overall DR requirement is a cross-region DR strategy with the goal of minimizing RTO.

Backup and Recovery Practices

Guide:

A section describing the Current JDE workload of the Customer: Backup and Recovery- RTO and RPO

Example:

Current high-level backup and recovery practices are described below:

- File system and Database backups are retained for 30 days for production and at least 7 days for non-production.
- Oracle Recovery Manager (RMAN) is the standard backup tool that handles all JDE workload Databases.
- Backup of the Oracle Databases uses the standard file system agent which backs up the Oracle RMAN disk-based backup to tape.
- Backup frequency standards are:
  - Weekly full,
  - Daily incremental backup, which includes the archive log backups. *Example:*

Security Requirements

Guide:

Capture the Non-Functional Requirements for security-related topics. Security is a mandatory subsection that is to be reviewed by the x-workload security team. The requirements can be separated into:

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

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

Example:

The foundation of security is access control, which refers to how the system is being accessed and by whom. User security consists of three principal components: authentication, authorization, and an audit trail. All current browser-based password login screens send the password as a parameter in the HTTP form submission. Using an HTTPS connection will encrypt this information. The best practice is therefore to use HTTPS for all web-based access. The requirement is to take extra steps to ensure security is not compromised, either from the Infrastructure side or from the Application endpoints.

At the time of this document creation, no Security requirements have been specified.

Workload Access Requirements

Guide:

A section describing the Current JDE workload of the Customer: How the Customer accesses their Application

Example:

The Customer wants to access the JDE application or workload, once they move to OCI, in the same way as they currently do On-Premises. They also need to secure their external internet-facing endpoints from internet threats.

The Customer has both internal and external endpoints of their JDE workload.

Internal Users:

Users access JDE using the URL https://`<Internal LB URL:port>`. The connection flows via the external/internal firewall to the Load Balancer in DMZ. Load Balancer terminates the Secure Socket Layer (SSL) and passes the request on port 8010 to JDE internal servers. The internal JDE servers communicate with JDE RAC Database on Linux VMs using Database listener port 1531 and validate the user request.

External Users:

External users access JDE using the URL https://`<External LB URL:port>`. The connection flows via the external/internal firewall to the Load Balancer in DMZ. Load Balancer terminates the SSL and passes the request on port 8010 to JDE external server.

Workload Monitoring Requirements

Guide:

A section describing the Current JDE workload of the Customer: Monitoring of the Workload

Example:

JD Edwards monitoring can oftentimes be extremely manual and time-consuming. However, Oracle Management Cloud (OMC) provides complete visibility into JD Edwards components and enables you to stay in sync and continuously improve the system.

Future State Architecture

Guide:

The Workload 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.

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

Mandatory Security Best Practices

Guide:

Use this text for every engagement. Do not change. Aligned with the Cloud Adoption Framework

Example:

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

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

CATEGORY	TOPIC
User Management	IAM Defau Domain

CATEGORY	TOPIC
	OCI Emergency Users

CATEGORY	TOPIC
	OCI Administra
	Applicatio Users

CATEGORY	TOPIC
Cloud Posture Management	OCI Cloud Guard

CATEGORY	TOPIC
	OCI Vulnerabili Scanning Service
Monitoring	SIEM Integration

CATEGORY	TOPIC
Additional Services	Budget Control

OCI Secure Landing Zone Architecture

Guide:

This chapter describes landing zone best practices. 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 for brownfield deployments.

Example:

The design considerations for an OCI Cloud Landing Zone have to do with OCI and industry architecture best practices, along with Customer 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.

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, matches Oracle's best practices and Customer requirements.

Oracle recommends the following Resource Naming Convention:

- The name segments are separated by “-“
- Within a name segment avoid using `<space>` 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\>
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\>

Resource Type	Abbreviation	Example
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

Security and Identity Management

Guide:

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

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.

Authentication and Authorization for OCI

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

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.

Customer 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 Customer.

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 Customer using the application, compute instance and database-specific authorization.

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 Customer'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 Customer.

Responder Rules

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

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.

OCI 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.

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.

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.

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.

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.

Regulations and Compliance

Customer 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.

Physical Architecture

Guide:

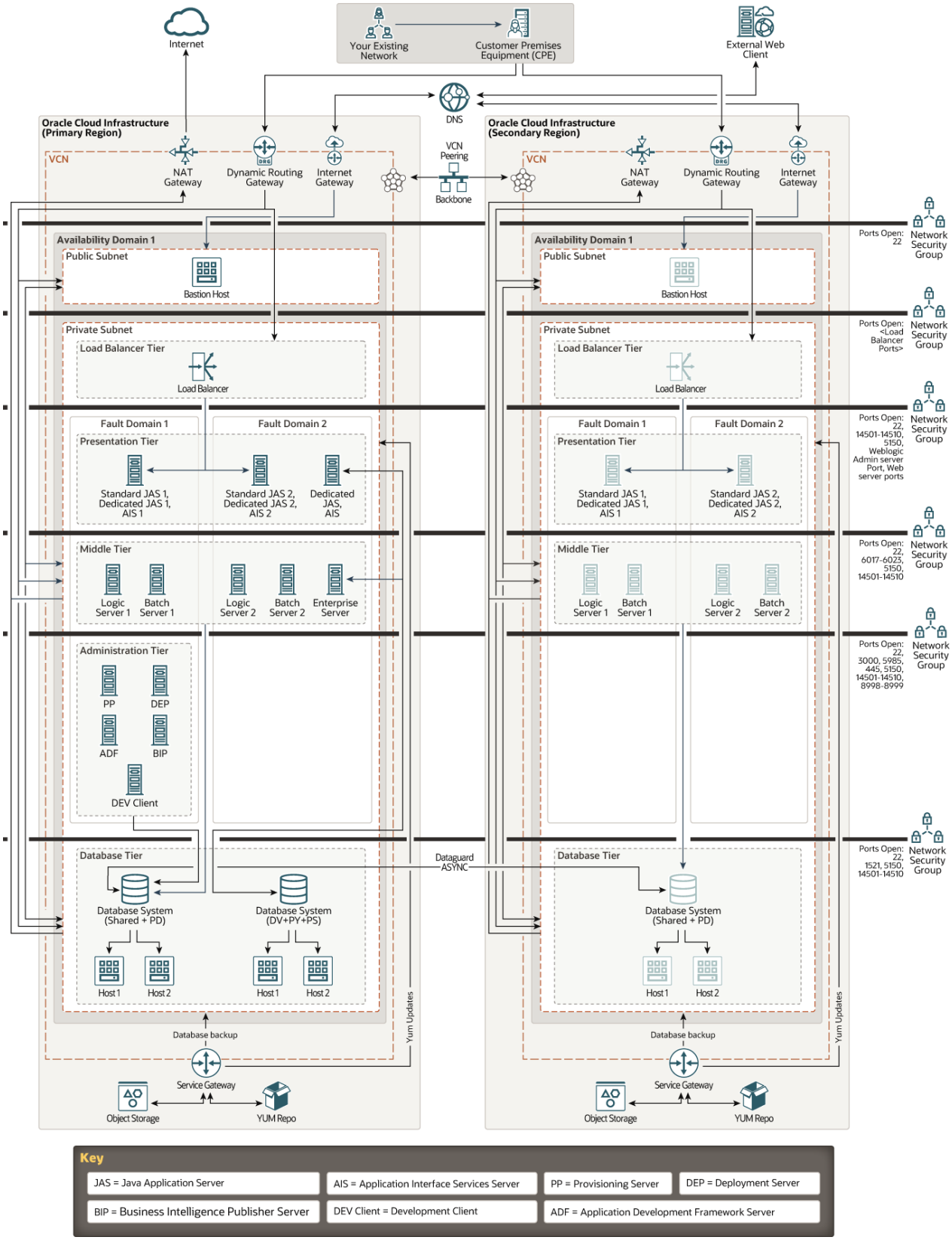
A section describing the Deployment Design and its associated Components in OCI

Example:

The Tenancy of Customer will be managed by a Managed Service Provider. The design plan which has been decided is to create One Tenancy where Virtual Cloud Network (VCN) will be provisioned for both the Customer as well as for Managed Service provider. Traffic for Each VCN will be terminated at their respected Dynamic Routing Gateways (DRG).

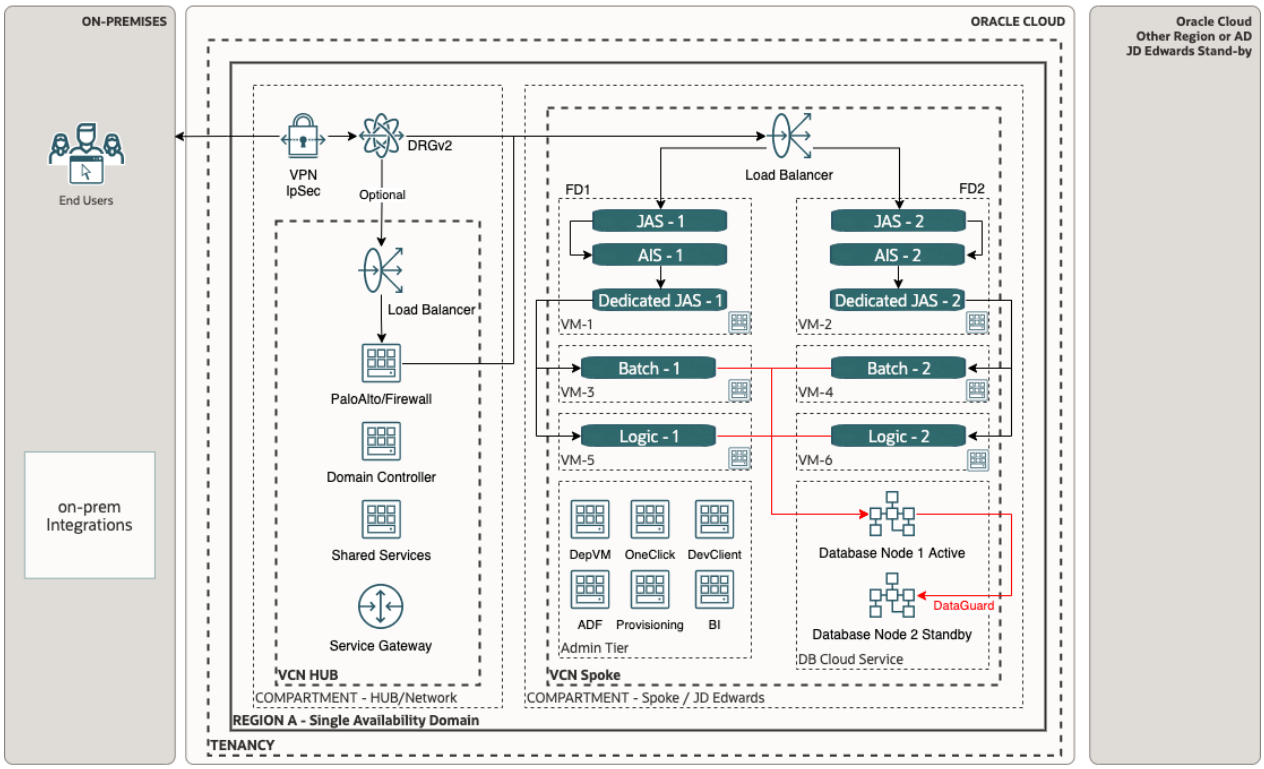
In the **following sections** we are describing the **Deployment Design Diagrams** as well as all the relevant components present in the Design diagram.*

Deployment architecture for the 'JDE-X' environment of the Customers JD Edwards Workload, in OCI - Multi AD DR design diagram, is illustrated below:



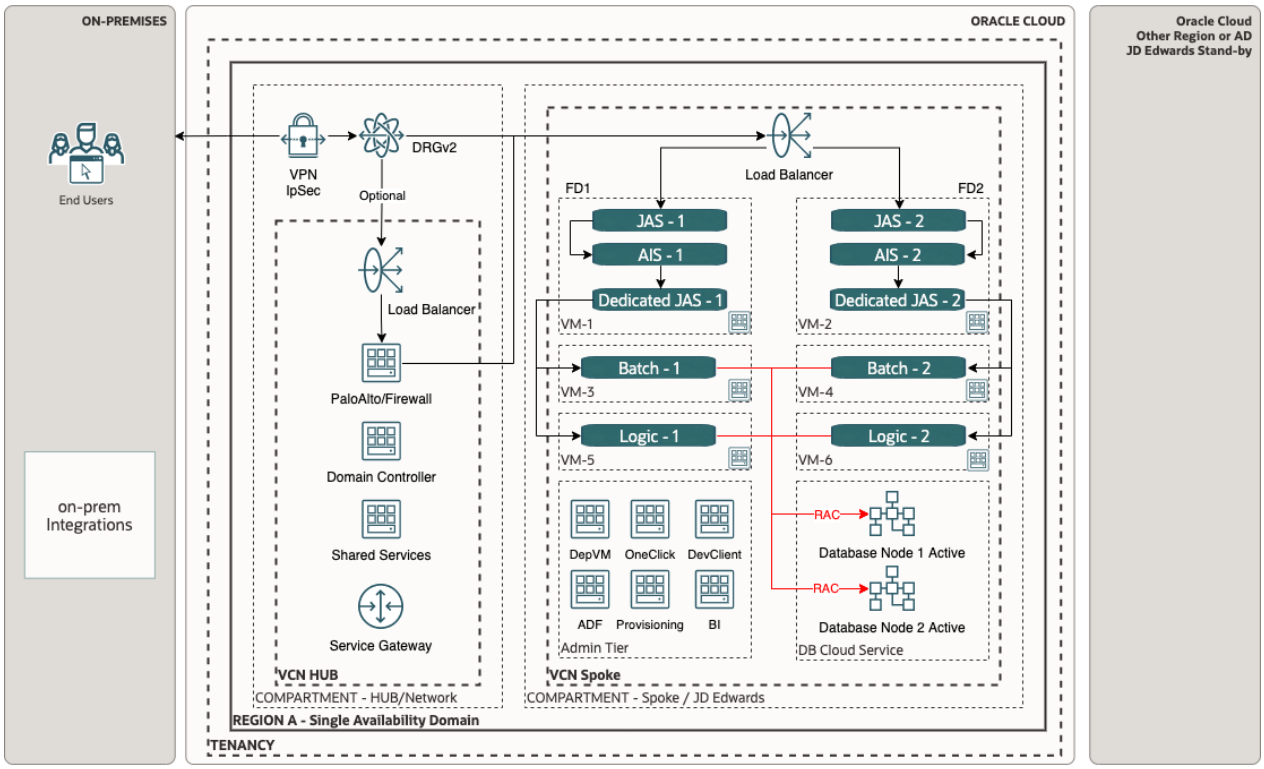
Deployment architecture for the 'JDE-X' environment of the Customers JD Edwards Workload, in OCI - Max Availability Architecture, Single AD design diagram, with Standby Database Node, BRONZE, is illustrated below:

BRONZE

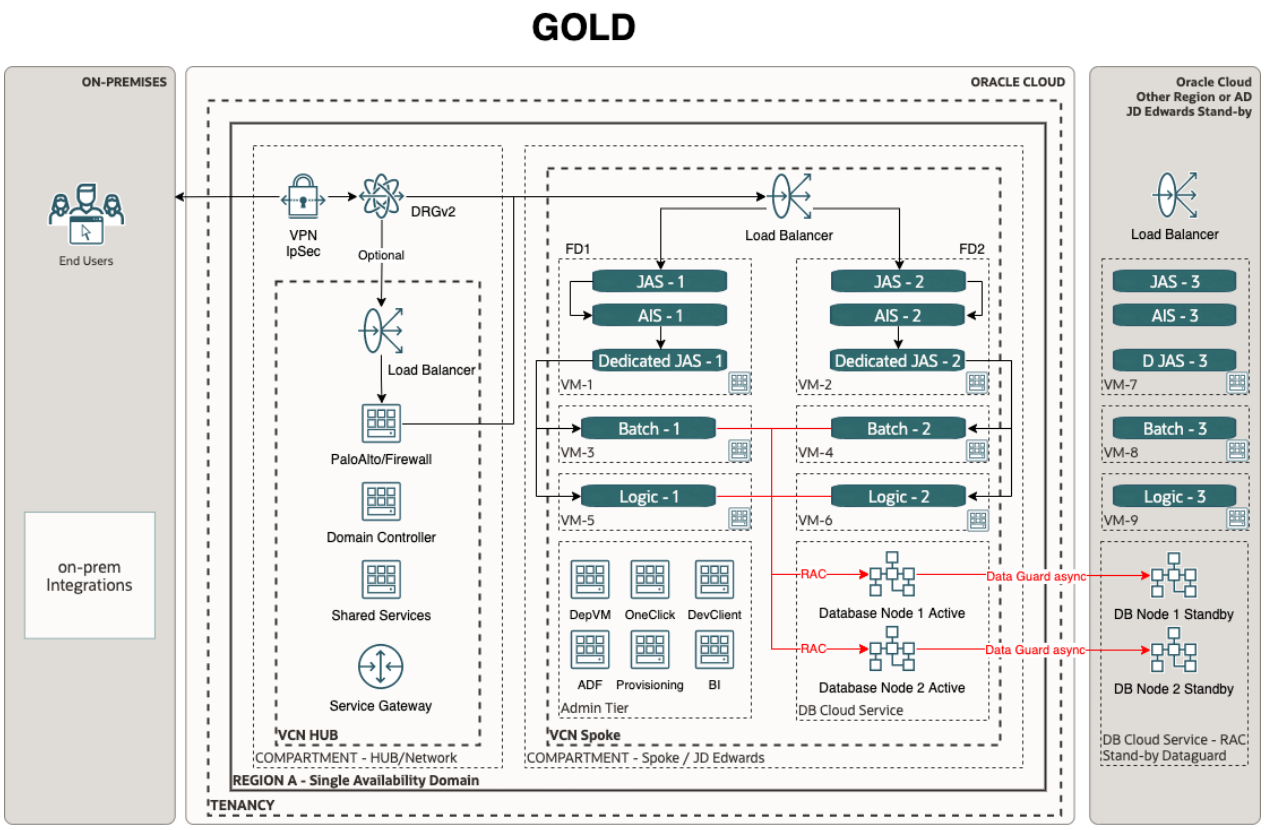


Deployment architecture for the 'JDE-X' environment of the Customers JD Edwards Workload, in OCI - Max Availability Architecture, Single AD design diagram, with RAC enabled Database Nodes, SILVER, is illustrated below:

SILVER

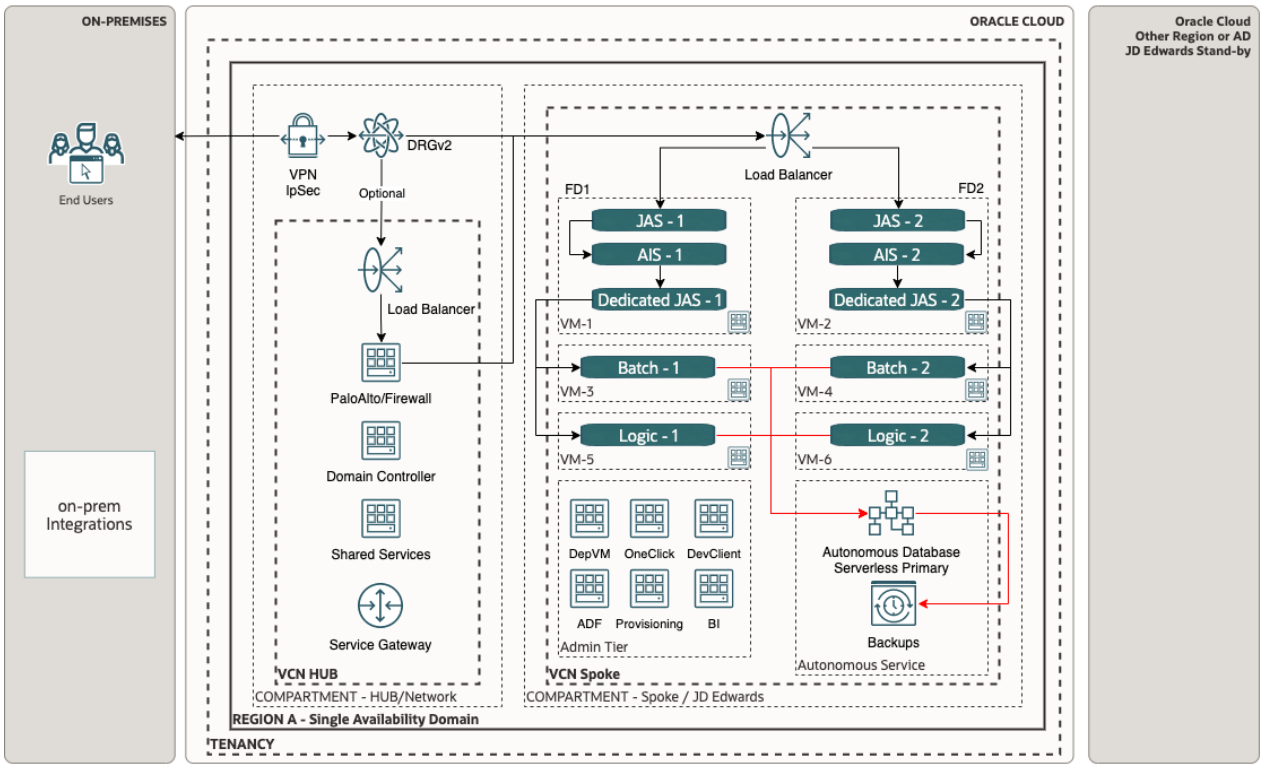


Deployment architecture for the 'JDE-X' environment of the Customers JD Edwards Workload, in OCI - Max Availability Architecture, Multy AD design diagram, with RAC enabled Database Nodes, and remote Standby, GOLD, is illustrated below:



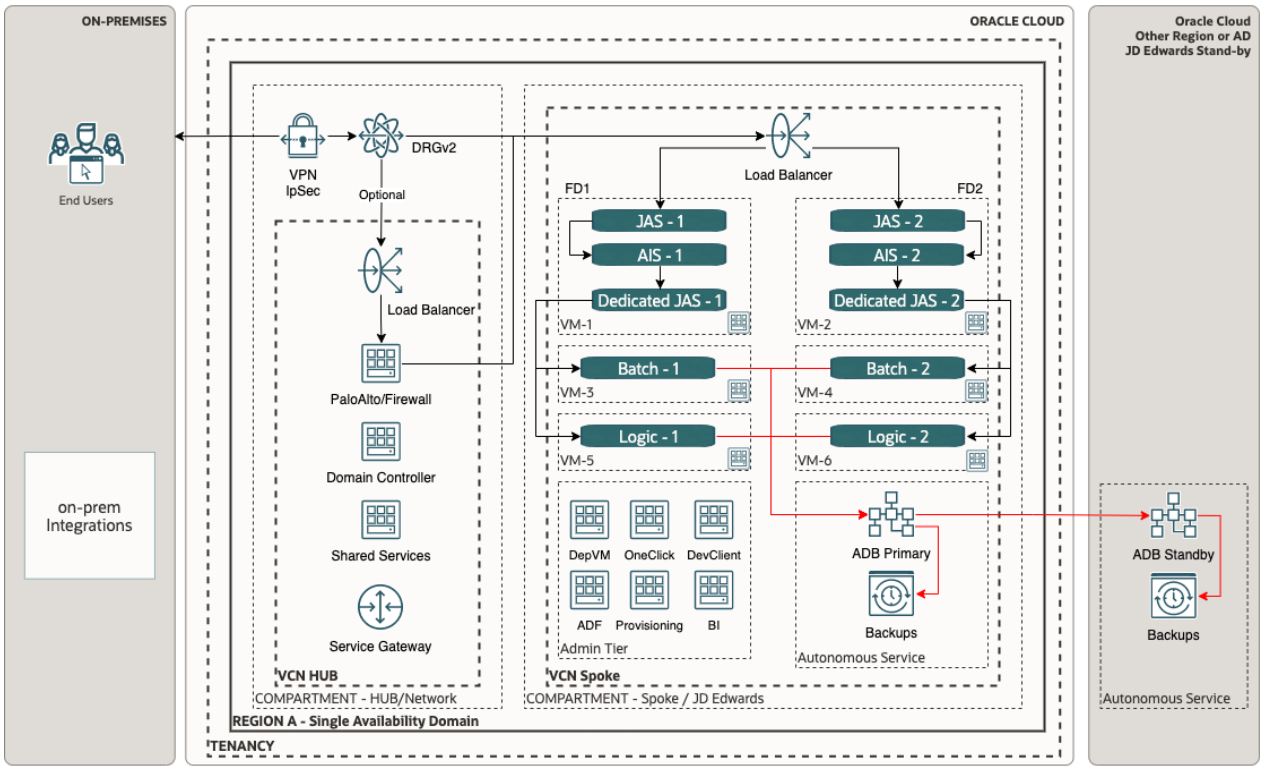
Deployment architecture for the 'JDE-X' environment of the Customers JD Edwards Workload, in OCI - **Max Availability Architecture - ADB** , Single AD design diagram, with ADB Database Nodes, SILVER, is illustrated below:

SILVER

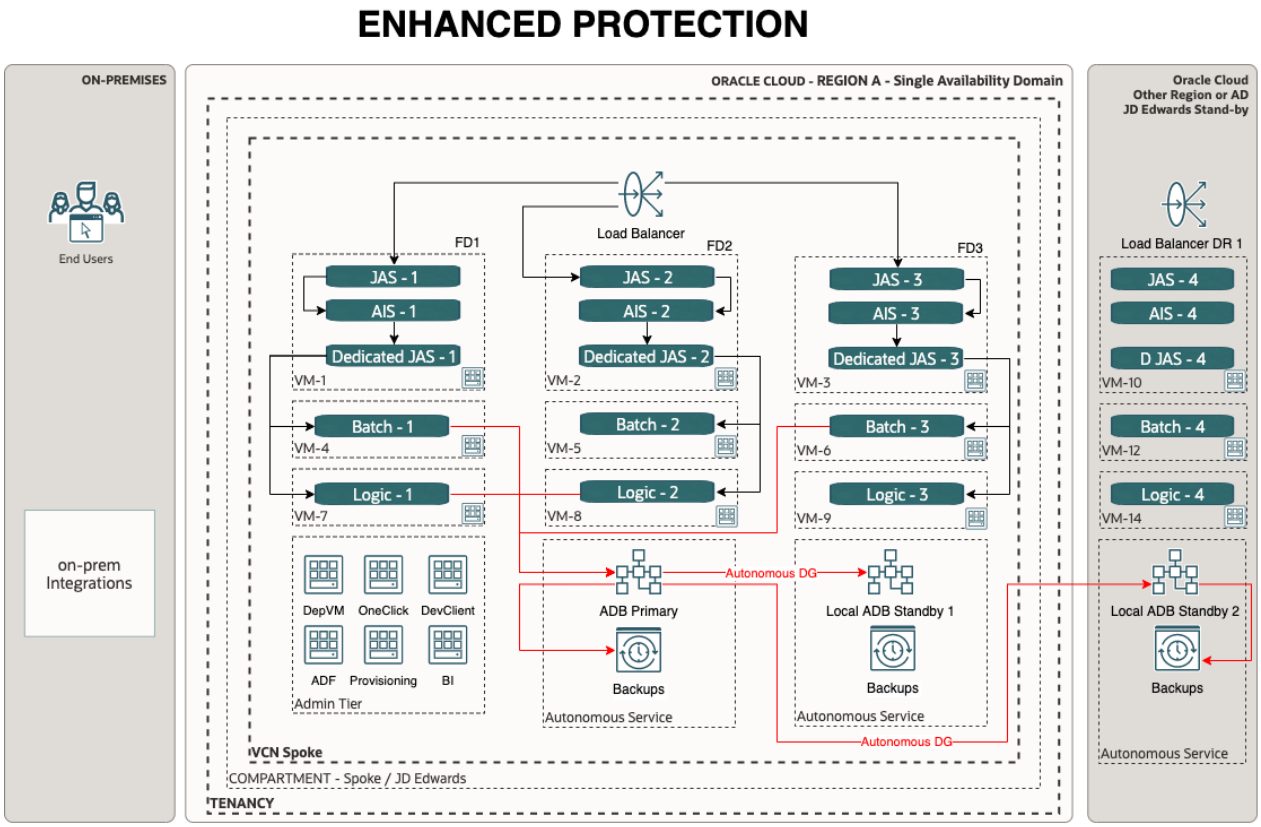


Deployment architecture for the 'JDE-X' environment of the Customers JD Edwards Workload, in OCI - Max Availability Architecture - ADB, Single AD design diagram, with remote standby ADB Database Node, AURUS, is illustrated below:

AURUS



Deployment architecture for the 'JDE-X' environment of the Customers JD Edwards Workload, in OCI - Max Availability Architecture - ADB, Single AD design diagram, with remote standby ADB Database Node and Apps nodes, Enhanced Protection diagram, is illustrated below:



Reference:

The Oracle Cloud Notation, OCI Architecture Diagram Toolkits

Solution Considerations

Guide:

A section describing the Future JD Edwards workload of the Customer in OCI 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?

Example:

The proposed plan is to migrate JDE Application servers in the compute VM shapes on the latest OS and kernel version (which is supported). On-Premises RAC Database (**19c**) will be migrated to a VM-DB RAC system based on a multitenant architecture.

Oracle JD Edwards has a long-term roadmap to support the key capabilities of Oracle Autonomous Database that provide significant benefit to our customers. Oracle Autonomous Database is available through two deployment options: Dedicated Exadata Infrastructure and Shared Exadata Infrastructure. Oracle JD Edwards customers can leverage the capabilities of the Oracle Autonomous Database and reap significant benefits from it.

Oracle Cloud Infrastructure Web Application Firewall (WAF) helps you make your endpoints more secure by monitoring and filtering out potentially malicious traffic. It is a cloud-based, Payment Card Industry (PCI) compliant, global security service that protects applications from malicious and unwanted internet traffic.

High Availability and Disaster Recovery

Guide:

Please describe the Oracle MAA in the context of JDE.

Example:

Oracle Maximum Availability Architecture (MAA) is Oracle's best practice blueprint based on proven Oracle high availability technologies and recommendations. The goal of MAA is to achieve the optimal high-availability architecture at the lowest cost and complexity. Papers are published on the Oracle Technology Network OTN.
To achieve maximum Oracle JKD Edwards database availability, Oracle recommends deploying JDE on an Oracle Database MAA foundation that includes the following technologies:
- Oracle Real Application Clusters (RAC)
- Oracle Data Guard
- Oracle Flashback Database
- Oracle Automatic Storage Management
- Oracle Recovery Manager and Oracle Secure Backup
- Oracle Online Upgrade Using Edition-Based Redefinition

Please refer to the following reference paper for detail.

Reference:

JD Edwards EnterpriseOne High Availability Architecture

Backup and Recovery

Guide:

A section describing the 'Backup and Recovery' practices of the Customer in OCI

Example:

We will follow the current Backup and Recovery strategy and practices of the Customer. Customer has the following Recovery Time Objective (RTO) and Recovery Point Objective (RPO) requirements which will be achieved with the proposed architecture:

- Official RTO practices: less than 24 hrs
- Official RPO practices: 4 hours

Security

Guide:

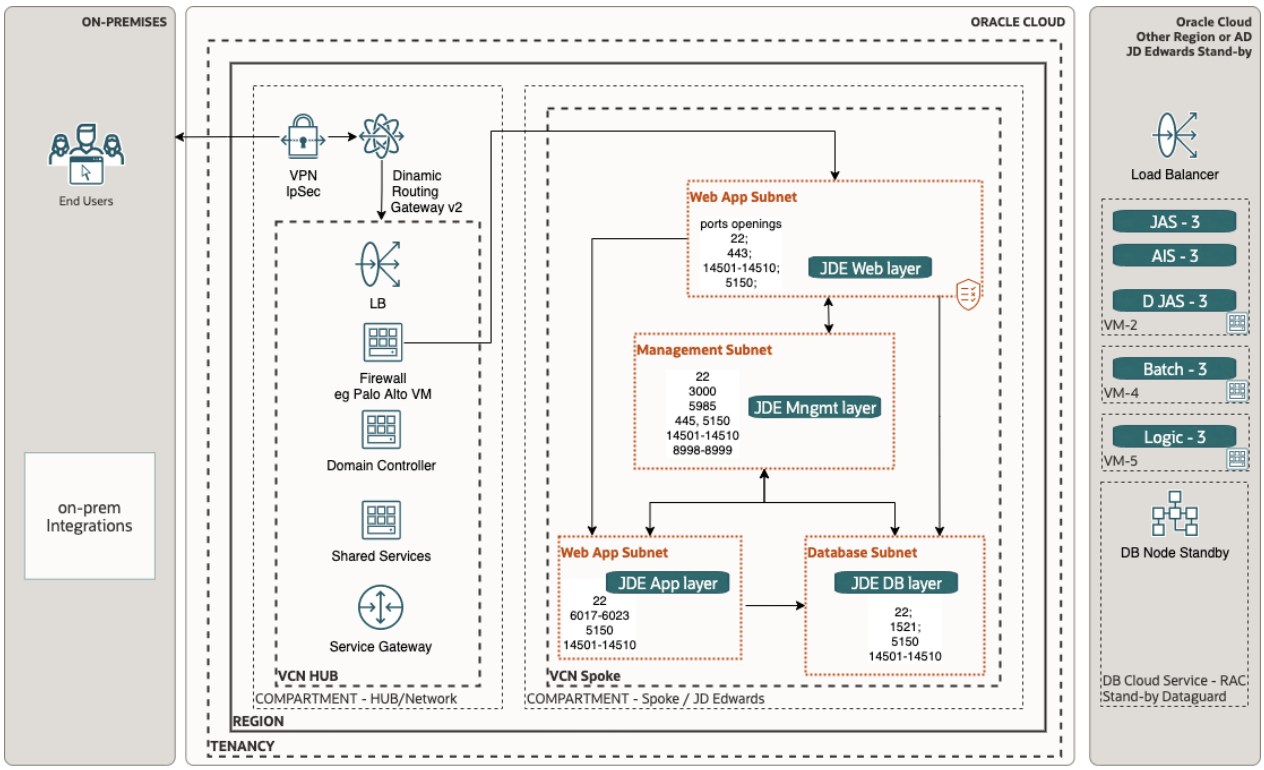
A section describing the Security in OCI in the context of the JDE Application

Example:

The objective of the security architecture is to enable you to maintain your security posture when running JDE and associated applications in the Oracle Cloud.

Oracle has designed security into every aspect of our infrastructure to help our customers achieve better protection, isolation, and control. We started by taking a unique design approach, separating the network and server environments. This way, if an attack occurs on a VM, we can contain that threat and prevent it from moving to other servers, resulting in better protection and lower risk for customers.

We also hyper-segment our physical network and backend infrastructure for secure isolation between customer instances and backend hosts. Additionally, we've implemented a hardware-based root of trust, making sure each server is pristine each and every time it is provisioned.



Note: Please see generic OCI security guidelines in the Annex.

For each customer's VCN there is a range of defense in depth protections available spanning across **layers 3-7**.

VCN (1): A VCN provides isolation for your workload from any other workload on Oracle Cloud Infrastructure, including your other workloads in a different VCN.

Internal Firewalls (2): Implement virtual firewalls at the subnet level using VCN security lists.

Load Balancing Traffic Securely (3): TLS 1.2 is supported by default to securely balance traffic within the implementation and from external connections.

Secure Traffic Between ADs and Regions: Communications between ADs are encrypted with Media Access Control security (MACsec) to prevent layer 2 security threats such as wiretapping, DDoS, intrusion, man-in-the-middle, and playback attacks. VCN traffic that travels between regions is either sent over private links or is encrypted.

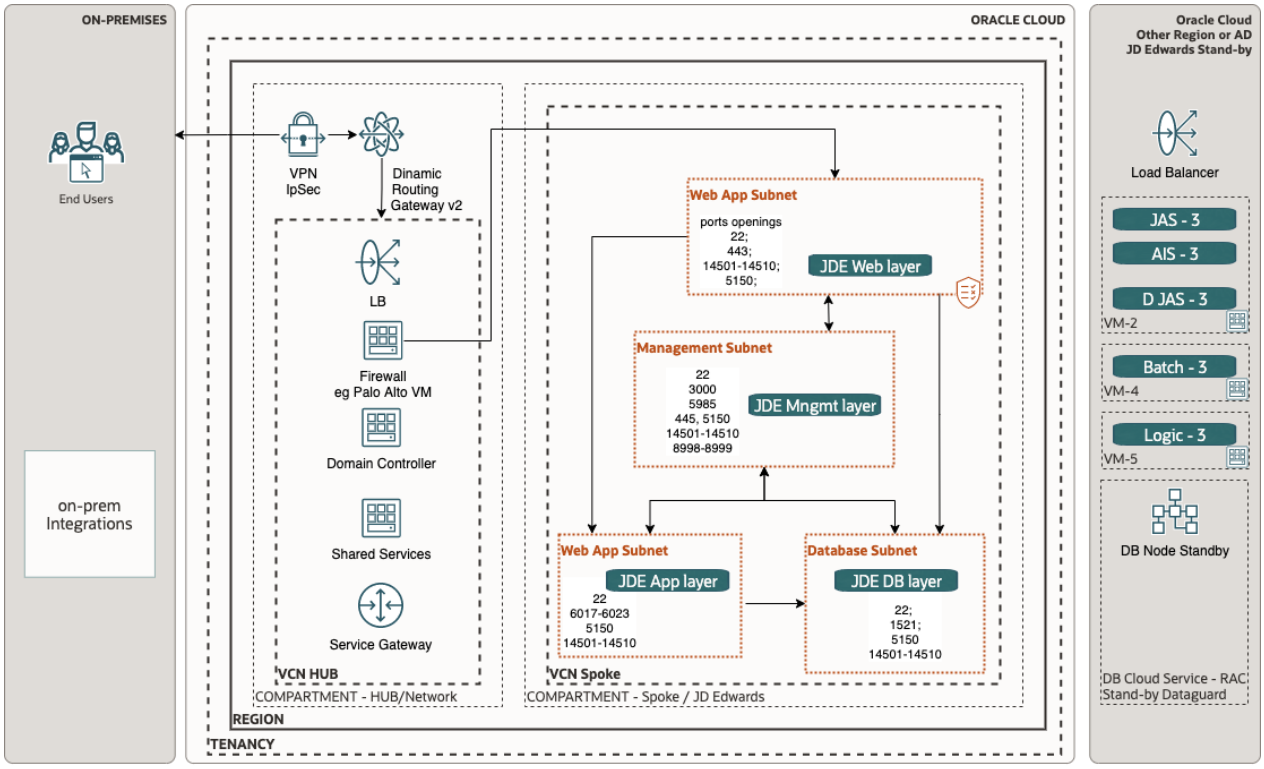
Secure Connectivity to Public Internet (4): For security, a VCN has no internet connectivity by default. Therefore, internet-bound traffic to/from a VCN must pass through an IGW. Virtual routing tables can be implemented with private IP addresses for use with NAT and 3rd party firewall devices for additional security.

Secure Connectivity Between Your VCN and Data Center (5): Traffic can be routed through a DRG for private traffic. It is used with an IPSec VPN or FastConnect connection to establish private connectivity between a VCN and an On-Premises or other cloud network.

Protect Internet-Facing Applications (6): Oracle Cloud Infrastructure Web Application Firewall is a regional-based and edge enforcement service that is attached to an enforcement point, such as a load balancer or a web application domain name. WAF protects applications from malicious and unwanted internet traffic. WAF can protect any internet-facing endpoint, providing consistent rule enforcement across a customer's applications. It also inspects any request going from the web application server to the end user. Additionally, Oracle's optional global 'anycast' DNS service also takes advantage of DNS-based DDoS protections providing resiliency at the DNS layers.

- Specific to some use cases: Route details for a specific use case like Hub and Spoke

- Application authentication and authorization details (If applicable how Application users are going to access the Application and associated privilege control mechanism(for example role-based access control), federation with other IdP like Microsoft/Azure AD)
- Specific to some use cases: Using any specific security services available in OCI like Security Zone, Security Advisor
- Specific to some use cases: Customer from specific industries (Financial) might require PCI-compliant services like WAF
- Oracle JD Edwards requires policies with the following ports and protocols to be open



__Note:__Please see generic OCI security guidelines in the Annex.

Workload Access

Guide:

A section describing how Customer will access their Application in OCI

Example:

Customer will access the JDE workload internally over the OCI FastConnect connectivity solution and JDE external endpoints will be secured by OCI Web Application Firewall (WAF). FastConnect is a private, dedicated connectivity that improves security, it supports bandwidths from 1Gbps to 10Gbps.
An alternative option to FastConnect is Virtual Private Network (VPN). VPN could also be a backup configuration if FastConnect is down.

Workload Monitoring

Guide:

A section describing how Customer will monitor their Application in OCI

Example:

JD Edwards monitoring can oftentimes be extremely manual and time-consuming. However, Oracle Management Cloud (OMC) provides complete visibility into JD Edwards components and enables you to stay in sync and continuously improve the system.

From the homepage, you can monitor the performance of the JD Edwards application from your end-user perspective in the Pages pane, analyze your server workloads in the Server Requests pane, and identify problems in associated tiers and drill down into operational data in the AppServers pane.

Oracle Management Cloud monitors all of the following elements of your JD Edwards environment:

```
- User activities
- System performance
- Critical jobs not completing in time
- Slow, bad running jobs, etc.
```

Reference by Quest:

Monitor JD Edwards or Peoplesoft using OCI Application Performance Monitoring

Regulations and Compliances

Guide:

A section describing any Customer-specific 'Regulation and Compliance if any' in OCI

Example:

None has been discussed at the time of Migration.

JD Edwards One-Click Provisioning Tool

Guide:

A section describing the JD Edwards One-Click provisioning tool for JDE Workload

Example:

What is JD Edwards One-Click provisioning

JD Edwards One-Click provisioning provides an easy-to-use, automated framework for deploying JD Edwards EnterpriseOne environments. It introduces a console that provides an automated process for deploying and scaling out a JD Edwards EnterpriseOne environment with a single click. Configure your account details and orchestrate your deployment plan by choosing the JD Edwards EnterpriseOne components, server names, and virtual machine sizes to deploy.

What means Migrating JD Edwards EnterpriseOne to Oracle Cloud

Currently, the Oracle Cloud Migration Utility only supports the migration of a single pathcode from your on-premise environment to the Compute Service instance environment. You can only run this process a single time from end to end. However, you do have the option to import from one on-premise pathcode to a different pathcode on the Compute Service instance. For example: you can export your on-premise PD920 environment and import to DV920 on the Compute Service instance. The utility has scripts packaged within the database migration that will synchronize the database records accordingly.

The Oracle Cloud Migration Utility can be used only if the on-premises environment is running at least Tools release 9.2.x with Applications 9.1 and later. After the migration is complete, your cloud compute instance will be running the same applications release as your on-premises environment.

- Supported on-premises environment
- Enterprise One Applications release 9.1 and later
- Enterprise One Tools 9.2
- Oracle database on Linux
- This is Oracle's recommended way to deploy JD Edwards on OCI

Migrating JD Edwards EnterpriseOne to Oracle Cloud

OCI Networking

Guide:

A section describing OCI networking capabilities and features

Example:

Oracle Cloud Infrastructure (OCI) networking and connectivity products and services enable customers to manage and scale their networks.
Please refer to the following article for a better understanding of OCI networking capabilities and how they can be leveraged for Customer advantage.

Reference:

- Oracle's Networking capabilities
- OCI Networking Best Practices
- Best practices for hybrid and multicloud OCI networking design

Sizing and Bill of Materials

Guide:

A section describing the Future JDE workload sizing in OCI

Example:

A sample sizing of the JDE workload is reflected in the diagram below for reference purposes:

OCI - JDE Bill of Materials MISSING

Annex

Security Guidelines

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.

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.

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).

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