

ORACLE

JD Edwards on Oracle Cloud Infrastructure

Validated Solution Guide

May 30, 2019

Copyright © 2020, Oracle and/or its affiliates

Purpose statement

This validated solution guide provides an overview of procedures, supporting services, reference architectures, and the business benefits you can gain when you move JD Edwards to Oracle Cloud Infrastructure. It is intended solely to help you assess the business benefits of migrating JD Edwards to Oracle Cloud Infrastructure and to plan your IT projects.

Disclaimer

This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this confidential material is subject to the terms and conditions of your Oracle software license and service agreement, which has been executed and with which you agree to comply. This document and information contained herein may not be disclosed, copied, reproduced or distributed to anyone outside Oracle without prior written consent of Oracle. This document is not part of your license agreement nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

This document is for informational purposes only and is intended solely to assist you in planning for the implementation and upgrade of the product features described. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle.

Due to the nature of the product architecture, it may not be possible to safely include all features described in this document without risking significant destabilization of the code.

Table of contents

Solution Overview	4
Audience and Business Problem	4
Top-Level Value Proposition	4
TCO Analysis	5
Unique Infrastructure and Tools	5
Proven Customer Success	6
Validated Solutions that Address All Business Requirements	6
Key Workload Requirements	6
Architectures that Meet These Requirements	7
Networking and Connectivity Best Practices	7
Resiliency and High Availability Best Practices	9
Disaster Recovery / Multi-Availability Domain Best Practices	10
Single Region Reference Best Practices	11
Multiple Region Disaster Recovery Best Practices	12
Migration Best Practices	12
Security and Identity Best Practices	14
Cost Management and Governance Best Practices	16
Monitoring	17
Additional Resources	18

Solution Overview

Audience and Business Problem

Typically, JD Edwards customers have made significant investments in building on-premises or hosted implementations. These include specific hardware and architecture choices, software configurations, and third-party integrations, as well as management tools, internal processes, and training.

In order to gain the benefits of faster infrastructure updates, easier scaling up (and down), lower CapEx, and less personnel dedicated to basic infrastructure maintenance, many datacenter applications and operations are moving to the cloud. But teams managing database-intensive workloads like JD Edwards often don't go the route of traditional cloud deployment due to concerns about cost, performance, re-architecting, compatibility, and expertise. Frankly, to most, deploying JD Edwards in the cloud sounds like a science project — there seems to be no guarantee that the results will be worth the risk.

This Validated Solution Guide will provide an overview of the outcomes possible when moving JD Edwards to Oracle Cloud Infrastructure (OCI), proof points for these outcomes, and highlights of the tools and architectures recommended by Oracle to achieve these outcomes. The first part of this document focuses on overall outcomes, Oracle's unique capabilities, a Total Cost of Ownership (TCO) analysis, and short customer case studies. The second part of this document describes typical enterprise technical and business requirements, and shows many of the specific tools, components, and architectures that help achieve them.

Top-Level Value Proposition

Most on-premises JD Edwards EnterpriseOne deployments can be migrated to run on OCI without significant configuration, integration, or business process changes, and will result in an implementation that is more flexible, reliable, higher performance, and lower cost than either on-premises or other cloud approaches.

Oracle has a validated solution to accomplish these outcomes quickly and reliably, which includes procedures, supporting OCI platform services, and reference architectures. These consider real production needs, like security, network configuration, high availability and disaster recovery (HA / DR), identity integration, and cost management.

Running JD Edwards on OCI offers a number of benefits:

- High availability with RTO < 4 hours and RPO < 4 hours
- Much greater resiliency in primary datacenter than is possible on premises
- Rapid, in-place technology refresh and patching
- Proactive costs and usage monitoring
- Near-instant scaling up or down
- Federated identity with your existing systems
- Fast provisioning time for new JD Edwards environments

In other words, moving to OCI could be the last significant upgrade you need to do.

TCO Analysis

Beyond being straight-forward to migrate, easier to manage, and more flexible to scale, a JD Edwards implementation on OCI is actually cheaper than running it on-premises or in another cloud.

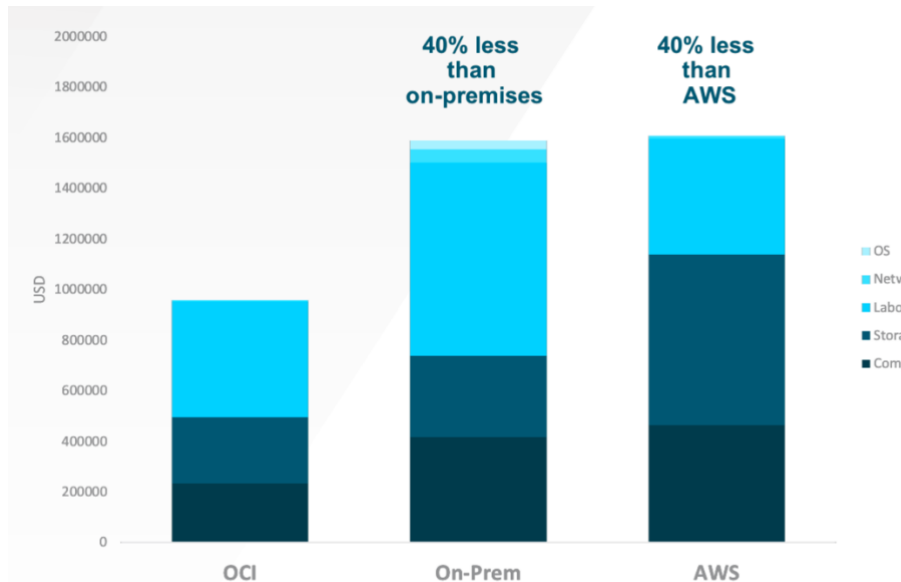


Image 1 Operating JD Edwards in OCI can be as much as 40% cheaper than continuing to run as an on-premises deployment, or even on another cloud provider.

Unique Infrastructure and Tools

These advantages exist because OCI was designed specifically to support workloads like JD Edwards by the people who make JD Edwards. OCI delivers higher-performance compute, storage, networking, and managed database instances that result in a better experience for your users at a lower cost of operation. OCI is the only cloud where you can run JD Edwards with RAC or Exadata. Other clouds are limited to less robust configurations.

In addition, Oracle provides JD Edwards-specific tooling and automation to streamline deployment, migration, upgrading, and maintaining your implementation, reducing the time and expertise needed, as well as the risk and cost of migration and day-to-day operations. Tools include:

- **One-Click Provisioning Console:** The One-Click Provisioning console allows customers to deploy JD Edwards EnterpriseOne on OCI in three simple steps: configure, orchestrate, and deploy. Customers simply configure server manager details, create a deployment plan, and initiate scripts for automated provisioning.
- **JD Edwards Terraform Scripts:** Terraform, or open-source infrastructure as code, allows users to quickly and easily deploy JD Edwards on OCI.
- **Enterprise Manager and Oracle Management Cloud for Hybrid Application Management:** Get a unified view of the health and performance of your application and infrastructure in a multi-cloud and / or hybrid cloud environment.

Proven Customer Success

These are not idle claims. Many JD Edwards customers have achieved these results for themselves, for example:

- **TruGreen** is the largest lawn-care company in the U.S., with 13,000 employees and \$1.3B in annual revenue. The company replaced its outdated JD Edwards, Websphere, DB2, and AIX stack with modern infrastructure and software with the help of Oracle and system integrator Velocity Technology Solutions. Velocity's VCAMP orchestration tool uses Oracle Cloud APIs to automate deployment and management. TruGreen tripled end-user performance, reduced its ERP query response time to 0.09 seconds (down from 0.25-0.40 seconds), and achieved a 30-40% TCO savings, as well as better security isolation than on other clouds.
- **Phibro Animal Health Corporation** is a diversified global developer, manufacturer and supplier of a broad range of animal health and mineral nutrition products for livestock. The company helps veterinarians and farmers produce healthy, affordable food while using fewer natural resources. Every tier of Phibro's JD Edwards implementation was too old to support, and it faced global load-balancing challenges. As part of its OCI migration, Phibro upgraded to a much more current version of JD Edwards, drove average user response time down from 0.32 seconds to 0.13 seconds (a 40% reduction!). At one point, the local admin team was troubleshooting a recurring heavy load spike and was able to scale up CPUs for the affected process. The cost of adding the extra CPUs on demand was 97% cheaper than the on-premises alternative of procuring and operating additional physical servers, as well as much faster to deploy.

Validated Solutions that Address All Business Requirements

Because OCI was built for exactly the type of usage pattern found in applications like JD Edwards, existing deployments can be easily moved and even improved on OCI with little or no modification to the environment or your business processes. Oracle can provide architectural patterns that meet all your networking, connectivity, performance, HA, DR, and multi-region requirements.

Key Workload Requirements

Most JD Edwards customers have a similar set of requirements for any migration project. Below are questions they might ask before migrating to OCI:

- How can we implement a full HA / DR capability?
- How do we deploy a secure architecture and integrate with our identity management system?
- How do we match our high-performance, highly isolated network model?
- How do we deploy or migrate into the cloud?
- How do we maintain control over — and visibility into — operating costs, especially for multiple departments?
- Can our current version be supported? Can it be easily updated once in the cloud?

Architectures that Meet These Requirements

In customer deployments, there are many variations of architecture that will work. In some cases, these variations are designed to achieve a particular outcome; in other cases, they are to support a particular hardware capability (or limitation). In still others, variations reflect the preferences of the architect. In every case, designing a new architecture can be time-consuming and comes with the risk that some important consideration will be overlooked.

In this Validated Solution Guide, Oracle provides a baseline architecture that takes best advantage of OCI capabilities, and also addresses most of the important technical and business requirements. This guide allows you to be confident in achieving your deployment objectives without investing in a long analysis project.

To meet any special requirements not covered by this reference architecture, other design choices are possible. Oracle expects that the design process for those changes is much easier when starting from a reference architecture.

Networking and Connectivity Best Practices

OBJECTIVES

- Access from corporate campus(es) to the application via private network links or encrypted links over the public Internet
- Access from remote offices or mobile workers via public Internet endpoints
- Private network connectivity to other systems or services hosted on OCI
- Network-level isolation between application tiers
- Monitoring and management access to all application and database tiers
- Load-balancing across multiple application nodes for performance and availability
- Isolation from other customers and your other workloads

REFERENCE ARCHITECTURE

Dedicated Network Access via FastConnect (1): Multiple partners in regions across the world offer dedicated network connections between customer premises and Oracle datacenters. This allows customers to access their JD Edwards implementation as if it was running in their own datacenter.

Secure Network Access via IPSec VPN (2): For lower cost, but still secure access over the internet, you can use an encrypted Internet Protocol Security (IPsec) virtual private network (VPN) tunnel to connect from your HQ or on-premises data center to your JD Edwards resources in OCI. From your on-premises environment, you can access your cloud instances in a private subnet by connecting through a Dynamic Routing Gateway (DRG). The DRG is the gateway that connects your on-premises network to your cloud network. Read more about [IPSec VPN](#).

Built-in, Pre-Configured OCI Load Balancing (3): Pre-configured, redundant load balancers are available on private and public subnets to balance traffic within the implementation and from external connections, respectively.

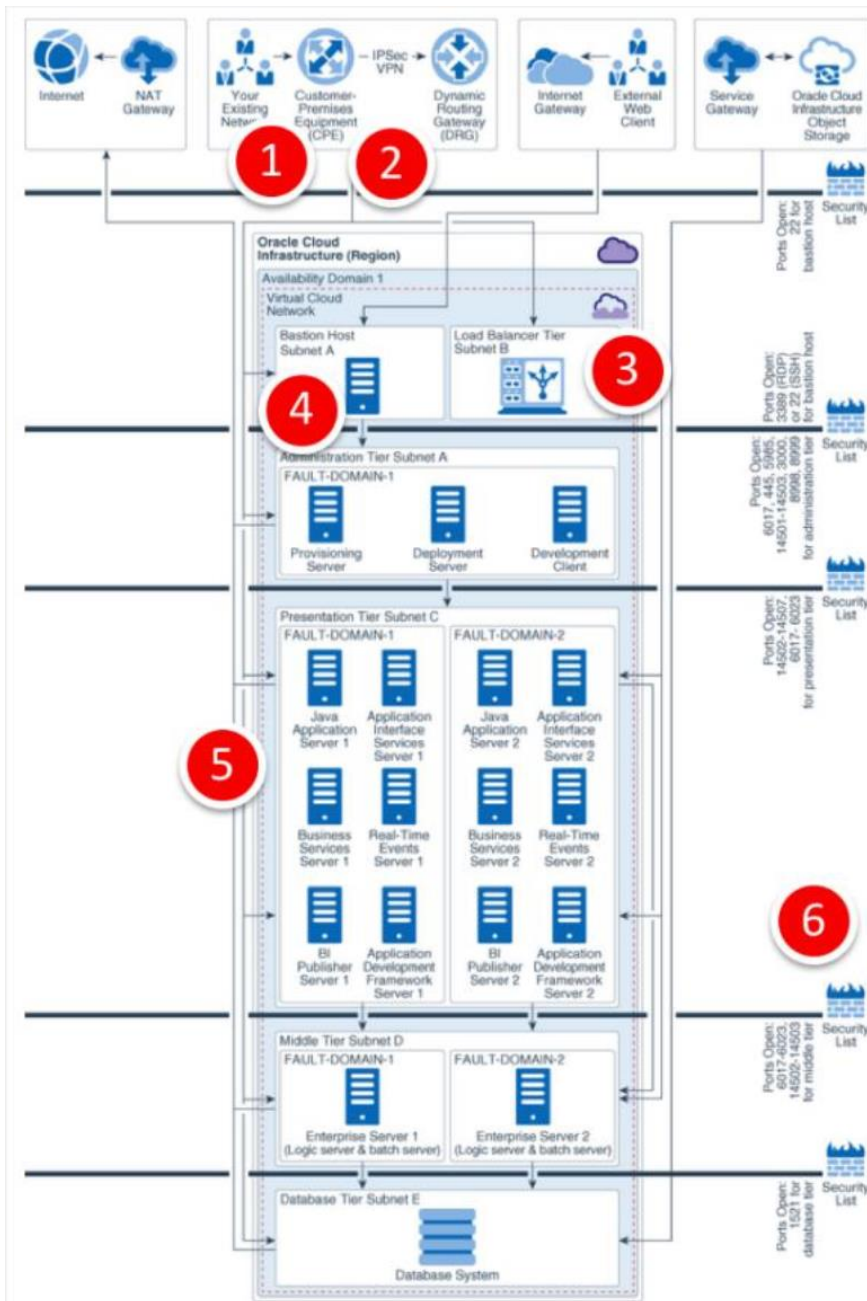


Image 2 Networking reference architecture

Secure Access to Any Tier via the Bastion host (4): The bastion host is an optional component that can be used as a jump server to access OCI instances in the private subnet. You can also access the instances in the private subnet by using dynamic SSH tunneling.

On-Cloud Network Isolation via Virtual Cloud Network (5): A virtual cloud network (VCN) is basically your own private network within OCI. It provides isolation for your JD Edwards workload from any other workload on OCI, including your other workloads in a different VCN. You can subdivide your VCN using subnets to ensure resource isolation and apply security rules to enforce secure access. You can also add route tables and rules to send traffic out of your VCN, similar to traditional network route rules.

You can create instances in a private or a public subnet based on whether you want to permit access to the instances from the internet. Instances that you create in a public subnet are assigned a public IP address and you can access

these instances from the public internet. Conversely, you cannot assign a public IP address to instances created in a private subnet, therefore you can't access these instances over the internet. You can, however, add a [NAT Gateway](#) to your VCN to give instances in a private subnet the ability to initiate connections to the internet and receive responses for the purposes of applying OS and application updates. NAT gateways won't receive inbound connections initiated by the internet.

We recommend creating separate subnets for each tier, such as bastion host, database, application, and load balancing, to ensure that appropriate security requirements can be implemented across the different tiers. You can read more about [VCNs and Subnets](#).

Multiple Internal Firewalls (6): A security list provides a virtual firewall for each tier, with ingress and egress rules that specify the types of traffic allowed in and out. Read more about [Security Lists](#).

Resiliency and High Availability Best Practices

OBJECTIVES

- Multiple active-active nodes at each application tier
- System resilience – using multiple fault domains
- Backup strategy for non-database tiers
- Redundancy strategy for database tier
- Backup strategy for database tier

REFERENCE ARCHITECTURE

Active-Active Server Redundancy (1): To ensure high availability within an availability domain (AD), deploy redundant instances of every component making use of fault domains. All instances are active and they receive traffic from the load balancer and middle tier.

System Resilience (2): Fault domains are a grouping of hardware and infrastructure that is distinct from other fault domains in the same AD. Each AD has three fault domains. By properly leveraging fault domains, you can increase the availability of applications running on OCI.

Database Redundancy (3): For performance and HA 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 OCI.

Backup Strategy Application Tier (4): Backup of the application tiers can be configured by using the policy-based backup feature of OCI Block Volumes. OCI Block Volumes provides you with the capability to perform volume backups automatically based on a schedule and retain them based on the selected backup policy.

Backup Strategy Database Tier (5): Use of OCI Object Storage to perform a backup by using Oracle Recovery Manager (RMAN). To back up or patch the database to OCI 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.

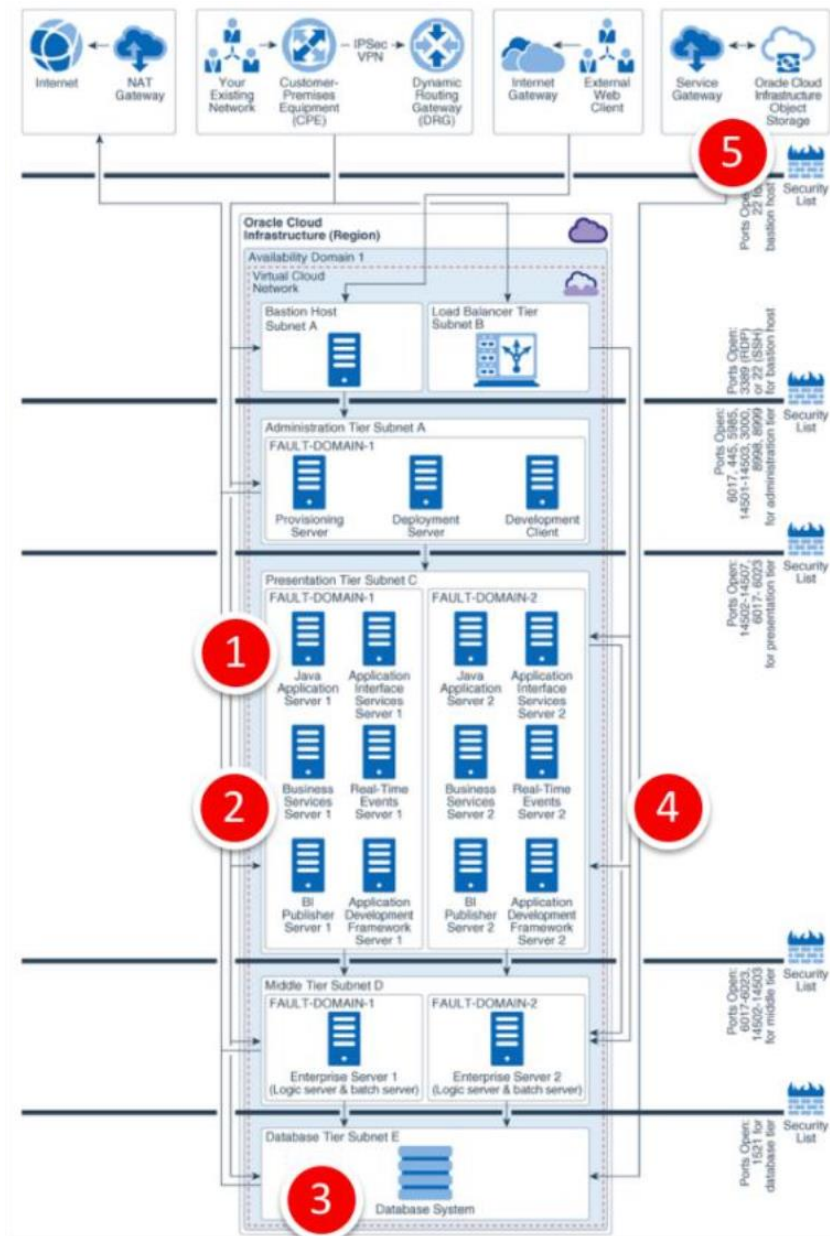


Image 3 Resilience and availability reference architecture

Disaster Recovery / Multi-Availability Domain Best Practices

OBJECTIVES

- Single Region DR
 - Active-active components across ADs – Active-passive components across ADs – Regional subnets across ADs
 - Load balancing across ADs
 - Storage synchronization across ADs
 - Database DR across ADs
- Multiple Region DR
 - Application replication between regions
 - Storage replication between regions
 - Cross-region copy lets you asynchronously copy Object Storage

- Cross-region backup copy for OCI block volumes
- Database protection between regions

Single Region Reference Best Practices

Active-Active Components Across ADs (1): Clustering of supported services across ADs provides protection from an AD failure. For an Active-Passive architecture, synchronize application servers across availability domains using rsync.

Regional Subnets Across ADs (2): Regional subnets span the entire region, providing resilience against AD network failure, as well as simplified JDE service deployment and management.

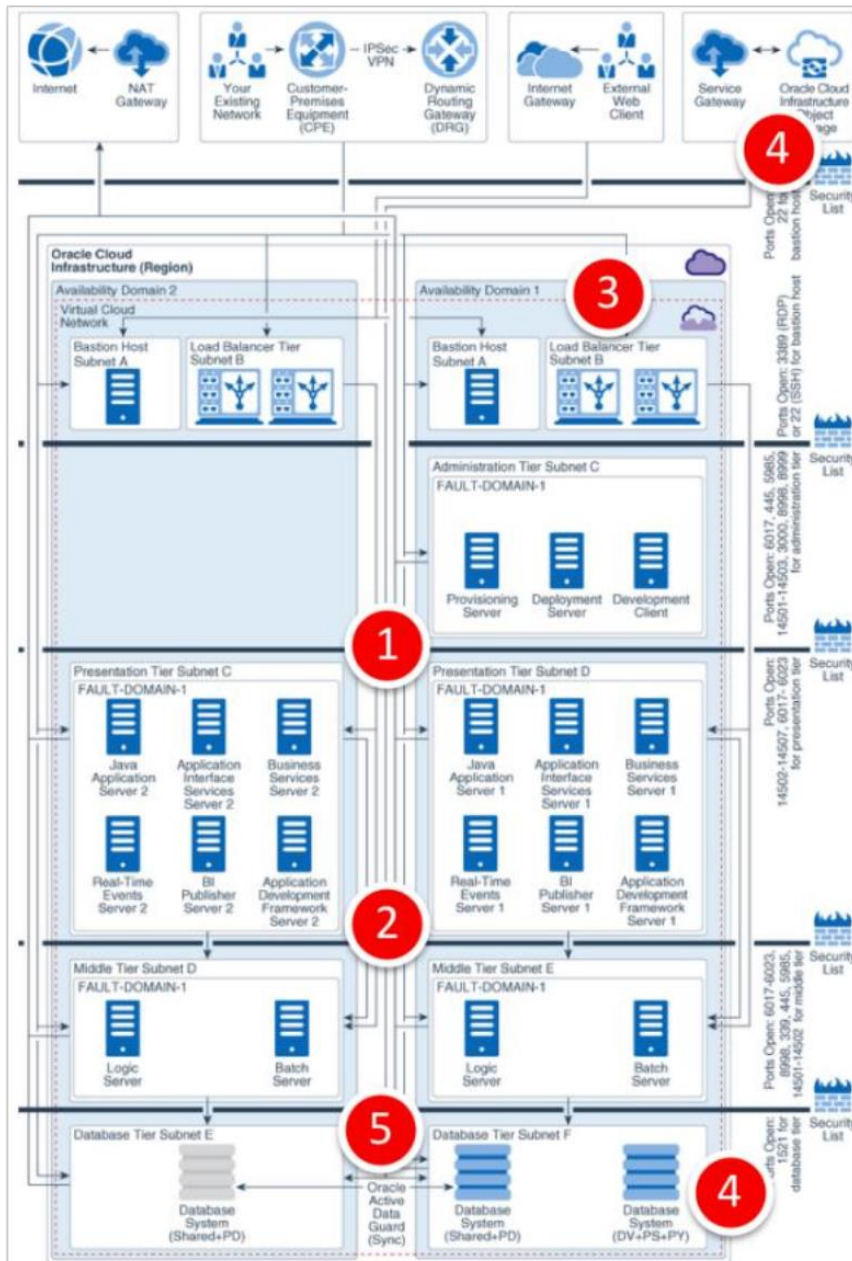


Image 4 Single Region Reference Best Practices

Load Balancing Across ADs (3): OCI Public Load Balancing distributes traffic across JD Edwards servers across all configured ADs, providing protection from an AD failure.

Storage Synchronization Across AD (4): Block Volume backups (boot and block) are replicated across all the ADs within a region and can be restored to any AD within the same region. Object Storage is a regional service. Data is stored redundantly across multiple storage servers and across multiple ADs automatically.

Database DR Across ADs (5): Data Guard or Active Data Guard may be selected dependent on your use case and database edition. Active Data Guard requires Enterprise Edition – Extreme Performance.

Multiple Region Disaster Recovery Best Practices

Active-Active Components Across ADs: Clustering of supported services across ADs provides protection from an AD failure.

Active-Passive Components Across Regions: If you are using Active-Passive to synchronize application servers across ADs, use rsync.

VCN Peering Across Regions: VCNs can connect between regions within a tenancy or even between tenancies. Connectivity is achieved using Oracle’s internal backbone between regions.

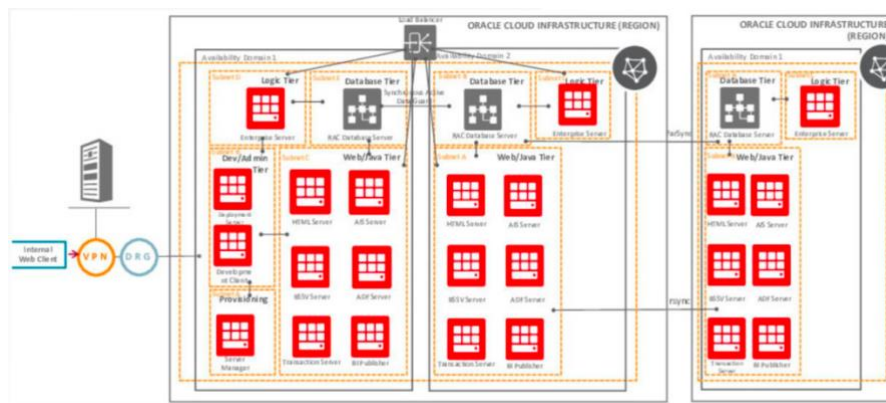


Image 5 Multiple Region Disaster Recovery Best Practices

Storage Synchronization Across ADs: Block volume backups between regions can be done using the console, CLI, SDKs, or REST APIs. Copying block volume backups to another region at regular intervals makes it easier for to rebuild applications and data in the destination region if a region-wide disaster occurs in the source region. You can also easily migrate and expand applications to another region. With Object Storage cross region copy, data asynchronously copies objects between buckets in the same region or to buckets in other regions.

Database DR Across Availability Domains: The use of either Data Guard or Active Data Guard is dependent on your use case and database edition. Active Data Guard requires Enterprise Edition – Extreme Performance.

Migration Best Practices

OBJECTIVES

- Application-aware migration
- Migration application configuration
- Migration of data
- Conversion from non-Oracle databases

- Conversion from non-Linux servers
- Upgrade from older versions of EnterpriseOne

SUPPORTING SERVICES

Application-aware migration tools help organizations move complex applications to OCI. They also enable users to reconfigure the applications after the migration is complete. OCI offers an application-aware migration tool for JD Edwards. During an application-aware migration, VMs and physical machines will never be captured or migrated. Only data and specific configuration files are captured and prepared for migration. The migration tool being used will deploy a new instance of the application in the Oracle environment or use an existing instance of the application in the target environment.

For more information, read the resources listed below:

- [Migrating JD Edwards EnterpriseOne Release 9.2 to Oracle Cloud Linux](#)
- [Migrating JD Edwards EnterpriseOne to Oracle Cloud for Oracle Database on Windows](#)
- [Migrating JD Edwards EnterpriseOne to Oracle Cloud for Microsoft SQL Server on Windows](#)
- [Upgrading JD Edwards EnterpriseOne to Release 9.2 on a One-Click Provisioned Target Environment on Linux](#)
- [Upgrading JD Edwards EnterpriseOne on Microsoft Windows Using Silent Mode to Import an Oracle Database](#)
- [Upgrading JD Edwards EnterpriseOne on Microsoft Windows Using Interactive Mode to Import an Oracle Database](#)

ONLINE TRANSPORT

It's important to consider bandwidth and security when transporting data, VMs, and files over the wire. Organizations can migrate datasets over the public internet, or set up private connectivity between on-premises data centers and OCI. Data should always be encrypted at rest and in transit.

VPN Over Internet

Relatively small datasets — up to approximately 2 terabytes (TBs) — can typically be transported over the public internet without problems. Use a VPN between the source environment and OCI to ensure secure connectivity. Internet Protocol Security (IPsec) VPN is the best option in this case.

The first step to setting up an IPsec VPN between the source environment and Oracle is establishing a dynamic routing gateway (DRG). The DRG should be set up to connect Oracle's cloud with any on-premises routers. Use multiple IPsec tunnels to ensure redundancy. See [Oracle's IPsec VPN documentation](#) for detailed instructions.

FastConnect

Oracle FastConnect is another option for securely connecting on-premises data centers and networks to OCI. It's the right choice for organizations that need to transport large datasets. Port speeds are available in 1 Gbps and 10

Gbps increments when working with a third-party connectivity provider, and 10 Gbps increments when co-locating with Oracle.

FastConnect enables organizations to quickly scale up, scale down, and terminate connections as needed. For example, an organization may choose to set up a 1 Gbps connection to transport a single application with a small dataset during the testing phase, then quickly scale up to a 10 Gbps connection when deploying multiple applications with large datasets. Finally, the organization can quickly terminate the connection once the transfer is complete.

Several Oracle partners offer solutions for setting up high-speed connections from on-premises data centers or other public clouds to OCI. Visit [Oracle's FastConnect page](#) for a listing of providers and solutions.

Storage Gateway

Once a secure connection has been established, organizations can use the OCI Storage Gateway to securely create copies of on-premises files and place them into Oracle Object Storage without the need to modify applications. Read [Oracle's Storage Gateway FAQ](#) for more detailed information.

OFFLINE TRANSPORT

For organizations with large, petabyte-scale datasets that are concerned about long upload times, Oracle recommends the OCI Data Transfer Service. This service uses commodity hard disks or the Oracle Data Transfer Appliance to quickly and securely transport data to Oracle without going over the wire.

Data Transfer Appliance

Each Data Transfer Appliance enables organizations to migrate up to 150 TBs of data. Appliances can be requested via the OCI management console after creating a transfer job. The appliance should be configured and connected to the on-premises network. Migration teams also need to mount NFS volumes off the appliance and copy the data onto the appliance. After the data is copied, ship the appliance back to Oracle and monitor the status of the data transfer. The [Data Transfer Service Launch Blog](#) provides details on how to use the service.

Data Transfer Disk

Oracle's Data Transfer Disk is another offline data transfer solution. Organizations send data as files on encrypted disks to an Oracle transfer site. Then site operators upload the files into the organization's designated object storage bucket. Users are free to move the uploaded data into other OCI services as needed. For details on the supported disk types, see [Oracle's Data Transfer Disk Documentation](#).

After all the VMs, data, and files have been securely transported to OCI, it's time to provision and deploy the target environment.

Security and Identity Best Practices

OBJECTIVES

- Ensure JD Edwards and associated data assets are isolated
- Protect internet-facing applications
- Data encryption

- Segregate operational responsibilities and restrict access to cloud services
- Use existing and third party security assets
- Audit and monitor actions
- Demonstrate compliance readiness

REFERENCE ARCHITECTURE

Virtual Cloud Network (1): Provides isolation for JD Edwards from any other workload on Oracle Cloud. Subdivide using subnets and apply security rules to isolate and control access to resources.

Internal Firewalls (2): A security list provides a virtual firewall for each tier, with ingress and egress rules that specify the types of traffic allowed in and out.

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

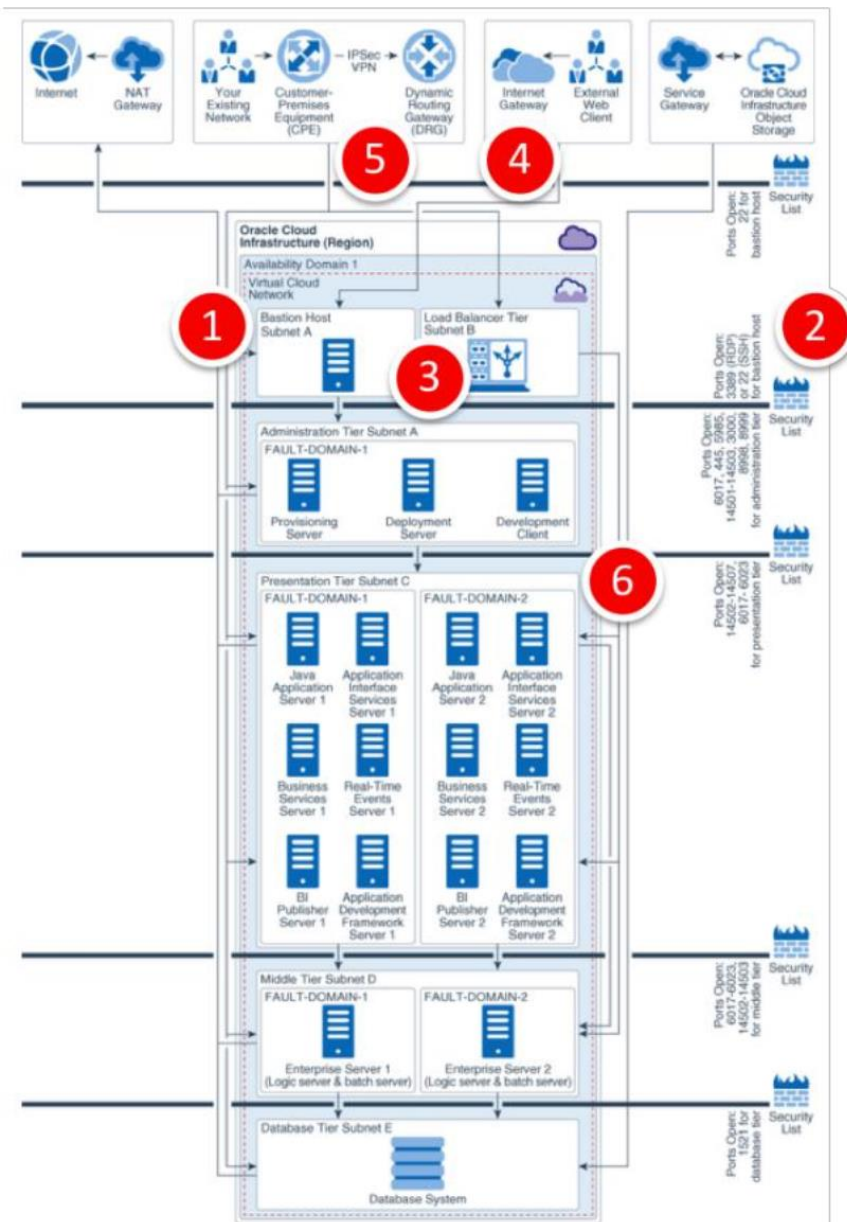


Image 6 Security and Identity reference architecture

Secure Connectivity to Internet (4): Internet bound traffic to / from a VCN must pass through an Internet Gateway. Virtual routing tables can be implemented with private IP addresses for use with NAT and 3rd party firewall devices.

Secure Connectivity to Your 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 to your premises or other cloud network.

Protect Web Applications (6): Oracle provides a Web Application Firewall (WAF) service that inspects any request from the web application server to end user.

Cost Management and Governance Best Practices

OBJECTIVES

When transitioning from a capital expenditure (CapEx) model, where many costs are fixed at the implementation of a project, to an operating expenditure (OpEx) model, where costs scale up and down with the usage of the system, customers often require cost management tools to understand and control these cloud costs within their organization. Oracle provides tools to meet these needs.

Outcomes these tools can enable:

- Set and manage cloud budgets
- Prevent overspending
- Ensure accurate cost tracking across departments and projects
- Analyze which departments, services and projects are contributing to cloud usage over time
- Get granular usage details for invoice reconciliation
- Identify areas to optimize costs

SUPPORTING SERVICES

Compartments: As discussed earlier in the Identity and Access Management section, compartments can be used to ensure isolation of cloud resources between business units. In addition, they are also used to logically group resources for the purposes of measuring usage and billing. We typically recommend creating a compartment for each major part of your organization, i.e., business unit or department. Compartments can also be nested to support sub-departments as well. Learn more about [Compartments](#).

Tagging: Leverage tags to track cost and usage of resources that are associated with a particular project that span multiple departments. In addition, you can streamline resource management by tagging and then scripting bulk actions on exactly the OCI resources you want. Tags leverage policies and controls to ensure tagging integrity and to prevent users from creating excessive tags, duplicate tags, and manipulating existing tags. Learn more about [Tagging](#).

Budgets: Once resources are assigned to compartments that match your specific use cases, departments, or regions of operation, you can set budgets, view how spend is tracking against those budgets, and configure alerts so that

unexpected usage is flagged before a budget is actually exceeded. Learn more about [Budgets](#).

Cost Analysis: The billing cost analysis dashboard can help visualize the big buckets that are contributing to cloud usage and cost. You can analyze costs by cloud service, compartments and tags. For example, an analyst or administrator can use this tool to identify the difference between increased production or dev / test usage, as well as the difference between increased usage of storage versus networking. Learn more about [Cost Analysis](#).

Detailed Usage Reports: CSV files containing detailed resource-level and hour-by-hour data, including all associated metadata, i.e., tags and compartments. Export detailed usage reports as CSV files and import into existing business intelligence tools for invoice reconciliation use cases, to get more granularity into your bill, and to identify areas for cost optimization. For example, you can leverage the detailed usage data and combine with CPU utilization data from the OCI Monitoring service to identify instances with low CPU utilization to shut down. Learn more about [Usage Reports](#).

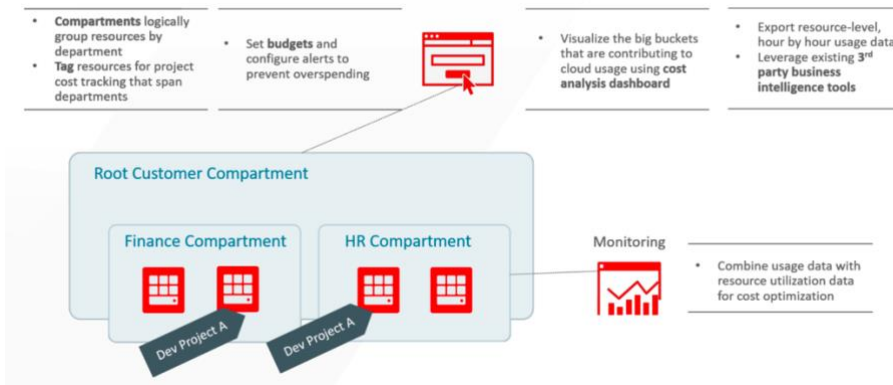


Image 7 Cost Management and Governance Supporting Services

Monitoring

OBJECTIVES

You need to be able to monitor the health and capacity of cloud infrastructure resources in order to optimize JD Edwards performance at all times and in real time. Objectives include ensuring availability and performance of JD Edwards on the cloud and detecting and fixing anomalies before they can impact your business. Additionally, you may require the visibility to identify bottlenecks and under- utilized resources in order to optimize accordingly.

SUPPORTING SERVICES

Infrastructure Monitoring: Chances are, you are already leveraging monitoring tools like Oracle Enterprise Manager and Oracle Management Cloud for your existing JD Edwards deployment. Oracle Cloud Infrastructure offers infrastructure monitoring natively within the console, but it can also support your existing monitoring tools. Depending on if you plan to migrate all JD Edwards applications and datasets into the Oracle Cloud or will maintain a hybrid cloud environment, Oracle recommends the following monitoring tools.

Multi-Tier Monitoring of Hybrid / Multi-Cloud Environments: For most multi-tier migration scenarios, we recommend leveraging Oracle Management Cloud. Oracle Management Cloud provides integrated monitoring across hybrid and multi- cloud environments. It performs monitoring through use of agents across various tiers from infrastructure to application performance, security, and even end-user activity. And it integrates with Oracle Enterprise Manager for Oracle Database performance and capacity analytics. Learn more about Oracle Management Cloud and Oracle Enterprise Manager.

Oracle Cloud Infrastructure Monitoring: Cost-effective and out-of-the-box metrics and dashboards are provided for IT to monitor cloud resources such as compute instances, block volumes, virtual NICs, load balancers, and object storage buckets natively within the OCI console. For example, you can leverage monitoring to track CPU utilization, memory utilization, and integrate with compute autoscaling. You can also integrate with open-source visualization tools, run your own metrics queries, and have your applications emit their own custom metrics, enabling you to visualize, monitor, and alarm on all critical time- series data from one place in the console. Learn more about Metrics and Alarms.

OCI performs agentless monitoring. Currently, this native infrastructure monitoring service does not monitor database services. For that, we recommend either Oracle Management Cloud or Oracle Enterprise Manager, depending on if Oracle Database is deployed on-premises or as a cloud service.

Additional Resources

- [JD Edwards EnterpriseOne Reference Architecture for Oracle Cloud Infrastructure](#)
- [Deploying JD Edwards EnterpriseOne on Oracle Cloud Infrastructure on Linux](#)
- [Deploying JD Edwards EnterpriseOne on Oracle Cloud Infrastructure on Microsoft Windows](#)

Connect with us

Call **+1.800.ORACLE1** or visit **oracle.com**. Outside North America, find your local office at: **oracle.com/contact**.

 blogs.oracle.com

 facebook.com/oracle

 twitter.com/oracle

Copyright © 2020, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

This device has not been authorized as required by the rules of the Federal Communications Commission. This device is not, and may not be, offered for sale or lease, or sold or leased, until authorization is obtained.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 0120

Disclaimer: This document is for informational purposes. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, timing, and pricing of any features or functionality described in this document may change and remains at the sole discretion of Oracle Corporation.