

ORACLE

# PeopleSoft 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 PeopleSoft to Oracle Cloud Infrastructure. It is intended solely to help you assess the business benefits of migrating PeopleSoft 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

---

<b>Solution Overview</b>	<b>4</b>
Audience and Business Problem Being Solved	4
Top-Level Value Proposition	4
TCO Analysis	4
Unique Infrastructure and Tools	5
Proven Customer Success	6
Validated Solutions that Address Your Business Requirements	6
<b>Key Workload Requirements</b>	<b>6</b>
<b>Architectures that Meet These Requirements</b>	<b>7</b>
Networking and Connectivity	7
Resiliency and High Availability	10
Disaster Recovery	12
Security	15
Identity and Access Management	18
Cost Management and Governance	20
Monitoring	21
Migration and Deployment	22
Additional Resources	25

## Solution Overview

### Audience and Business Problem Being Solved

When your organization depends on PeopleSoft to manage human resources, finances, supply chain, inventory, or higher education campus experiences and you want to get to the cloud but are not ready to move to SaaS because of deep customization, integration or control requirements, Oracle has a validated cloud solution for you.

You can migrate your current PeopleSoft deployment to Oracle Cloud Infrastructure and gain access to better elasticity to support peak seasons, agility to add new capabilities, streamlined infrastructure management, and lower total cost of ownership (TCO). With Oracle Cloud Infrastructure, you have granular control over your PeopleSoft environment all while taking advantage of the same software, the same licenses, and the same training your staff and end-users currently have. In addition, only Oracle offers consistent high performance at guaranteed service levels.

### Top-Level Value Proposition

Oracle provides a simple way to migrate most on-premises PeopleSoft deployments to Oracle Cloud Infrastructure that doesn't require significant re-architecture, re-integration or business process changes. Once on Oracle Cloud Infrastructure, PeopleSoft will be more flexible, more reliable, and deliver higher performance at a lower cost than deployments running on-premises or with other cloud providers.

Oracle has a validated solution to accomplish these goals, quickly and reliably. It includes procedures, supporting services, and reference architectures. These consider real production needs, including security, network configuration, high availability, disaster recovery, identity integration, and cost management. With this validated solution, you can take advantage of:

- 38-52% lower TCO
- 2-10x faster reporting speed
- No single point of failure
- Quick and seamless migration without re-architecture
- Rapid in-place technology refresh and patching
- Proactive costs and usage monitoring
- Near instant scaling up or down
- Ability to retain control over security and governance using familiar tools

### TCO Analysis

Operating PeopleSoft in Oracle Cloud Infrastructure can be 38% less than running it on-premises. Significant savings come from eliminating upfront hardware, ongoing facilities, IT administration and support costs. We also estimate that PeopleSoft costs 52% less on Oracle than on Amazon Web Services (AWS).

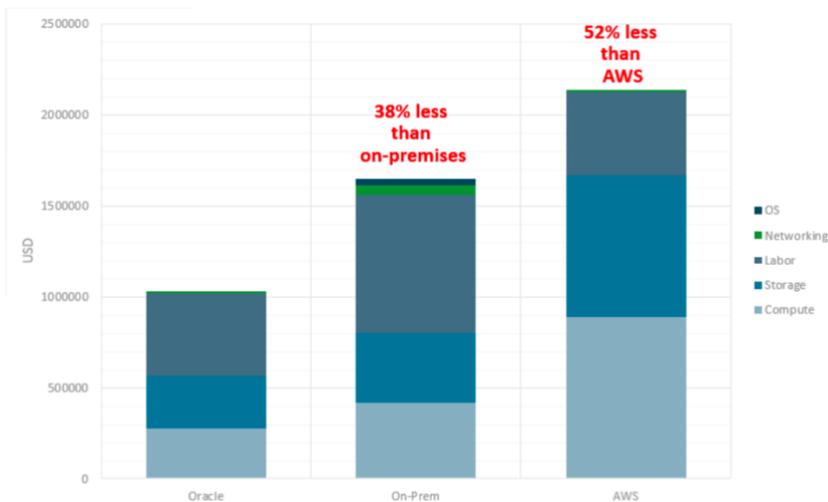


Figure 1 Operating PeopleSoft in Oracle Cloud Infrastructure can be 38% less than running it on-premises

## FIVE YEAR TCO FOR PEOPLESOFT ON ORACLE CLOUD INFRASTRUCTURE

### Assumptions

- Assume bring your own licensing for PeopleSoft and Oracle Database
- 5,000 concurrent users
- 6 environments (2 production, dev, testing, staging, QA)
- Oracle: 80 vCPUs per environment, 6TB database storage, 50GB / vCPU storage, 1Gbps FastConnect, Backups, 1TB outbound, 25% cloud discount
- On-Premises: 15 servers with 28 cores, 128 GB RAM per environment, 15 TB storage
- AWS: Same as Oracle, reserved instances for production environments, 7% EA discount

### Unique Infrastructure and Tools

Oracle Cloud Infrastructure offers unique infrastructure capabilities, tools and support that are optimized for PeopleSoft.

At the highest level, Oracle tests PeopleSoft on Oracle Cloud Infrastructure and not on any other cloud. PeopleSoft Cloud Manager is available only for workloads running in the Oracle Cloud to help streamline migration and ongoing lifecycle management. And there are single vendor support advantages to running your Oracle application and database on Oracle's cloud infrastructure. Oracle professional services and our ecosystem of partners can assist to make your move as seamless as possible.

There are also significant performance benefits when you run PeopleSoft on Oracle's cloud. Our unique non-oversubscribed networks and single-tenant offerings like bare metal compute and Exadata ensure consistent performance. Unlike other clouds, we also offer service level agreements to back up performance guarantees. In addition, [many services run cheaper](#), as we outlined in the [TCO Analysis](#) section, and you can also bring existing database licenses to Oracle's cloud.

Finally, we designed our core cloud services with enterprise applications in mind to deliver the same level of control you are accustomed to having with your on-premises environment. PeopleSoft customers can leverage Oracle's flexible compartment structure, Virtual Cloud Networks (VCNs) and bare metal compute so you don't have sacrifice control nor change your business processes.

### **Proven Customer Success**

The [University of Santiago](#), one of the oldest universities in Chile, saved 35% by implementing PeopleSoft in Oracle Cloud. This was their first major foray into cloud, and they worked with their systems integrator Astute Business Solutions to complete the migration in under 6 months. By modernizing in the cloud, they were also able to implement PeopleTools Fluid UI responsive design capabilities, which improved desktop and mobile enrollment and schedule management experiences for over 23,000 students.

[Alliance Data Systems](#), an \$8 billion dollar loyalty and marketing services company was able to migrate PeopleSoft, Hyperion, OBIEE, 30 database and 25 Terabytes of critical financial and HR data from Exadata on premises to Oracle Cloud Infrastructure and Exadata Cloud Service, with expectations to save \$1 million in just the first year of deployment. Not only is Alliance Data Systems saving on TCO, but they are also experiencing 30-50% improved performance for their applications. They doubled their disk space, increased memory by 5 times and computing power by 3 times. And as a data intensive company, they can continue to leverage the superior performance of Exadata in the Oracle Cloud, not available on any other cloud.

[Covanta](#), a \$2 billion global waste management and energy company, was able to migrate PeopleSoft to Oracle Cloud Infrastructure while maintaining control and enhancing security. They leverage VCNs to keep complete control over their networks, configuring network firewalls, subnets and route tables. Covanta also required a higher level of security at the edge of its network to prevent malicious hackers from targeting their web applications. Therefore, they also use Oracle Web Application Firewall (WAF) to secure PeopleSoft's internet-facing finance, supply chain and procurement portals that their staff access daily.

### **Validated Solutions that Address Your Business Requirements**

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

### **Key Workload Requirements**

Any version of PeopleSoft on any data platform can run on Oracle Cloud Infrastructure. Customers on PeopleSoft application release 9.2, PeopleTools release 8.55 and Oracle Database 12c can take advantage of the automated lift and shift deployment and one-touch provisioning capabilities in PeopleSoft Cloud Manager.

If you are on a prior version of PeopleSoft, Oracle Cloud Infrastructure can still support manual deployment on supported operating systems. As you begin planning to deploy or migrate, we recommend discussing with your Oracle

account team and / or partner the combination of PeopleSoft application release, PeopleTools release, Oracle Database version, and the operating system on which you want to run your applications.

Next, we'll share validated architectures to help you address these requirements.

- Matching your high-performance and highly isolated network model
- Designing for high availability and disaster recovery
- Deploying a secure architecture
- Integrating with your identity management system
- Maintaining visibility over costs and usage
- Monitoring infrastructure health and performance
- Migrating your application and database environments into 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, and in other cases they are to support a particular hardware capability or limitation. And in still others, they reflect preferences of the architect.

In every case, we recommend leveraging the baseline reference architecture and adjusting as needed so that your specific requirements are met. Starting from scratch can be time-consuming and comes with the risk that some important consideration has been overlooked. The reference architectures can help reduce the time and effort required to successfully deploy your PeopleSoft environment in the cloud.

### **Networking and Connectivity**

#### OBJECTIVES

The primary objectives for the networking and connectivity architecture is to provide secure, high-speed connectivity between your cloud resources and any users and / or systems that would need to access those resources. Additionally, it illustrates mechanisms by which you can design a network topology that best meets your needs, with the ability to isolate resources between bastion host, application tiers, database tiers and load balancing for security and management purposes.

Outcomes this architecture can provide:

- Isolation from other customers and your other workloads
- Network-level isolation between web / application tiers and database tiers
- Monitoring and management access to all application and database tiers
- Private / dedicated access from corporate campus(es) to the application
- Ensuring low latency between cloud environment and your data center
- Secure network access to the application via encrypted links over the public internet

- Private network connectivity to other systems or services hosted on Oracle Cloud Infrastructure
- Load balancing across multiple application nodes for performance and availability

## REFERENCE ARCHITECTURE

**Virtual Cloud Network (1):** A Virtual Cloud Network (VCN) is basically your own private network within Oracle Cloud Infrastructure. It provides isolation for your PeopleSoft workload from any other workload on Oracle Cloud Infrastructure, 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](#).

**Bastion Host (2):** The bastion host is an optional component that can be used as a jump server to access and manage Oracle Cloud Infrastructure instances in the private subnet. You can also access instances in a private subnet by using dynamic SSH tunneling. Read more about [securing networking](#).

**Internet Gateway (IGW):** You can connect to instances that are placed in public subnets using the IGW. To access your instances from the internet, you also need to create your bastion host in a public subnet and access the bastion host from the IGW. Learn more about [enabling access to the internet](#).

There are 3 scenarios for placing PeopleSoft instances across public and / or private subnets:

1. Deploy all instances in a private subnet – Recommended for all production environments with no internet-facing endpoints. This type of deployment is useful when you want to have a hybrid deployment with the cloud as an extension to your existing data centers.
2. Deploy instances in public and private subnets - You can deploy a few instances in a public subnet and a few instances in a private subnet. This type of deployment is useful when the deployment includes internet-facing and non-internet facing endpoints. In this configuration, some application instances are placed in a public subnet, and others are placed in a private subnet. For example, you may have application instances

servicing internal users and another set of application instances servicing external users.

3. Deploy all instances in a public subnet – Best for quick demos or for production-grade deployments with no internal endpoints. This deployment is suitable only if you don't have your own data center or you can't access instances over VPN, and you want to access the infrastructure over the internet. Although instances with public IP addresses can be accessed over the internet, you can restrict access by using security lists and security rules.

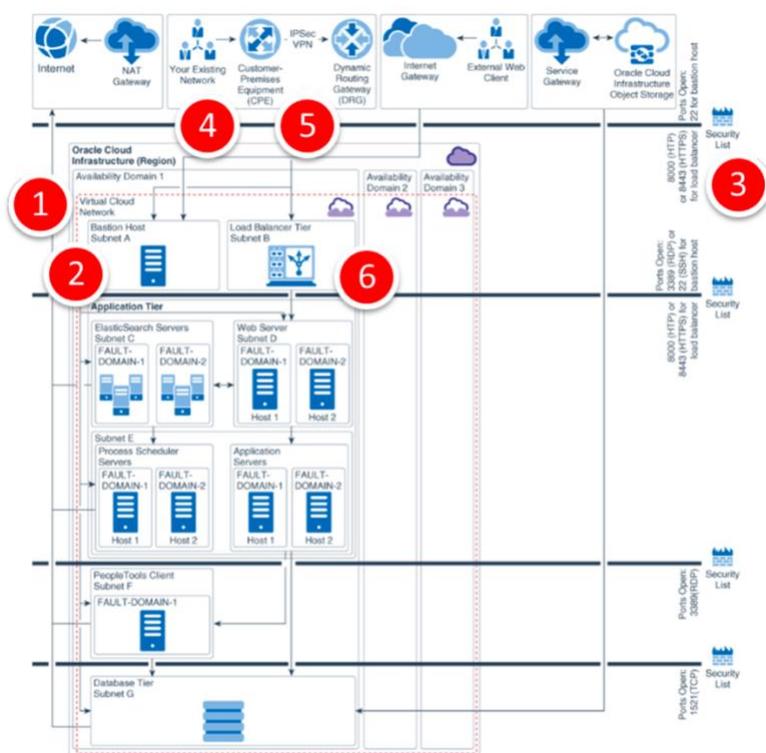


Figure 2 Networking and connectivity reference architecture

**Internal Firewalls (3):** 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](#).

**FastConnect (4):** If you require fast and predictable data transfer speeds, we offer FastConnect which guarantees a certain level of accessible bandwidth. Multiple partners across the world offer dedicated network connections between customer premises and Oracle data centers. This allows you to access your PeopleSoft implementation as if it is running in your own data center. Read more about [FastConnect](#).

**IPsec VPN Connect (5):** 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 PeopleSoft resources in Oracle Cloud Infrastructure. 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](#).

**Load Balancing (6):** Pre-configured, redundant load balancers are available on private and public subnets to balance traffic within the implementation and from external connections, respectively.

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. 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 IGW.
- For accessing both internal and internet-facing endpoints, you can set up private load balancers to serve 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. You can read more on [Load Balancing](#).

## Resiliency and High Availability

### OBJECTIVES

The primary objective for this architecture is to build resiliency, redundancy and high availability (HA) into the cloud infrastructure that is supporting PeopleSoft and its backend datasets.

Outcomes this architecture can provide:

- Ensure system resiliency and anti-affinity, meaning that PeopleSoft is available even if an application instance goes down
- Server redundancy via multiple active-active nodes at each application tier
- Redundancy strategy for database tier
- Backup strategy for non-database tiers
- Backup requirements for database tier

### REFERENCE ARCHITECTURE FOR DEPLOYING PEOPLESOFT IN A SINGLE AVAILABILITY DOMAIN

At a basic level, you can achieve resiliency and redundancy for your PeopleSoft deployment even within a single availability domain (AD). Learn more about [ADs and regions](#).

**Bastion Host (1):** The bastion host is an optional component that you can use as a jump server to access the instances in the private subnet.

**Load Balancer Tier (2):** We recommend having load balancers in their own tier or subnet to load balance traffic to PeopleSoft web servers. The load

balancer receives requests from users, and then routes these requests to the application tier.

**System Resilience (3):** A fault domain is a grouping of hardware and infrastructure that is distinct from other fault domains in the same AD, and each AD has three fault domains. Fault domains let you distribute your application instances so that they are not on the same physical hardware within a single AD. As a result, a hardware failure or hardware maintenance event that affects one fault domain does not affect instances in other fault domains. By using fault domains, you can protect your instances against unexpected hardware failures and planned outages.

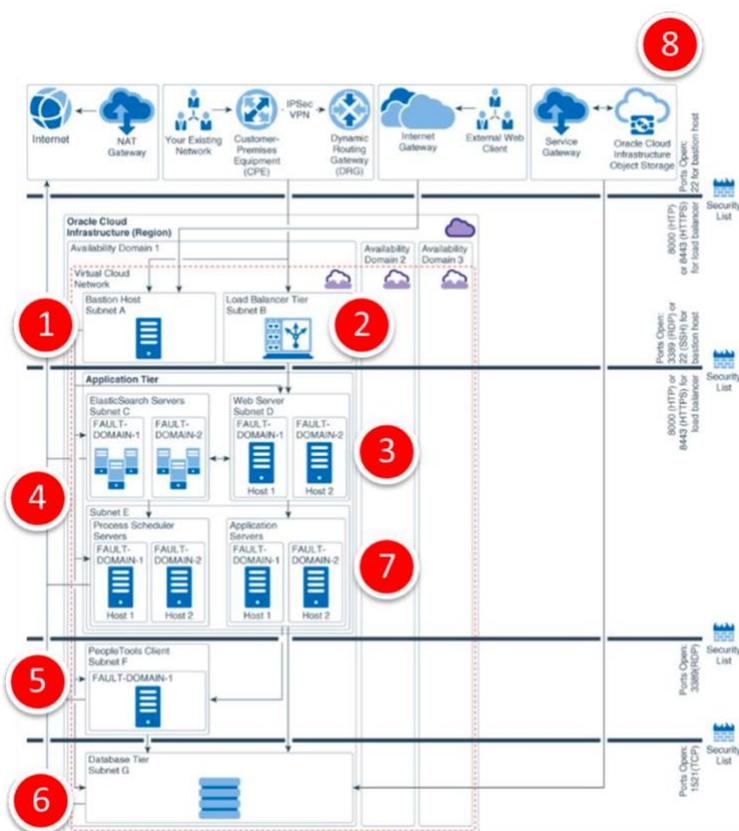


Figure 3 Reference Architecture for deploying Peoplesoft in a single availability domain

**Active-Active Server Redundancy in the Application Tier (4):** This tier contains redundant instances of the PeopleSoft application servers, PeopleSoft web servers, ElasticSearch servers, and PeopleSoft Process Scheduler to provide high availability. Redundancy is enabled for all servers in the application tier through the usage of fault domains. This helps ensure that you can continue accessing the application even if an instance goes down. All instances are active and receive traffic from the load balancer and middle tier.

**PeopleTools Client (5):** Use the PeopleTools client to perform administration activities, such as development, migration, and upgrade.

**Redundancy in the Database Tier (6):** This tier contains database system instances. For performance and HA requirements, Oracle recommends that you use two-node Oracle Real Application Clusters (RAC) [database systems](#) or [Oracle Database Exadata Cloud Service](#) in Oracle Cloud Infrastructure.

**Backup Strategy – Application Tier (7):** Backup of the application tiers can be configured by using the policy-based backup feature of Oracle Cloud

Infrastructure [Block Volumes](#). Block Volumes provide 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 (8):** Use [Oracle Cloud Infrastructure Object Storage](#) to perform a backup using Oracle Recovery Manager (RMAN). To back up or patch the database to Object Storage, the database system's VCN must be configured with either a [service gateway](#) or an IGW. It is recommended that you use a service gateway rather than an IGW for backup and patching because service gateway does not traverse the internet.

Learn more about this [reference architecture for deploying PeopleSoft in a single AD](#).

## Disaster Recovery

### OBJECTIVES

The primary objectives for the following architectures are to ensure you can build disaster recovery (DR) into your deployment in case of unforeseen events which would require you to failover and still keep PeopleSoft up and running.

- Outcomes these architectures can provide:
- DR within a single region
  - 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
- DR across multiple regions
  - Application replication between regions
  - Storage replication between regions
  - Cross-region copy lets you asynchronously copy object storage datasets
  - Cross-region backup copy for block volumes
  - Database protection between regions

### REFERENCE ARCHITECTURE FOR DEPLOYING PEOPLESOFT IN SINGLE REGION

To ensure that PeopleSoft is available if one AD goes down, we recommend that you deploy across multiple ADs.

**Active-Active Components Across ADs (1):** Clustering of supported services across ADs provides protection from an AD failure. In this architecture bastion hosts, load balancers, and application tier servers in both ADs are in active state.

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

**Regional Subnets Across ADs (2):** Regional subnets span the entire region providing benefits like protection from AD network failure, simplified PeopleSoft service deployment and management.

**Load Balancing Across ADs (3):** Public load balancing distributes traffic across the PeopleSoft servers across all configured ADs, providing protection from an AD failure.

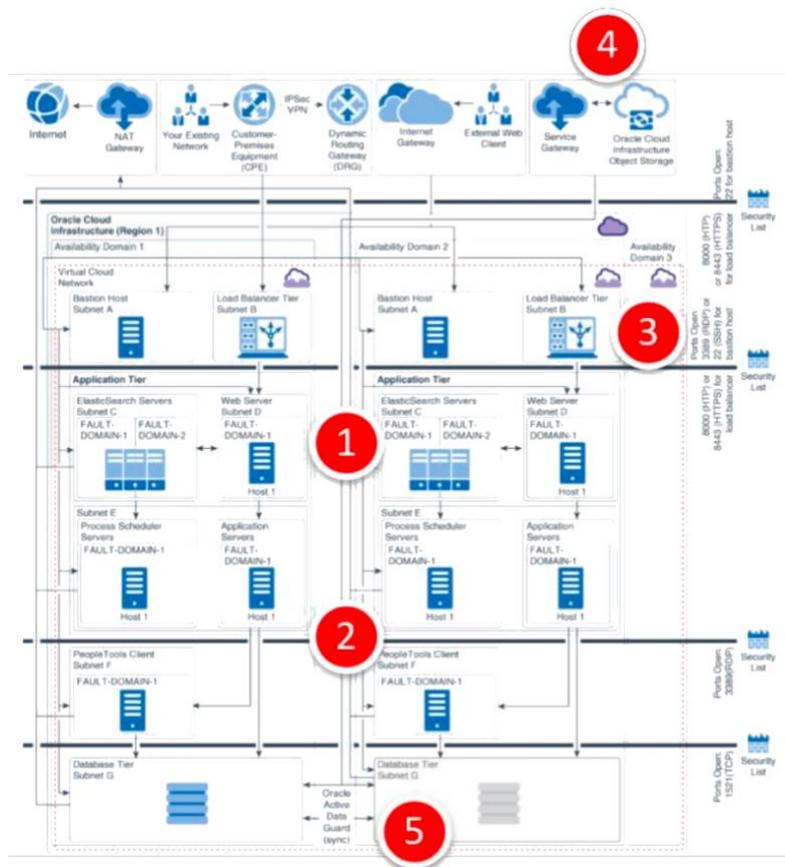


Figure 4 Reference architecture for deploying PeopleSoft across multiple ADs in a single region

**Storage Synchronization Across AD (4):** Block Volume backups (boot and block) are replicated across all 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):** We recommend setting up database instances in both ADs. AD 1 hosts the primary database instances while AD 2 hosts the standby database instances. In each AD, at least two database instances are set up to ensure high availability. If a database instance is not available in AD 1, then the second database instance in AD 1 continues processing requests. Data Guard or Active Data Guard may be selected depending on your use case and database edition for replication across ADs. Active Data Guard requires Enterprise Edition – Extreme Performance.

Learn more about this [reference architecture for deploying PeopleSoft across multiple ADs in a single region](#).

## REFERENCE ARCHITECTURE FOR DISASTER RECOVERY ACROSS MULTIPLE REGIONS

For true DR capabilities, we recommend setting up a DR site for PeopleSoft in a different geographical region.

**Active-Active Components Across ADs (1):** Clustering of supported services across ADs provides protection from an AD failure. Again, bastion hosts, load balancers, and application tier servers in both ADs are in active state.

**Active-Passive Components Across Regions (2):** If you are using Active-Passive architecture, use rsync to synchronize application servers across ADs.

**Regional Subnets Across ADs (3):** Regional subnets span the entire region providing benefits like protection from AD network failure, simplified PeopleSoft service deployment and management.

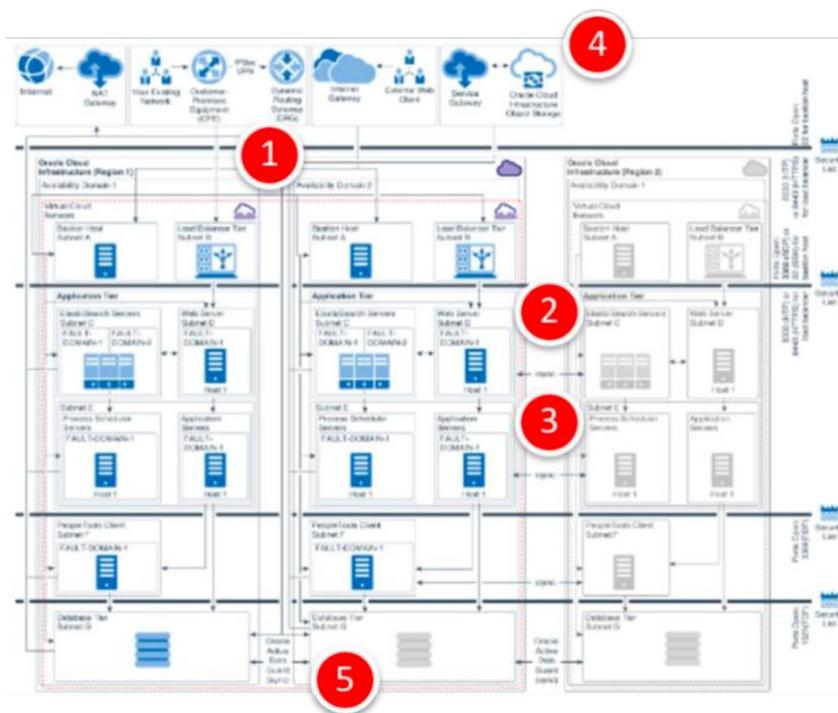


Figure 5 Reference architecture for deploying PeopleSoft across multiple regions

### Infrastructure

**Load Balancing Across ADs (4):** Load Balancing distributes traffic across the PeopleSoft servers across all configured ADs, providing protection from AD failure.

**Storage Synchronization Across ADs (5):** 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 (6):** 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.

Learn more about this [reference architecture for deploying PeopleSoft across multiple regions](#).

## Security

### OBJECTIVES

The objective of the security architecture is to enable you to maintain your security posture when running your business-critical PeopleSoft application and associated applications in the Oracle Cloud. Even though you may be reducing the overhead of building and maintaining data center infrastructure, you still need unparalleled control and transparency over what you're running in the cloud.

Outcomes this architecture can provide:

- Ensure PeopleSoft and associated data assets are completely isolated from other tenants' workloads and Oracle's staff so to limit the effect of noisy neighbors and prevent lateral movement of attacks
- Protect your internet-facing PeopleSoft applications from cyberattacks
- Encrypt your data in a way that allows you to meet your security and compliance requirements
- Segregate operational responsibilities and restrict access to cloud services in order to reduce risk associated with malicious and accidental user actions
- Be able to leverage existing security assets such as identity providers and other third-party security solutions to secure access to your PeopleSoft application and data
- Audit and monitor actions taken on your cloud resources so that you can meet audit requirements
- Demonstrate compliance readiness to internal security and compliance teams, end-customers, auditors and regulators

### REFERENCE ARCHITECTURE

As a cloud provider, it is our job to provide and operate our secure infrastructure. We've designed security into every aspect of our infrastructure to help our customers achieve better protection, isolation and control. We started with 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 hardware-based root of trust, making sure each server is pristine each and every time it is provisioned.

However, security is a shared responsibility between Oracle and our customers. Therefore, we provide security tools and also support your existing tools, so you can maintain granular control over identity and access management (IAM), networking, compute, and data management for your PeopleSoft deployment in the cloud without having to rebuild your security posture.

**Secure Network Isolation:** We discussed VCNs, subnets and security lists earlier in the section on Network and Connectivity. For each customer's VCN there is a range of defense in depth protections available spanning layers 3-7.

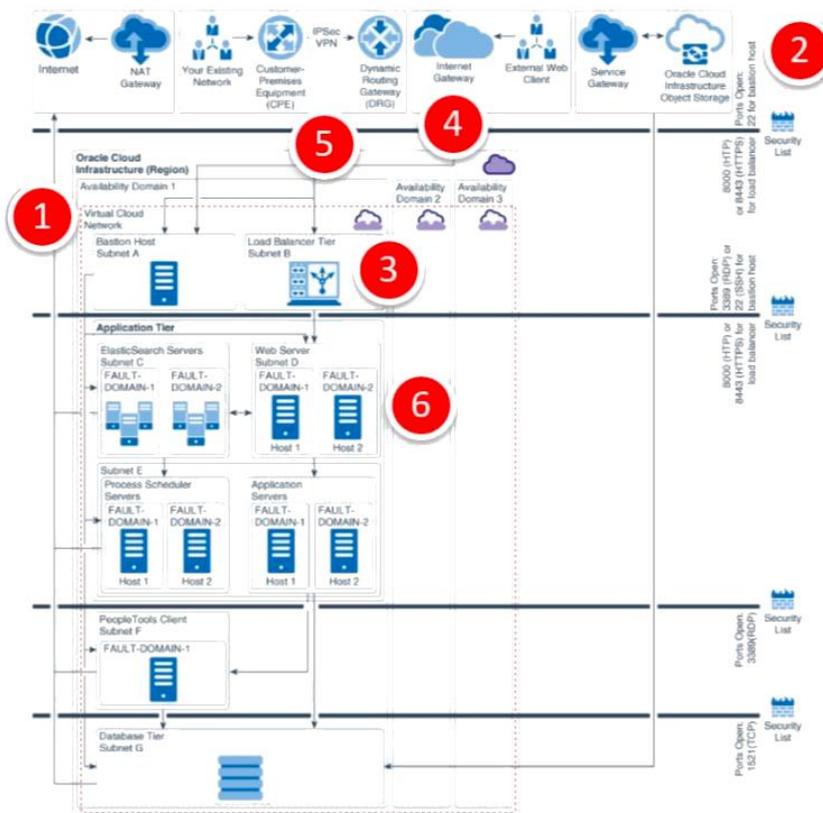


Figure 6 Defense in depth protections

**VCN (1):** A VCN provides isolation for your PeopleSoft 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 travel between regions are either sent over private links or are 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 provides a Web Application Firewall (WAF) service with 250 pre-defined OWASP and compliance rules. Oracle Cloud Infrastructure WAF acts as a reverse proxy that inspects all traffic flows or requests before they arrive at the origin web application. 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.

**Server Isolation:** If you require complete workload and data isolation at the server level for security and / or performance requirements, you can leverage bare metal compute shapes. These shapes are single tenant, so they offer consistently high performance and are immune to noisy-neighbor issues. There is also no Oracle managed hypervisor and Oracle staff have no access to memory nor local NVMe storage while the instance is running.

If you have more flexible requirements for PeopleSoft, our multi-tenant VM shapes leverage a security-hardened hypervisor that provides strong isolation between customers. And regardless of shape type, bare metal or VM, all servers are wiped clean and installed with gold state firmware when newly provisioned.

**Data Encryption:** By default, all data that customers store with any of Oracle Cloud Infrastructure's storage or data management services, including Block Volumes, boot volumes, Object Storage, File Storage, and Database, is encrypted at rest using strong AES keys or TDE in the case of database encryption.

**Key Management:** For customers that require the ability to control their own cryptographic keys for security or compliance purposes, we offer Oracle Cloud Infrastructure Key Management. With [Key Management](#), you can centralize key lifecycle management in FIPS 140-2 Level 3 hardware security modules (HSMs).

**Identity and Access Management:** Identity management including authentication, authorization, tools to help you organize and control access to resources according to organizational hierarchy, and the ability to leverage existing identity providers is such a rich topic that we devoted a separate section to IAM below.

**Audit and Logging:** Oracle automatically records calls to all supported Oracle Cloud Infrastructure public application programming interface (API) endpoints as log events. Currently, all services support logging by our Audit service. You can leverage this data to perform diagnostics, track resource usage, monitor compliance, and collect security-related events. Learn more about [Oracle Cloud Infrastructure Audit](#).

**Compliance:** Depending on where you do business and industry-specific practices, you may need to demonstrate compliance readiness to internal teams and to external auditors. Oracle continually engages with external assessment entities and independent auditors to meet a broad set of

international and industry-specific compliance standards for service deployments on our cloud. Learn more about [compliance](#).

Learn more about [security best practices](#) when running applications like PeopleSoft in Oracle Cloud Infrastructure.

## Identity and Access Management

### OBJECTIVES

With the IAM architecture, you can group and isolate resources according to your organizational structure and hierarchy, control who has access to cloud resources, what type of access a group of users has, and to which specific resources.

Outcomes this architecture can provide:

- Securely isolate cloud resources based on organizational structure
- Authenticate users to access cloud services via browser interface, REST API, SDK or CLI
- Authorize groups of users to perform actions on appropriate cloud resources
- Enable managed service provider (MSP) or systems integrator (SI) to manage infrastructure assets while still allowing your operators the ability to access resources
- Authorize application instances to make API calls against cloud services
- Federate identities using your existing identity provider (IDP)

### SUPPORTING SERVICES

Oracle Cloud Infrastructure offers a single model for authentication and authorization, and we also integrate with your existing identity provider. We have architected IAM to be secure by default, leveraging the security principle of least privilege. This means that new users cannot access nor take any action on cloud resources unless an administrator grants them appropriate permissions to do so. To begin, we recommend organizing and isolating your cloud resources appropriately so that you can apply policies to grant the right groups of users access to the right resources.

**Compartments:** Compartments are a fundamental component of Oracle Cloud Infrastructure for organizing and isolating your cloud resources. A common approach is to create a compartment for each major part of your organization. For example, you can place all database resources in a database compartment and only grant database administrators access. You can also use them to ensure isolation between business units and to logically group resources for the purposes of measuring usage and billing. Learn more about [compartments](#).

**Authentication and Credential Management:** By default, Oracle Cloud Infrastructure enforces a strong password policy for access to the console user interface and to the Swift client for database backups to Object Storage. Administrators can also modify password policies for all local or non-federated users using Oracle IAM service. Each user can automatically reset their own console passwords and manage their own API keys. However, you

must have administrator permissions to manage credentials for users other than yourself. Learn more about [managing user credentials](#).

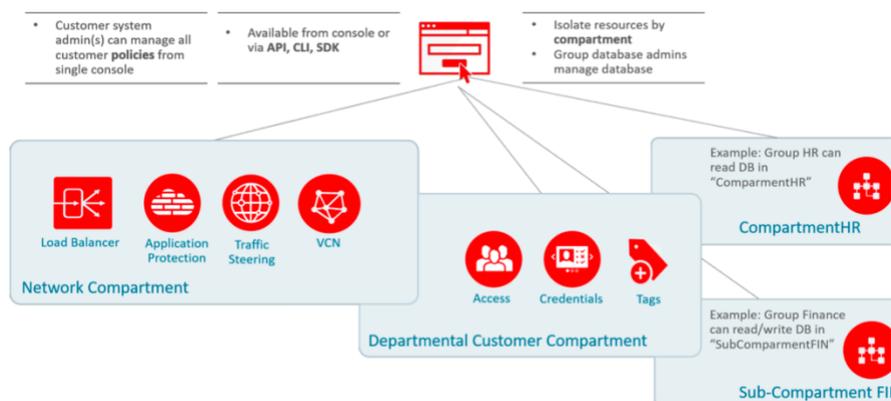


Figure 7 Compartments are a fundamental component of Oracle Cloud Infrastructure for organizing and isolating your cloud resources

**Policies:** Leverage policies to authorize a group of users to take action on cloud resources in a specified compartment or across the tenancy. Oracle Cloud Infrastructure policies are written in human-readable language, so they are simple to define and easy to understand.

**IAM for MSP / SIs:** A common use case is to have an MSP or SI manage your cloud infrastructure assets while still retaining the entitlement to operate your cloud resources. Compartments and policies can be used in conjunction to ensure clear separation of duties.

**Instance Principals:** Allow users to call IAM-protected APIs from an Oracle Cloud Infrastructure compute instance without the need to create users or manage credentials for that instance. You may have a PeopleSoft application or an integrated application running on a compute instance that requires access to object storage. By grouping the appropriate compute instances as “principal” actors, you can simply attach policies to enable them to make API calls against other cloud services such as object storage.

**Federation:** Oracle IAM supports federation with Oracle Identity Cloud Service (IDCS) and any other SAML 2.0 compliant identity provider. Learn more about [federation](#).

When you sign up for Oracle Cloud Infrastructure, your tenant administrator account is automatically federated with Oracle Identity Cloud Service. Federating with Oracle Identity Cloud Service automatically allows you to have a seamless connection between services without having to create a separate username and password for each one.

As a PeopleSoft customer, you may be leveraging the application’s own security mechanisms to provide authentication with integrated applications on-premises that leverage Lightweight Directory Access Protocol (LDAP), Oracle Access Manager (OAM) or other 3rd party solutions. Therefore, we recommend federating your favorite IDP with IDCS which will automatically provide federation for all Oracle cloud offerings. You can read [whitepapers about configuring federation with OAM and other IDPs](#).

Learn more [Best Practices for IAM in Oracle Cloud Infrastructure](#).

## Cost Management and Governance

### 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 Oracle Cloud Infrastructure 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 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 Oracle Cloud Infrastructure Monitoring service to identify instances with low CPU utilization to shut down. Learn more about [Usage Reports](#).

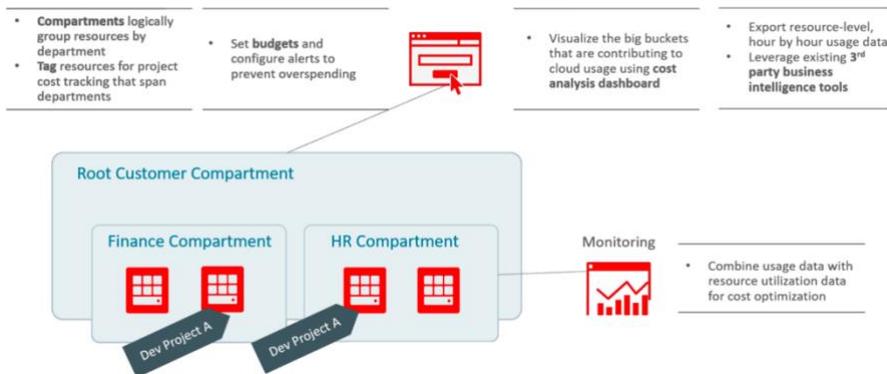


Figure 8 Usage Reports

## Monitoring

### OBJECTIVES

You need to be able to monitor the health and capacity of cloud infrastructure resources in order to optimize PeopleSoft performance at all times and in real time. Objectives include ensuring availability and performance of PeopleSoft 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 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 PeopleSoft 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 PeopleSoft 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 Oracle Cloud Infrastructure 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](#).

Oracle Cloud Infrastructure 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.

## **Migration and Deployment**

### OBJECTIVES

We understand that when it comes to migrating a complex, highly customized and deeply integrated application like PeopleSoft, it's important to do it with as little re-architecture as possible so that there's limited downtime and the transition is completely seamless for end-users.

Outcomes this architecture can provide:

- Application-aware tooling so that you can keep existing customizations and integrations
- Post-migration application configuration
- Data migration

### REFERENCE ARCHITECTURE

Application Migration: PeopleSoft Cloud Manager is an application-aware migration and administration tool that can help you migrate, deploy and manage your PeopleSoft environment on Oracle Cloud Infrastructure along with the different services that are needed by the application to run seamlessly. It can also help you configure the application after the migration is complete.

PeopleSoft Cloud Manager helps with key application lifecycle activities as outlined below.

- Lift and shift an on-premises environment to Oracle Cloud
- Provision PeopleSoft environments on Oracle Cloud Infrastructure Compute and Oracle Database Cloud Services
- Create reusable deployment templates
- Self-service provisioning of PeopleSoft environments, if desired
- Manage multiple environments from a single page
- Perform on-demand health checks on environments
- Enable application lifecycle management in Oracle Cloud
- Automatically download PeopleSoft Update Manager (PUM) images, PeopleSoft Release Patchsets (PRPs) and PeopleTools patches
- Clone environments by creating templates from running instances

Therefore, we recommend that PeopleSoft customers that are interested in migrating to the cloud leverage this tool. PeopleSoft Cloud Manager can be

easily launched to VM instances from directly within the Oracle Cloud Infrastructure console. It is supported on PeopleSoft application version 9.2 and PeopleTools version 8.55. And if you are leveraging Oracle Database in the backend, PeopleSoft Cloud Manager supports Oracle Database version 12c. PeopleSoft Cloud Manager deploys PeopleSoft environments on Linux VMs and uses a Microsoft Windows VM to install PeopleTools components. Oracle provides both custom Linux and Windows images for PeopleSoft Cloud Manager, and detailed installation guides can be found [here](#).

Once installed, PeopleSoft Cloud Manager enables the automated migration of on-premises PeopleSoft environments to Oracle Cloud in two steps:

- **Lift:** Using the lift utility provided in PeopleSoft Cloud Manager, PeopleSoft application environment data and the supporting Oracle Database is packed into DPK format and uploaded to Oracle Object Storage. The lift utility “lifts” the application tier (middle tier) and database tier independently and packages them into separate DPKs. PeopleSoft Cloud Manager supports two types of database lift – hot backup and cold backup. Hot backup is performed with RMAN using Oracle Database Cloud Backup Module (ODCBM). Cold backup is performed by taking a cold backup of the pluggable database.
- **Shift:** PeopleSoft Cloud Manager downloads the lifted DPKs and creates a new environment on Oracle Cloud. Once shifted, customers can use Oracle Cloud Infrastructure to further manage, scale up or scale down or clone these environments.

**Application Configuration and Deployment:** In addition to lift and shift, you can also use PeopleSoft Cloud Manager to define a multi-node topology including the number, type and size of VMs (CPU, memory, storage) needed for Linux and Windows together. Once your topology is defined, you can combine with your PeopleSoft DPK to create an environment template that can be deployed at a click.

For detailed steps on operating PeopleSoft Cloud Manager after installation, see the [PeopleSoft Cloud Manager online documentation](#). If you are on a prior version of PeopleSoft or if you want to customize your deployment per specific needs, Oracle still supports manual lift and shift.

You can also leverage [Terraform scripts](#) to automate orchestration for your PeopleSoft deployments on Oracle Cloud Infrastructure.

**Data Migration:** 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. PeopleSoft Cloud Manager will deploy a new instance of the application in the Oracle Cloud environment or use an existing instance of the application in the target environment.

**Online Transport:** It's important to consider bandwidth and security when transporting datasets over the wire. Organizations can migrate datasets over the public internet or set up private connectivity between on-premises data centers and Oracle Cloud Infrastructure. Data should always be encrypted at rest and in transit.

**FastConnect:** Oracle FastConnect is another option for securely connecting on-premises data centers and networks to Oracle Cloud

Infrastructure. It's the optimal 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.

**IPSec VPN Connect:** Relatively small datasets—up to approximately 2 terabytes (TBs)—can typically be transported over the public internet without problems. We recommend using IPSec VPN Connect, which provides encrypted and secure connectivity between your source environment and Oracle Cloud Infrastructure to securely write data into Object Storage and then restore from there. The first step to setting up an IPSec VPN Connect between the source environment and Oracle is establishing a 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.

**Storage Gateway:** Once a secure connection has been established, organizations can use Oracle Cloud Infrastructure 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 who are concerned about long upload times, Oracle recommends the Oracle Cloud Infrastructure 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 Oracle Cloud Infrastructure 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. You can send data as files on encrypted disks to an Oracle transfer site. Then site operators upload the files into your designated object storage bucket. Users are free to move the uploaded data into other Oracle Cloud Infrastructure 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 Oracle Cloud Infrastructure, it's time to provision and deploy the target environment.

**Migration Expertise from Oracle and Partners:** Oracle Managed Cloud Services (OMCS) and established SI partners also provide extensive PeopleSoft migration expertise and experience. Visit Migration Central for information on SI partners that have done successful PeopleSoft deployments on Oracle Cloud Infrastructure.

**3rd-Party Integrations:** If you are running PeopleSoft on Oracle Cloud Infrastructure you can integrate with other ISV applications. We have a broad ecosystem of ISV partners that we are working with in our Marketplace already and have a process for onboarding additional ISVs into our cloud.

### **Additional Resources**

#### INSTALLATION GUIDES AND DOCUMENTATION

- [Installing PeopleSoft Cloud Manager in Oracle Cloud Infrastructure](#)
- [Creating a Custom Linux Image for PeopleSoft Cloud Manager on Oracle Cloud Infrastructure](#)
- [Creating a Custom Windows Image for PeopleSoft Cloud Manager on Oracle Cloud Infrastructure](#)
- [Deploying PeopleSoft Applications on Oracle Cloud Infrastructure Instances](#)
- [Learn About Deploying PeopleSoft on Oracle Cloud Infrastructure](#)
- [General Oracle Cloud Infrastructure Documentation](#)

---

## 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](https://blogs.oracle.com)

 [facebook.com/oracle](https://facebook.com/oracle)

 [twitter.com/oracle](https://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.