ORACLE
Cloud Infrastructure

Blueprint: Oracle PeopleSoft on Oracle Cloud Infrastructure

ORACLE WHITE PAPER | NOVEMBER 2019

ORACLE

Disclaimer

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. 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 for Oracle's products remains at the sole discretion of Oracle.

Revision History

The following revisions have been made to this white paper since its initial publication:

Date	Revision
November 15, 2019	Initial publication

Table of Contents

Overview

The Oracle PeopleSoft architecture blueprint bootstraps the design and provisioning processes for a PeopleSoft environment on Oracle Cloud Infrastructure. In addition to covering the foundational services needed to run PeopleSoft on Oracle Cloud Infrastructure, this blueprint covers high availability, security, and connectivity considerations on Oracle Cloud Infrastructure.

This blueprint is intended for Oracle partners and customers who are implementing PeopleSoft on Oracle Cloud Infrastructure. The architectures contained here support both batch and online workloads for up to 7,500 concurrent users on Oracle Cloud Infrastructure. We recommend customers test this blueprint before using it in production to ensure that it meets their requirements.

Note: Many PeopleSoft customers use nonproduction or test and development environments in addition to their production environment. The architecture for these environments can be derived from this blueprint based on the organization's needs (such as storage size, user count, performance requirements, and so on).

Oracle Cloud Infrastructure Services

This blueprint references core Oracle Cloud Infrastructure services such as Compute, Database, Networking, and Storage. It also references other Oracle Cloud Infrastructure services such as Identity and Access Management (IAM), Monitoring, Audit, Policy Management, and Service Gateway. These services help to secure the environment and support business continuity if a service outage occurs. You need to customize the blueprint based on your specific requirements for performance, high availability, and recovery (RPO/RTO).

Conceptual View of a PeopleSoft Environment

A typical PeopleSoft environment has three tiers:

- **Web tier:** A Java-enabled web server is required to extend the PeopleSoft architecture to the internet and intranet.
- **Application and Process Scheduler tier:** The application server is the core of the PeopleSoft internet architecture. It runs business logic and submits SQL to the database server. An application server consists of numerous PeopleSoft server processes, grouped in domains. The Process Scheduler runs with many of your batch programs, such as application engine programs.
- **Database tier:** The database server houses a database engine and your PeopleSoft application database, which includes all the PeopleTools metadata, application definitions, system tables, application tables, and application data.

Figure 1 illustrates the relationship among these tiers.

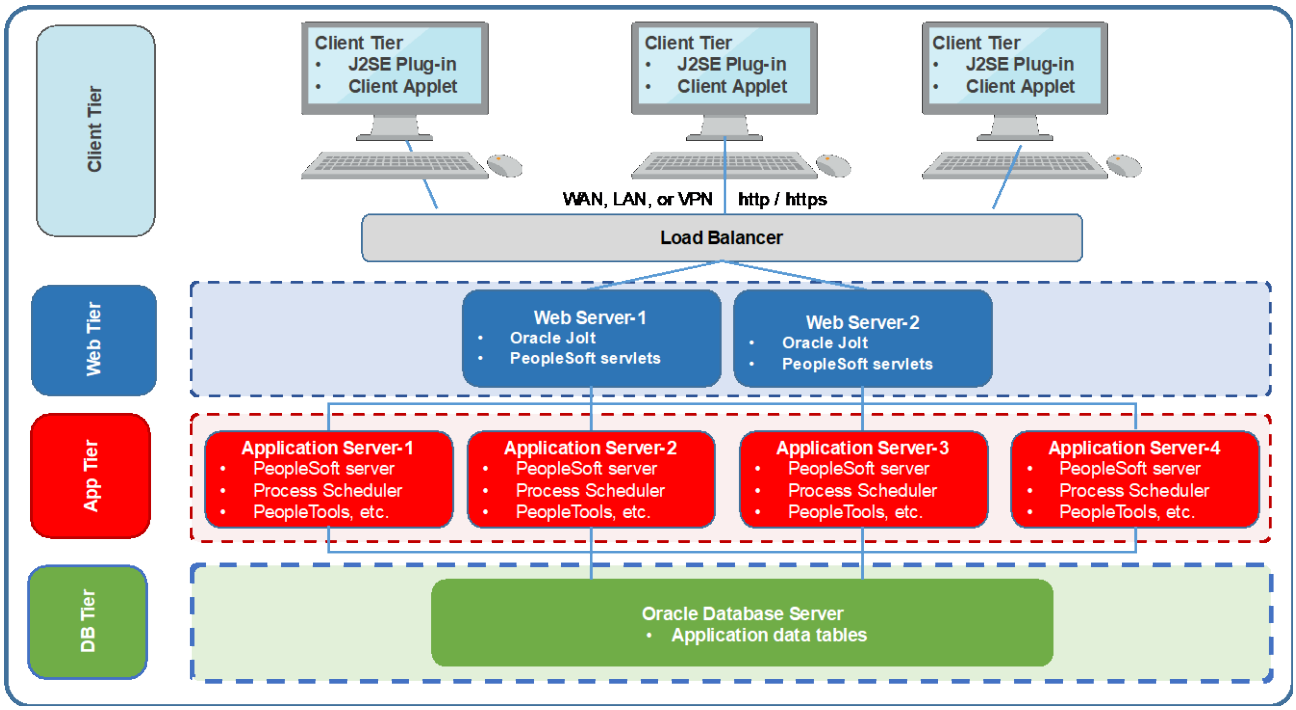

Figure 1: Typical PeopleSoft Tiers and Components

Table 1 summarizes the components shown in Figure 1.

TABLE 1: TYPICAL ORACLE PEOPLESOFT APPLICATION STACK

Component	Function
Load Balancer	Provides automatic load balancing of PeopleSoft client connections across multiple PeopleSoft web servers.
Web Servers	A Java-enabled web server is required to extend the PeopleSoft architecture to the internet and corporate intranet. This server runs a collection of PeopleSoft Java servlets designed to handle a wide range of PeopleSoft transactions.
Application Servers	Servers running application engine programs and process scheduler/batch processing services. Mainly used for high availability and parallel processing of client requests.
Database Server	An Oracle Database cloud service used to store application schemas for PeopleSoft applications.

Reference Architecture for PeopleSoft on Oracle Cloud Infrastructure

PeopleSoft can be run in a single availability domain or multiple availability domains.

Single-Availability-Domain, Multiple-Region Architecture

The following architecture is for PeopleSoft on Oracle Cloud Infrastructure in a single-availability-domain region with the disaster recovery (DR) site built in another Oracle Cloud Infrastructure region. For asynchronous replication, we use the `rsync` command for web and application tiers; however, database synchronization is performed using Oracle Data Guard between two cloud regions.

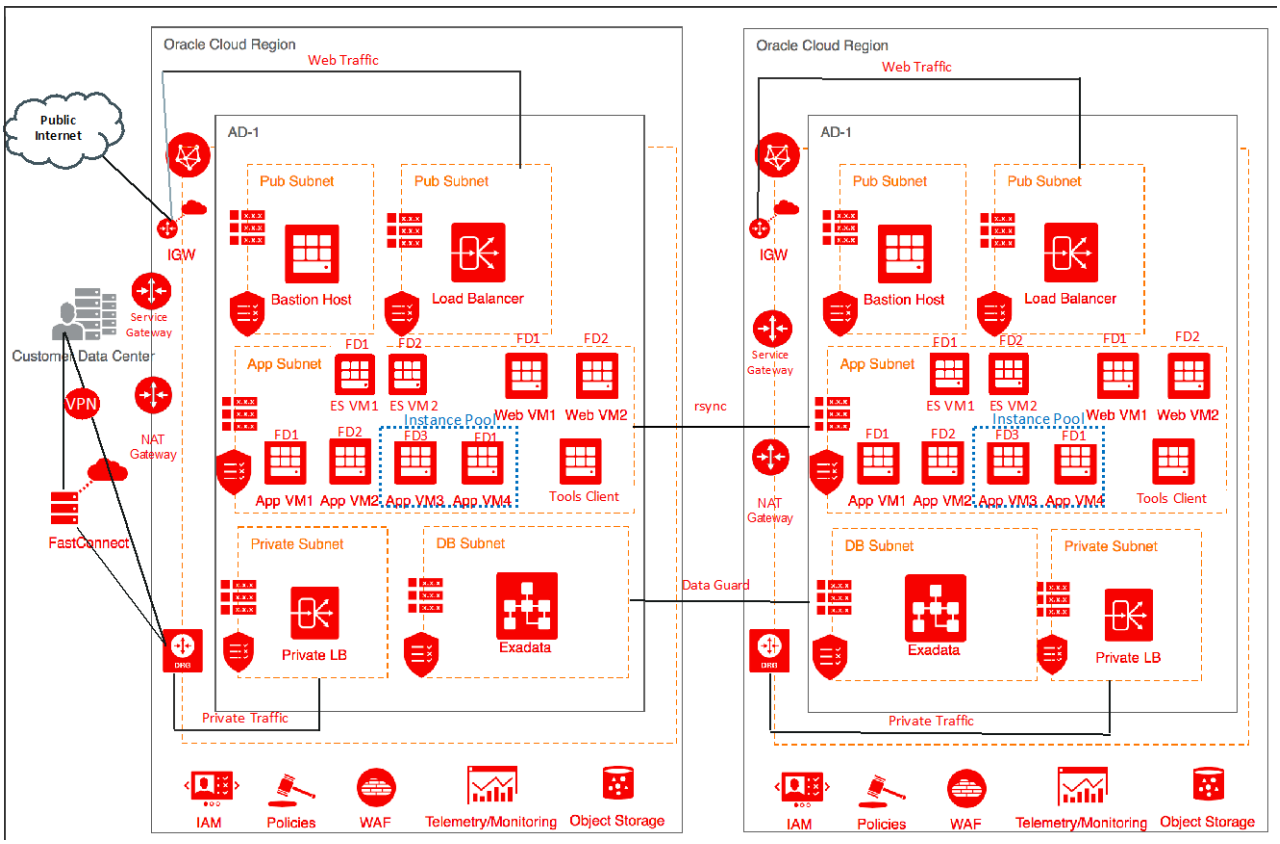

Figure 2: PeopleSoft on Oracle Cloud Infrastructure: Single Availability Domain, Multiple Fault Domains, Two Regions

Multiple-Availability-Domain, Single-Region Architecture

The following architecture is for PeopleSoft on Oracle Cloud Infrastructure in a multiple-availability-domain region. The primary/production instance is running in one availability domain with the DR site built in another availability domain. For asynchronous replication, we use the `rsync` command for web and application tiers; however, database synchronization is performed using Oracle Data Guard between the primary/production instance and the DR instance. You can also choose another Oracle Cloud Infrastructure cloud region for your DR site.

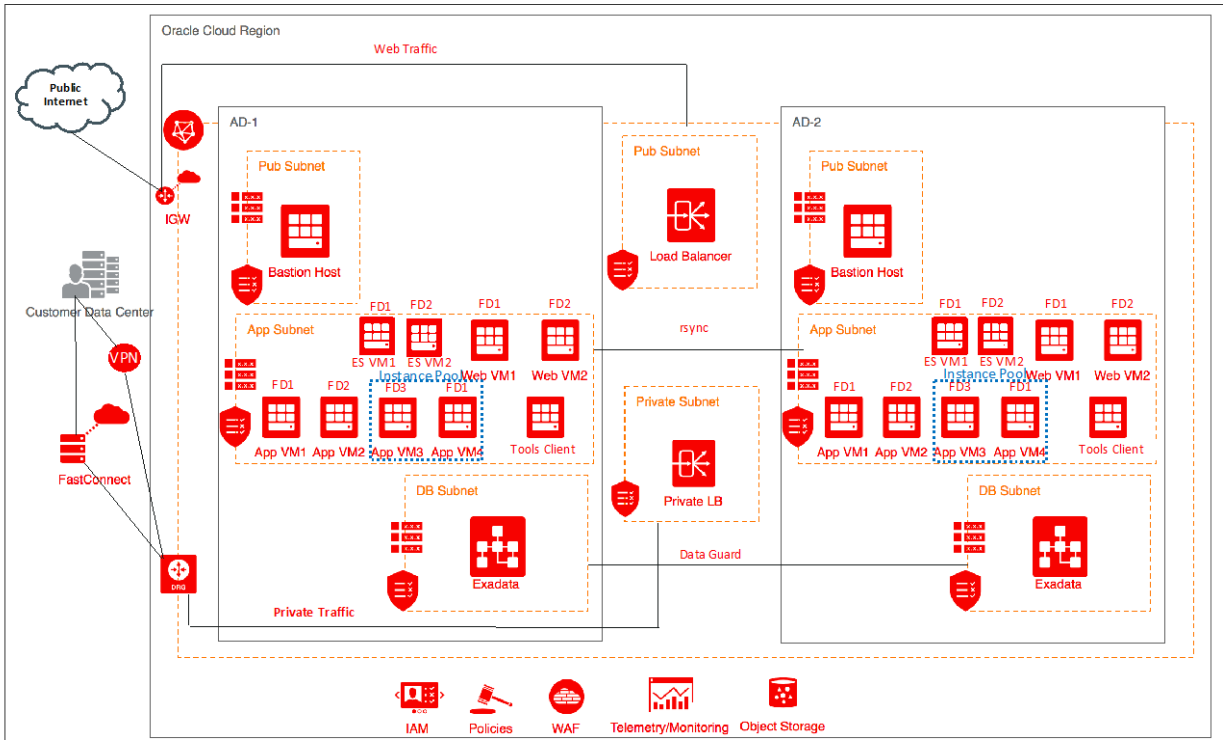

Figure 3: PeopleSoft on Oracle Cloud Infrastructure: Multiple Availability Domains, Single Region

Architectural Details

- **Traffic management**: Two Oracle Cloud Infrastructure load balancers are used in this architecture: a public load balancer and a private load balancer. The public one manages traffic from the public internet, and the private one manages traffic from the customer's network to the application servers.
- **High availability**: Each application server and web server is placed in a separate fault domain to increase the overall availability of the servers if hardware fails.

- **Database**: A quarter-rack (two-node Oracle RAC) Exadata DB system is depicted in this architecture for performance and higher availability. If requirements can be met with other Oracle Database systems, substitute Exadata with an Oracle Cloud Infrastructure VM or bare metal DB system.

  Note: If Exadata isn't a viable option (because of cost or regional availability), an alternative shape that you can use to support this configuration is the BM.DenseIO2.52 shape. However, this option is a single-instance database that doesn't provide high availability.

- **Disaster recovery**: In the single-availability-domain configuration, DR is accomplished by using another region. In the multiple-availability-domain configuration, DR is accomplished by crossing availability domains. The distance between the two availability domains might not meet the site separation requirements for some customers.
- **Built for scale:** This architecture uses instance pools in the application tiers for both the primary and DR environments. The advantage of using instance pools is that you can start with a smaller footprint and use Oracle Cloud Infrastructure's autoscaling feature to grow to support more concurrent users.

  Note: This blueprint uses an instance pool to support an increase in concurrent users. However, if you anticipate close to 7500 concurrent users immediately, we recommend that you provision four VMs in your production application tier. The DR tier can still be provisioned using an instance pool.

Use Terraform to Kickstart Environment Provisioning

Oracle Cloud Infrastructure uses Terraform to automate Oracle Cloud Infrastructure provisioning. The Terraform template at the following link provisions the PeopleSoft architectures depicted in Figures 2 and 3:

- https://orahub.oraclecorp.com/niranjan_mohapatra/oci_partner/tree/master/Oracle_PSFT (internal to Oracle)
- https://github.com/oci-partner/Oracle-PeopleSoft (publicly available)

Follow these instructions to get started with the Terraform template.

Note: To run the Terraform code and connect to Oracle Cloud Infrastructure with the command line, you need to configure your desktop or laptop with the required packages or RPMs. Instructions for the Terraform and command line setup are in the documentation.

1. Download the code repository to a local folder.
2. Open a terminal window and navigate to the local folder that contains the repository.

3. Deploy the Terraform module:

```
terraform init
terraform plan
terraform apply
```

Configuration Details

This section describes the Oracle Cloud Infrastructure resources, subnets, route tables, and security lists that are used to build the Oracle PeopleSoft architecture on Oracle Cloud Infrastructure. After the infrastructure is provisioned using Terraform, ensure that your security lists enable access to the appropriate TCP and UDP ports at the operating system. This enables communication among the web, application, and database tiers.

Oracle Cloud Infrastructure Resources

Table 2 describes the Oracle Cloud Infrastructure resources that are used in the blueprint and template.

TABLE 2: ORACLE CLOUD INFRASTRUCTURE RESOURCES USED IN THE BLUEPRINT

Component	Function
Compute	• Eight VM.Standard1.8 VMs are used as PeopleSoft application servers/process schedulers (four for production, four for DR). The PeopleSoft team recommends the application server-process scheduler combination. • Four VM.Standard1.8 VMs are used as web servers (two for production, two for DR). • Two VM.Standard1.8 VMs are used as PeopleTools clients (one for production, one for DR). • Four VM.Standard1.8 VMs are used for elastic search (two for production, two for DR).
Exadata Cloud Service	Two quarter-rack Oracle Database Exadata instances (one for production and one for DR) are used for the PeopleSoft database.
Public load balancers	Two public load balancers are used, one for production and one for DR.
Private load balancers	Two private load balancers are used, one for production and one for DR.
Virtual cloud network (VCN)	A VCN is used for internal and external access to the compute and database nodes.
Internet gateway	The internet gateway is used for internet access and for internet users connecting to PeopleSoft.
Dynamic routing gateway (DRG)	A dynamic routing gateway is used for private access from an on-premises data center to Oracle Cloud Infrastructure and to connect to PeopleSoft.

Component	Function
NAT gateway	A NAT gateway is used for egress internet access for the compute or database instances in private subnets. It enables instances in private subnets to access the internet for necessary software patches and updates.
Service gateway	A service gateway is used to access Oracle Cloud Infrastructure Object Storage and other services running on Oracle Cloud Infrastructure.
Route tables	Five route tables are created with different route rules. For details, see Route Tables.
DNS	DNS is used to automatically assign fully qualified names for the Oracle Cloud Infrastructure hosts.
Regional subnets	Seven regional subnets are created with the appropriate CIDR block. For details, see Regional Subnets.
Security lists	Seven security lists are created with different TCP/UDP ports enabled for ingress and egress traffic. For details, see Security Lists.
Bastion hosts	Two VM.Standard1.8 compute shapes are used as bastion hosts, one for production and one for DR.
File Storage	A File Storage system is used for shared Network File Storage (NFS) storage for the shared storage.
Object Storage	Object Storage is used for backup of the application tier after each patch and backup of the database.
Web Application Firewall (WAF)	WAF is used to protect the PeopleSoft application from certain internet-based threats.
Identity and Access Management (IAM)	IAM provides tools and policies that control access to Oracle Cloud Infrastructure resources.
Audit	Audit automatically records calls to all supported Oracle Cloud Infrastructure public API endpoints as log events. The default retention period is 90 days.

Regional Subnets

Figure 4 shows the relationship between the VCN and the regional subnets. Table 3 describes the function of each subnet.

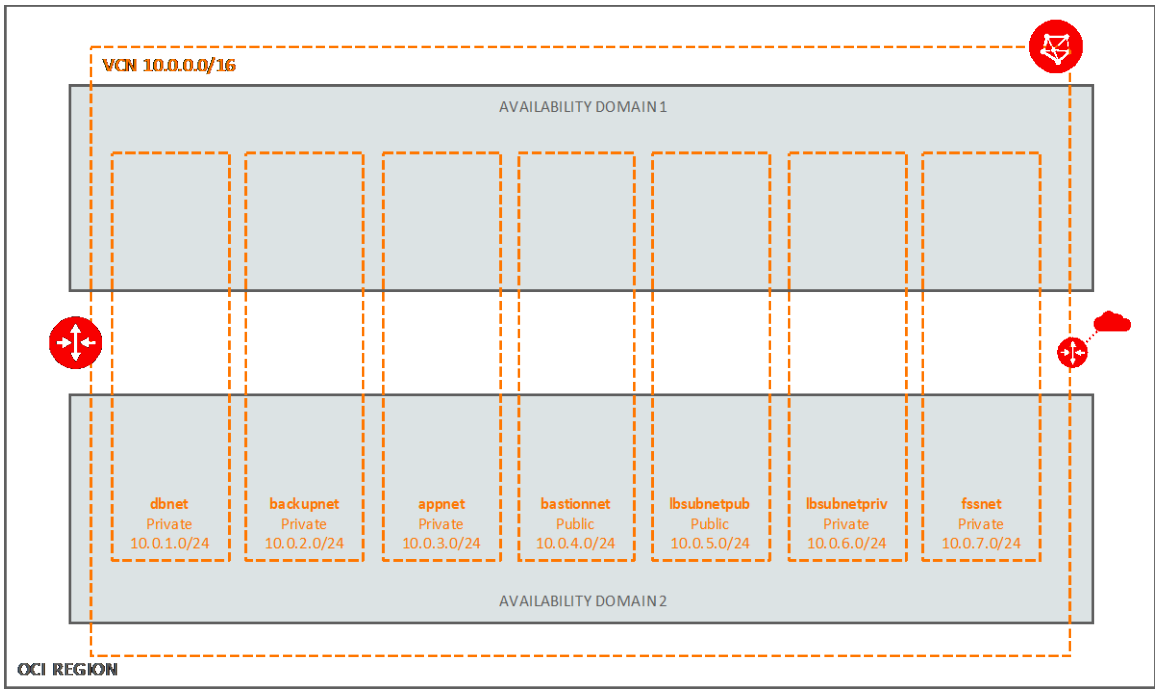

Figure 4: Relationship Between the VCN and Subnets

TABLE 3: REGIONAL SUBNETS USED IN THE BLUEPRINT

Subnet	Function
dbnet	A private subnet for the Exadata database node access
backupnet	A private subnet for the Exadata database backup
appnet	A private subnet for the Oracle PeopleSoft application stack
bastionnet	A public subnet for the bastion hosts
lbsubnetpub	A public subnet for the public load balancer
lbsubnetpriv	A private subnet for the private load balancer
fssnet	A private subnet for File Storage system access

Route Tables

Figure 5 shows the relationship among the VCN, regional subnets, and route tables. Table 4 provides information about each route table.

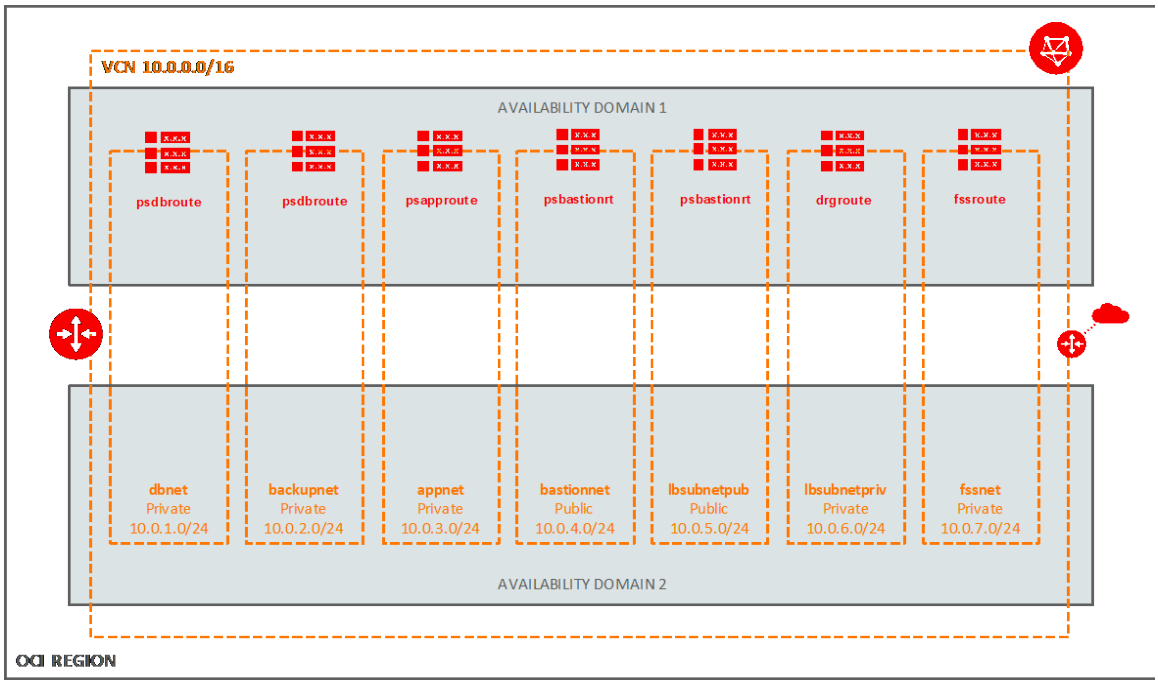

Figure 5: Relationship Among the VCN, Subnets, and Route Tables

TABLE 4: ROUTE TABLES USED IN THE BLUEPRINT

Route Table	Destination CIDR	Target Type	Function
psdbroute	0.0.0.0/0 Object Storage	NAT gateway Service gateway	Two route rules are created, one using the target type as NAT gateway and one for database backup using the target type as service gateway
psapproute	0.0.0.0/0	NAT gateway	One rule is created using the target type as NAT gateway.
psbastionrt	0.0.0.0/0	Internet gateway	One rule is created using the target type as internet gateway.
fssroute	0.0.0.0/0	Internet gateway	One rule is created using the target type as internet gateway.
drgroute	Customer Network	DRG	One rule is created using the target type as DRG.

Security Lists

Figure 6 shows the relationship among the VCN, regional subnets, and security lists. The sections that follow provide details about each security list.

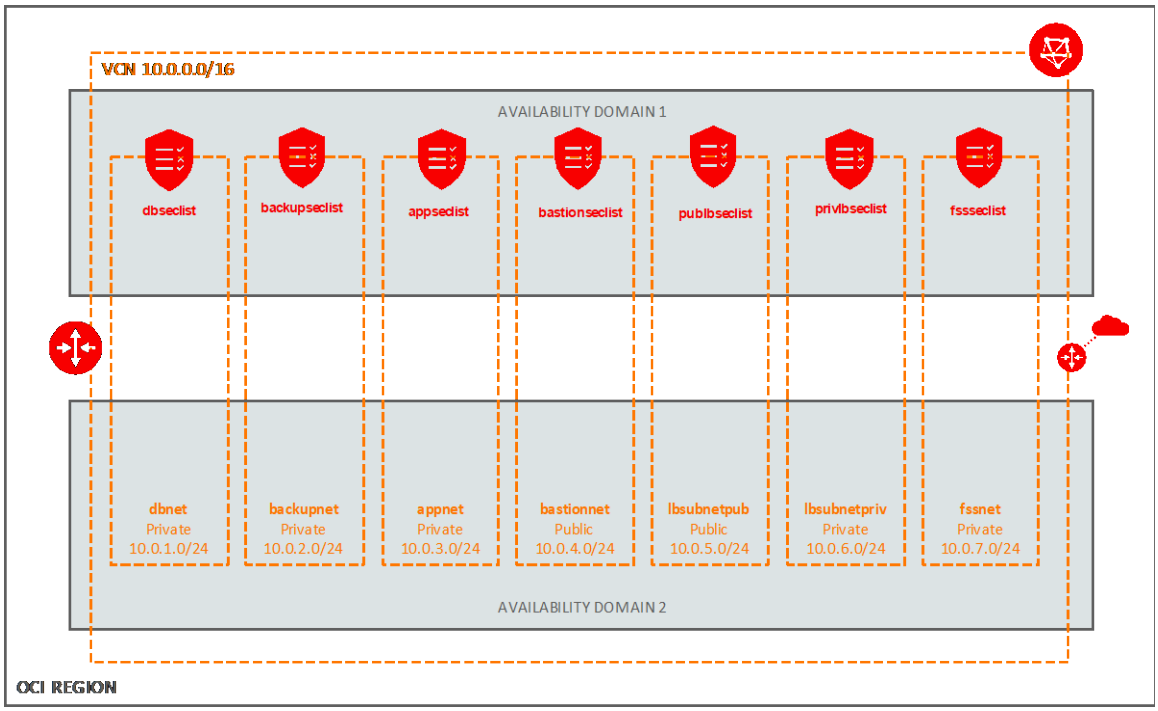

Figure 6: Relationship Among the VCN, Subnets, and Security Lists

dbseclist

The dbseclist security list has the following rules.

PERMIT TRAFFIC FROM THE BASTION HOST TO THE DATABASE TIER

Type	Source Type	Source	IP Protocol	Source Port Range	Destination Port Range	Allows
Ingress (stateful)	CIDR	<10.0.4.0/24>	TCP	All	22	TCP Traffic for Ports: 22

PERMIT TRAFFIC FROM THE APPLICATION TIERS TO THE DATABASE TIER

Type	Source Type	Source	IP Protocol	Source Port Range	Destination Port Range	Allows
Ingress (stateful)	CIDR	<10.0.3.0/24>	TCP	All	1521	TCP Traffic for Ports: 1521

PERMIT TRAFFIC FROM THE DATABASE TIER TO THE APPLICATION TIER

Type	Source Type	Source	IP Protocol	Source Port Range	Destination Port Range	Allows
Egress (stateful)	CIDR	10.0.3.0/24	TCP	All	All	TCP Traffic for Ports: All

PERMIT TRAFFIC BETWEEN THE DATABASE TIERS ACROSS AVAILABILITY DOMAINS FOR ORACLE ACTIVE DATA GUARD (FOR MULTIPLE-AVAILABILITY-DOMAIN ARCHITECTURE)

Type	Source Type	Source	IP Protocol	Source Port Range	Destination Port Range	Allows
Ingress (stateful)	CIDR	<10.0.1.0/24>	TCP	All	1521	TCP Traffic for Ports: 1521

For Oracle Database Exadata DB system provisioning, the following security rules are required:

Type	Source Type	Source	IP Protocol	Source Port Range	Destination Port Range	Allows
Ingress (stateful)	CIDR	<10.0.1.0/24>	TCP	All	All	TCP Traffic for Ports: All
Egress (stateful)	CIDR	0.0.0.0/0	TCP	All	All	TCP Traffic for Ports: All

Type	Source Type	Source	IP Protocol	Type	Code	Allows
Ingress (stateful)	CIDR	<10.0.1.0/24>	ICMP	All	All	ICMP Traffic for: All
Egress (stateful)	Service	0.0.0.0/0	ICMP	All	All	ICMP Traffic for: All

backupseclist

The backupseclist security list has the following rule.

PERMIT TRAFFIC FOR BACKUP OF DATABASE TO ORACLE CLOUD INFRASTRUCTURE OBJECT STORAGE

Type	Source Type	Source	IP Protocol	Source Port Range	Destination Port Range	Allows
Egress (stateful)	Service	<region> Object Storage	TCP	All	443	TCP Traffic for Ports: 443

appseclist

The appseclist security list has the following rules.

PERMIT TRAFFIC FROM THE BASTION HOST TO THE APPLICATION TIER (WEB SERVER, APPLICATION SERVER, AND ELASTIC SEARCH SERVER)

Type	Source Type	Source	IP Protocol	Source Port Range	Destination Port Range	Allows
Ingress (stateful)	CIDR	<10.0.4.0/24>	TCP	All	22	TCP Traffic for Ports: 22

PERMIT TRAFFIC FROM THE BASTION HOST TO THE PEOPLETOOL CLIENT (WINDOWS OS)

Type	Source Type	Source	IP Protocol	Source Port Range	Destination Port Range	Allows
Ingress (stateful)	CIDR	<10.0.4.0/24>	TCP	All	3389	TCP Traffic for Ports: 3389

PERMIT TRAFFIC FROM THE PUBLIC LOAD BALANCER TIER TO THE WEB SERVER OF THE APPLICATION TIER

Type	Source Type	Source	IP Protocol	Source Port Range	Destination Port Range	Allows
Ingress (stateful)	CIDR	<10.0.5.0/24>	TCP	All	8000, 8443	TCP Traffic for Ports: 8000, 8443

PERMIT TRAFFIC FROM THE PRIVATE LOAD BALANCER TIER TO THE WEB SERVER OF THE APPLICATION TIER

Type	Source Type	Source	IP Protocol	Source Port Range	Destination Port Range	Allows
Ingress (stateful)	CIDR	<10.0.6.0/24>	TCP	All	8000, 8443	TCP Traffic for Ports: 8000, 8443

PERMIT TRAFFIC ACROSS THE APPLICATION TIER (WEB SERVER, APPLICATION SERVER, ELASTIC SEARCH SERVER, AND PEOPLETOOLS CLIENT)

Type	Source Type	Source	IP Protocol	Source Port Range	Destination Port Range	Allows
Ingress (stateful)	CIDR	<10.0.3.0/24>	TCP	All	All	TCP Traffic for Ports: All

PERMIT TRAFFIC FROM THE APPLICATION TIER TO THE DATABASE TIER AND ACROSS APPLICATION INSTANCES IN THE APPLICATION TIER

Type	Source Type	Source	IP Protocol	Source Port Range	Destination Port Range	Allows
Egress (stateful)	CIDR	0.0.0.0/0	TCP	All	All	TCP Traffic for Ports: All

publbseclist

The publbseclist security list has the following rules.

PERMIT TRAFFIC FROM THE INTERNET TO THE LOAD BALANCER

Type	Source Type	Source	IP Protocol	Source Port Range	Destination Port Range	Allows
Ingress (stateful)	CIDR	0.0.0.0/0	TCP	All	443, 8000, 8448	TCP Traffic for Ports: 443, 8000, 8448

PERMIT TRAFFIC FROM THE LOAD BALANCER TIERS TO THE APPLICATION TIERS

Type	Source Type	Source	IP Protocol	Source Port Range	Destination Port Range	Allows
Egress (stateful)	CIDR	<10.0.3.0/24>	TCP	All	8000, 8448	TCP Traffic for Ports: 8000, 8448

privlbseclist

The privlbseclist security list has the following rules.

PERMIT TRAFFIC FROM THE ON-PREMISES CUSTOMER NETWORK TO THE LOAD BALANCER

Type	Source Type	Source	IP Protocol	Source Port Range	Destination Port Range	Allows
Ingress (stateful)	CIDR	<customer network IP>	TCP	All	443, 8888	TCP Traffic for Ports: 443, 8888

PERMIT TRAFFIC FROM THE LOAD BALANCER TIERS TO THE APPLICATION TIERS

Type	Source Type	Source	IP Protocol	Source Port Range	Destination Port Range	Allows
Egress (stateful)	CIDR	<10.0.3.0/24>	TCP	All	8000, 8448	TCP Traffic for Ports: 8000, 8448

fssseclist

The fssseclist security list has the following rules.

Type	Source Type	Source	IP Protocol	Source Port Range	Destination Port Range	Allows
Ingress (stateful)	CIDR	<10.0.7.0/24>	UDP	All	2048	UDP Traffic for Ports: 2048
Ingress (stateful)	CIDR	<10.0.7.0/24>	UDP	All	111	UDP Traffic for Ports: 111
Ingress (stateful)	CIDR	<10.0.7.0/24>	TCP	All	2048–2050	TCP Traffic for Ports: 2048-2050
Ingress (stateful)	CIDR	<10.0.7.0/24>	TCP	All	111	TCP Traffic for Ports: 111
Egress (stateful)	CIDR	<CIDR>	TCP	2048–2050	All	TCP Traffic for Ports: 2048-2050
Egress (stateful)	CIDR	<CIDR>	TCP	111	All	TCP Traffic for Ports: 111
Egress (stateful)	CIDR	<CIDR>	UDP	111	All	UDP Traffic for Ports: 111

bastionseclist

The bastionseclist security list has the following rules.

PERMIT SSH TRAFFIC FROM THE ON-PREMISES NETWORK TO THE BASTION HOST OVER THE INTERNET

Type	Source Type	Source	IP Protocol	Source Port Range	Destination Port Range	Allows
Ingress (stateful)	CIDR	0.0.0.0/0	TCP	All	22	TCP Traffic for Ports: 22

Traffic to the bastion host can also be restricted to only your data center. To enable this, create a security rule with your edge router IP address instead of the source CIDR as 0.0.0.0/0 in the stateful ingress rule.

PERMIT SSH TRAFFIC FROM THE BASTION HOST TO COMPUTE INSTANCES

Type	Source Type	Source	IP Protocol	Source Port Range	Destination Port Range	Allows
Egress (stateful)	CIDR	0.0.0.0/0	TCP	All	22	TCP Traffic for Ports: 22

Appendix: Oracle Cloud Infrastructure Service Descriptions

This appendix provides brief descriptions of the Oracle Cloud Infrastructure resources, with context provided for PeopleSoft.

Virtual Cloud Network

A virtual cloud network (VCN) is a private network that resembles a traditional network with firewall rules, subnets, and specific types of communication gateways that you can choose to use. You create a VCN to access the resources created on Oracle Cloud Infrastructure. A VCN resides in a single region.

For PeopleSoft, we recommend creating separate subnets and security lists for different instances, such as the bastion host, database instances, application instances, and the load balancer. Doing so ensures that appropriate security requirements can be implemented across the different subnets.

For more recommendations, see Securing Networking: VCN, Load Balancers, and DNS.

Private or Public Regional Subnet

To decide whether a PeopleSoft tier should have a public or private subnet, first decide whether you want to permit internet access to each tier of PeopleSoft instances. Instances that you create in a public subnet are assigned a public IP address and are accessible from the internet. You can't assign a public IP address to instances created in a private subnet.

In this architecture, the database servers are placed in a private subnet. You can access Oracle Cloud Infrastructure instances in the private subnet from your data centers by connecting through the DRG. The DRG is a gateway that connects your on-premises network to your cloud network. To enable communication between the DRG and the customer-premises equipment, use VPN Connect or Oracle Cloud Infrastructure FastConnect. You must also update the route table to enable traffic to and from the DRG.

To learn more about public and private subnets, see the Networking documentation.

NAT Gateway

Network Address Translation (NAT) is a networking technique used to give an entire private network access to the internet without assigning each host a public IPv4 address. The hosts can initiate connections to the internet and receive responses, but they can't receive inbound connections initiated from the internet. When a host in the private network initiates an internet-bound connection, the NAT device's public IP address becomes the source IP address for the outbound traffic. The response traffic from the internet uses that public IP address as the destination IP address. The NAT device then routes the response to the host in the private network that initiated the connection.

A NAT gateway is required for Oracle PeopleSoft to enable instances in private subnets to access internet resources such as application or operating system patches.

To learn more, see the NAT gateway documentation.

Bastion Host

The bastion host is an optional component used as a "jump server" to access instances in private subnets. A bastion host is an Oracle Cloud Infrastructure Linux based compute instance placed in a public subnet and assigned a public IP address to make it internet accessible.

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

To learn more, see the Bastion Hosts white paper.

Web Application Firewall

The Oracle Cloud Infrastructure Web Application Firewall (WAF) is a cloud-based, global security service that protects applications from malicious internet traffic. The WAF protects internet-facing endpoints, providing consistent rule enforcement across a customer's applications.

WAF lets you create and manage rules to limit internet threats such as Cross-Site Scripting (XSS), SQL Injection, and other vulnerabilities defined by Open Web Application Security Project (OWASP). WAF rules can also be created to limit traffic based on geography or the request signature.

To learn more, see the WAF documentation.

Fault Domain

A fault domain is a grouping of hardware within an availability domain. Fault domains enable you to distribute Oracle Cloud Infrastructure instances so that they aren't on the same physical hardware in a single availability domain. As a result, a hardware failure or maintenance affecting one fault domain doesn't affect instances in other fault domains.

In this architecture, we recommend using multiple fault domains for the application tier to limit the impact of a hardware failure.

To learn more, see Regions and Availability Domains.

File Storage

You can deploy Oracle PeopleSoft with multiple application-tier nodes working with an Oracle PeopleSoft database. When you deploy an Oracle PeopleSoft application tier with multiple nodes, you can have either a shared or non-shared application-tier file system. Using a shared application-tier file system reduces storage space requirements and eliminates the need to apply patches to each node.

The Oracle Cloud Infrastructure File Storage service is an option for creating the shared storage resource required for an Oracle PeopleSoft application-tier file system. File Storage is a persistent, shared file system in Oracle Cloud. For instructions on how to use File Storage for PeopleSoft on Oracle Cloud Infrastructure, see Sharing the Application Tier File System in Oracle PeopleSoft Release 12.2 or 12.1.3 Using the Oracle Cloud Infrastructure File Storage Service.

To learn more, see Overview of File Storage.

Load Balancer

The Oracle Cloud Infrastructure Load Balancing service load balancers receive requests from application users and load-balance traffic to PeopleSoft application servers. Use a load balancer to distribute traffic to your application instances within a VCN. This service provides a primary

instance and standby instance of the load balancer. If the primary load balancer goes offline, the standby load balancer forwards the requests.

The load balancer ensures that requests are routed to healthy application instances. If there's a problem with an application instance, then the load balancer removes that instance from configuration and starts routing requests to the remaining healthy application instances.

To learn more, see Overview of Load Balancing.

Service Gateway

A service gateway lets your VCN privately access specific Oracle services without exposing the data to the public internet. No internet gateway or NAT is required to reach those services. The resources in the VCN can be in a private subnet and use only private IP addresses. The traffic from the VCN to the Oracle service travels over the Oracle network fabric and never traverses the internet.

To learn more, Access to Oracle Services: Service Gateway.

Compute

To provide high availability, the PeopleSoft application tier contains more than one Oracle Cloud Infrastructure Compute service instance. We recommend distributing application instances across multiple fault domains or availability domains to limit downtime if a single application instance becomes unavailable.

To learn more, see Overview of the Compute Service.

Autoscaling

Autoscaling lets you automatically adjust the number of Compute instances in an instance pool based on performance metrics such as CPU utilization. As load increases, instances are automatically provisioned: the instance pool scales out. As load decreases, instances are automatically removed: the instance pool scales in. This helps you provide consistent performance for your end users when demand is high and reduce your costs when demand is low.

To learn more, see Autoscaling.

Database

The database tier uses Oracle Cloud Infrastructure Database service instances. If you have high-availability requirements, we recommend using an Oracle Real Application Clusters (RAC) database on a two-node VM database system or Exadata DB system.

To learn more, see Overview of the Database Service.

Identity and Access Management

Oracle Cloud Infrastructure Identity and Access Management (IAM) lets you control who has access to your cloud resources. You can control what type of access a group of users has and to which specific resources. A policy is a document that specifies who can access which resources, and how this access is permitted. Access is granted at the group and compartment level. As a result, you can write a policy that gives a group a specific type of access within a specific compartment, or to the tenancy itself. If you give a group access to the tenancy, the group automatically gets the same type of access to all the compartments in the tenancy.

To learn more, see Overview of Oracle Cloud Infrastructure Identity and Access Management.

Audit

The Oracle Cloud Infrastructure Audit service automatically records calls to all supported Oracle Cloud Infrastructure public API endpoints as log events. Currently, all services support logging by Audit. Object Storage supports logging for bucket-related events, but not for object-related events. Log events recorded by the Audit service include API calls made by the Oracle Cloud Infrastructure Console, CLI, SDK, your own custom clients, or other Oracle Cloud Infrastructure services. Information in the logs shows what time API activity occurred, the source of the activity, the target of the activity, what the action was, and what the response was.

Each log event includes a header ID, target resources, timestamp of the recorded event, request parameters, and response parameters. You can view events logged by the Audit service by using the Console, API, or the SDK for Java. You can view events, copy the details of individual events, and analyze events or store them separately. You can use data from events to perform diagnostics, track resource usage, monitor compliance, and collect security-related events.

To learn more, see Overview of Audit.

ORACLE

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

CONNECT WITH US

blogs.oracle.com/oracle
facebook.com/oracle
twitter.com/oracle
oracle.com

Integrated Cloud Applications & Platform Services

Blueprint: Oracle PeopleSoft on Oracle Cloud Infrastructure
November 2019
Author: Oracle Corporation