[Go to primary content](" \l "BEGIN)

|  |  |  |  |
| --- | --- | --- | --- |
| **\*\*\*\*\*Main book title missing in bookmap\*\*\*\*\*** | |  |  | | --- | --- | |  | [Contents](file:///C:\Projects\Solutions\Jira%2030538%20-%20Sylaja%20-%206\E93707_01\html\toc.htm) | |

|  |  |  |
| --- | --- | --- |
| [Previous](file:///C:\Projects\Solutions\Jira%2030538%20-%20Sylaja%20-%206\E93707_01\html\GUID-C464062F-FF7F-4043-B302-76A8CD5AF3A8.htm) | [Next](file:///C:\Projects\Solutions\Jira%2030538%20-%20Sylaja%20-%206\E93707_01\html\GUID-6123C9DB-93D7-42C2-8128-6E357FC64BA0.htm) |  |

# Learn About Deploying PeopleSoft on Oracle Cloud Infrastructure

Use this information to help you plan a multihost, secure, and highly available topology for deploying Oracle’s PeopleSoft on Oracle Cloud Infrastructure.

Learn about the key concepts that you need to understand to plan these deployment options:

* Architecture to deploy PeopleSoft in a single availability domain while ensuring high availability.
* Architecture to deploy PeopleSoft in multiple availability domains while ensuring high availability. Use this architecture when you want to ensure that your application is available even when one availability domain goes down. You can still access the application from the other availability domain.
* Architecture to deploy PeopleSoft while ensuring high availability and disaster recovery. Use this architecture when you want to set up a disaster recovery site for your application in a different region.

Use this information to plan the architecture while you perform these tasks:

* Provision PeopleSoft environments in Oracle Cloud Infrastructure
* Lift and shift PeopleSoft environments from your data center to Oracle Cloud Infrastructure

## Terminology

Before you plan your deployment of PeopleSoft on Oracle Cloud Infrastructure, become familiar with the Oracle Cloud Infrastructure terminology.

This table describes the key terms you need to know about.

| **Term** | **Definition** |
| --- | --- |
| Availability domains and regions | Oracle Cloud Infrastructure is physically hosted in regions and availability domains. A region is a localized geographic area, and an availability domain is one or more data centers located within a region. A region is composed of several availability domains. Oracle Cloud Infrastructure resources are either region-specific, such as a virtual cloud network (VCN), or availability domain-specific, such as a compute instance.  Availability domains are isolated from each other, are fault tolerant, and are unlikely to fail simultaneously and are unlikely to be affected by the failure of another availability domain. When you configure your cloud services, use multiple availability domains to ensure high availability and to protect against resource failure. Be aware that some resources must be created in the same availability domain such as an instance and the storage volume attached to it. |
| Database system (DB system) | The database service lets you quickly launch an Oracle database system (DB system) and create one or more databases on it. You have full access to the features and operations available with Oracle Database, but Oracle owns and manages the infrastructure.  You can use one of the following options to set up the database:   * Single-node, real application clusters (RAC) DB system. Oracle doesn’t recommend using this configuration because it doesn’t provide high availability. * Two-node, RAC DB systems on a virtual machine. Both database instances are active and highly available. * Oracle Database Exadata Cloud Service instances. This service provides Oracle Database hosted on Oracle Exadata Database Machine in Oracle Cloud. These database instances provide high availability. |
| Dynamic routing gateway (DRG) | A software-defined router that provides a path for private traffic between your VCN and your data center’s network. You can use a DRG with the Internet Protocol Security (IPSec) virtual private network (VPN) connection and an on-premises router to create a site-to-site VPN. |
| File storage service (FSS) | Use Oracle Cloud Infrastructure File Storage to provide the shared disk resource for an PeopleSoft shared application tier file system. An FSS supports the Network File System version 3.0 (NFSv3) protocol. |
| Internet gateway | A software-defined router that provides a path for network traffic from your VCN to the internet. |
| Instance | An instance is a compute host running in the cloud. An Oracle Cloud Infrastructure Compute instance enables you to utilize hosted physical hardware, as opposed to the traditional software-based virtual machines, ensuring a high level of security and performance. |
| Load balancer | A load balancer improves resource utilization, facilitates scaling, and helps ensure high availability.  Oracle Cloud Infrastructure Load Balancing  provides automated traffic distribution from one entry point to multiple servers that are reachable from your VCN. The service offers a load balancer with your choice of a public or private IP address, and provisioned bandwidth. |
| Security list | A common set of stateful firewall rules that are associated with a subnet and applied to all instances launched in the subnet. Security lists contain ingress and egress rules to filter traffic at the subnet level and contain information which communication ports allow data transfer. |
| Subnet | A section of a VCN’s IP address range that provides logical isolation for resource groups. You create a subnet by subdividing the VCN's address range. When you create a subnet in Oracle Cloud Infrastructure, you specify a contiguous IPv4 Classless Inter-Domain Routing (CIDR) block for the subnet. The subnet's CIDR block must fall within the VCN's CIDR block.  A subnet can’t span availability domains. You assign a subnet to one availability domain. When you launch an instance into a subnet, the instance's private IP address is allocated from the subnet's CIDR block.  When you create a subnet, you can specify whether the access type is private or public. A subnet is created with public access by default, which means that the instances in the subnet can be allocated a public IP address. However, instances launched in a subnet with private access can’t have public IP addresses, which ensures that these instances have no internet access. |
| Virtual cloud network (VCN) | A virtual cloud network is a virtual version of a traditional network—including subnets, route tables, and gateways—that your instances run on. A cloud network resides in a single region but can cross multiple availability domains. You can define subnets for a cloud network in different availability domains, but the subnet itself must belong to a single availability domain. You must set up at least one cloud network before you can launch instances. You can configure the cloud network with an optional internet gateway to handle public traffic, and an optional IPSec VPN connection to securely extend your on-premises network.  When you create your VCN, you assign a contiguous IPv4 CIDR block of your choice. You can create multiple VCNs with overlapping IP address ranges. However, if you intend to connect your VCN to your on-premises network through an IPSec VPN connection, we recommend that you ensure the IP address ranges don’t overlap. |

## Considerations for Deploying PeopleSoft on Oracle Cloud Infrastructure

The architecture doesn’t change if you deploy PeopleSoft manually or by using automation tools.

Private or Public Subnet Access

All the architecture diagrams assume that you don’t want to access your database and application hosts over the internet. The architecture diagrams consist of a virtual cloud network (VCN) with the bastion host, load balancer, application, and database instances placed in separate subnets. Oracle recommends creating separate subnets for the bastion host, database, application, and load balancer instances to ensure that the appropriate security list is assigned to instances in each subnet. In Oracle Cloud Infrastructure, you configure firewall rules through security lists. Create a security list for each subnet. Each subnet in a VCN uses a single route table.

You can create instances in a private or public subnet based on whether you want to permit access to the instances from the internet.

* Scenario 1: Deploying all instances only in a private subnet. In this deployment, the PeopleSoft application and database servers are created in a private subnet. A public IP address can’t be assigned to instances created in the private subnet, so you can’t access these instances over the internet. To access your PeopleSoft servers from your on-premises environment, you can:
  + Configure an IPSec VPN tunnel between your data center and Oracle Cloud Infrastructure before provisioning the PeopleSoft servers.
  + Use a bastion host in this configuration, and then access all the servers in private subnet from the bastion host.

Oracle recommends deploying all instances in private subnets for production environments where there are 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.

* Scenario 2: Deploying a few instances in a public subnet and a few instances in a private subnet. This deployment is useful when the PeopleSoft application server has internet-facing and non-internet-facing endpoints. In this configuration, some PeopleSoft application instances are placed in a public subnet, and others are placed in a private subnet. For example, you may have application instances serving internal users and another set of application instances serving external users. In this scenario, place the application instances serving internal traffic in a private subnet, and place the application servers that serve external traffic in a public subnet. You can also set up a public load balancer on top of the internet-facing application instances, instead of placing the external application servers in a public subnet. If you place the bastion host in a public subnet, then the bastion host is assigned a public IP address, and you can access it over the internet. To access the instances in the private subnet, you can use Secure Shell (SSH) to get to the bastion host. You can then connect to the instance on the private subnet from the bastion host.
* Scenario 3: Deploying all instances in a public subnet. In this deployment, the PeopleSoft application and database instances are created in a public subnet. Every instance in the public subnet has a public IP address attached to it. Although instances with public IP addresses can be accessed over the internet, you can restrict access by using security lists and security rules. Oracle recommends that you place a bastion host in this configuration for administration tasks. Instead of opening administration ports for servers over the internet, you can open the administration ports only for the bastion host and set up security lists to ensure that the instance can be accessed only from the bastion host.

Oracle recommends this deployment for quick demonstrations 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.

This image shows a VCN with public and private subnets.

[Description of the illustration GUID-A548ABCC-C7FA-4926-BD34-B25FA3F6D13F-default.png](file:///C:\Projects\Solutions\Jira%2030538%20-%20Sylaja%20-%206\E93707_01\html\img_text\GUID-A548ABCC-C7FA-4926-BD34-B25FA3F6D13F-default.htm)



You can access Oracle Cloud instances in the public subnet from the internet by enabling communication through the internet gateway (IGW). You’ll have to update the default route table to enable traffic to and from the IGW. You’ll also need to connect the bastion host to the IGW. To permit traffic from the internet, you must create load balancers in the public subnet.

You can access Oracle Cloud instances in the private subnet from your data centers by connecting through the dynamic routing gateway (DRG). The DRG is the gateway that connects your on-premises network to your cloud network. To enable communication between the DRG and the customer-premises equipment object, use Internet Protocol Security (IPSec) virtual private network (VPN) or Oracle Cloud Infrastructure FastConnect. You’ll also have to update the default route table to enable traffic to and from the DRG.

Logical Host Names

Oracle recommends that you use logical host names, not physical host names, when you set up the PeopleSoft database tier and application tier. The advantages of using logical host names are:

* Hide the servers that host the application and business software from end users for better security.
* Provide the capability of moving the database and application tiers to other machines without running a clone.
* Reduce the amount of reconfiguration required on failover for disaster recovery by using the same host name on the active and standby sites.
* Avoid rewiring or recloning the database and application tiers due to network configuration changes, such as a host name change.
* Seamlessly support data center migration by keeping the same logical host name.
* Simulate multiple machines on the same physical hardware for hosting external and internal sites.
* Use the logical host name to bind, and use the physical host name to access the application.

## Architecture for Deploying PeopleSoft in a Single Availability Domain

This architecture shows the deployment of a PeopleSoft application in a single availability domain while ensuring high availability.

The architecture consists of a virtual cloud network (VCN) with the bastion, load balancer, application, and database hosts placed in separate subnets of the VCN in a single availability domain. All instances in this architecture are deployed only in private subnets. You can place the different instances in public or private subnets based on your business requirements.

[Description of the illustration GUID-DFF9A128-D0F8-4AC2-9B68-4E40111374DA-default.png](file:///C:\Projects\Solutions\Jira%2030538%20-%20Sylaja%20-%206\E93707_01\html\img_text\GUID-DFF9A128-D0F8-4AC2-9B68-4E40111374DA-default.htm)



This architecture is divided into these tiers:

* Bastion host: The bastion host is an optional component that you can use as a jump server to access the instances in the private subnet. When you place the bastion host in private subnet, you can use it as a secondary option to Internet Protocol Security (IPSec) virtual private network (VPN).
* Load Balancer tier: This tier contains the Oracle Cloud Infrastructure Load Balancing instances that load balances the traffic to application hosts. The load balancer receives requests from users, and then routes these requests to application servers.
* Application tier: This tier contains more than one instance of the PeopleSoft application servers to provide high availability. Set up multiple instances of an application to ensure that you can continue accessing the application even if an application server goes down. To ensure high availability in an availability domain, you must have two instances of a web private internet access (PIA), an elastic search cluster, a PeopleSoft application server, and a Windows process scheduler.
* Windows client: Use the Windows client to perform administration activities, such as migration and upgrade.
* Database tier: This tier contains Oracle Cloud Infrastructure database system instances. For high availability requirements, Oracle recommends that you use two-node, real application clusters (RAC )DB systems or an Oracle Exadata system of Oracle Cloud Infrastructure.

## Architecture for Deploying PeopleSoft in Multiple Availability Domains

This architecture shows the deployment of PeopleSoft application servers in multiple availability domains. It shows a virtual cloud network (VCN) with the bastion, load balancer, application, and database hosts placed in separate subnets across two availability domains.

The bastion hosts in Availability Domain 1 and Availability Domain 2 are active and receive requests. The load balancer distributes traffic to the web private internet access (PIA) hosts in Availability Domain 1 and Availability Domain 2. The web PIA hosts route the request to application servers, and then the application servers forward the requests to the active database servers in Availability Domain 1 for processing.

In the architecture diagram, the bastion host is deployed in a public subnet, and all other instances are deployed in a private subnet. You can place the different instances in public or private subnets based on your business requirements.

[Description of the illustration GUID-23895333-7671-445E-B678-8CC7A9047910-default.png](file:///C:\Projects\Solutions\Jira%2030538%20-%20Sylaja%20-%206\E93707_01\html\img_text\GUID-23895333-7671-445E-B678-8CC7A9047910-default.htm)



This architecture supports these components:

* Bastion host: A bastion host is an optional component that you can provision in each availability domain to act as a jump host to access application and database instances. For example, the bastion host in Availability Domain 2 acts as a jump host to access application and database hosts in Availability Domain 2. Bastion hosts in both Availability Domain 1 and Availability Domain 2 are in the active state.
* Load balancer tier: Oracle Cloud Infrastructure Load Balancing instances distribute traffic across the application servers in both of the availability domains. Availability Domain 1 hosts primary load balancer instances. Availability Domain 2 hosts standby load balancer instances.
* Application tier: Both Availability Domain 1 and Availability Domain 2 contain at least one instance of Web PeopleSoft Internet Architecture (PIA), ES Cluster, an application server, and PeopleSoft Process Scheduler on Windows. All instances in the application tier across the two availability domains are in the active state.

Oracle recommends that you deploy a PeopleSoft multitier setup with shared application binaries. Use Oracle Cloud Infrastructure File Storage to create a shared file system to share PeopleSoft application binaries.

* Windows client: Use a Windows client to perform administration activities, such as migration and upgrade.
* Database tier: Availability Domain 1 hosts the primary database instances. Availability Domain 2 hosts the standby database instances. In each availability domain, at least two database instances are set up to ensure high availability. If a database instance goes down in Availability Domain 1, then the second database instance in Availability Domain 1 continues processing requests.

If Availability Domain 1 goes down, you must manually reroute requests to the bastion host on Availability Domain 2. In this scenario, the load balancer and the database instances in Availability Domain 2 act as the primary load balancer and database instances. The active load balancer in Availability Domain 2 receives requests, and then distributes traffic to the Web PIA instances in Availability Domain 2. The Web PIA instances route the request to application servers, and then the application servers forward the request to the active database servers in Availability Domain 2 for processing.

## Architecture for Deploying PeopleSoft Across Multiple Regions

This architecture shows the deployment of PeopleSoft application servers across multiple regions while ensuring high availability and disaster recovery. It shows a virtual cloud network (VCN) with the bastion, load balancer, application, and database instances placed in separate subnets across two regions.

In the architecture diagram, the bastion host and load balancer is deployed in a public subnet, and all the other instances are deployed in a private subnet. You can place the different instances in public or private subnets based on your business requirements.

To ensure that you can access PeopleSoft application instances, even when all availability domains in a region go down, deploy PeopleSoft across multiple regions. The architecture diagram shows two regions. In Region 1, PeopleSoft is deployed in multiple availability domains to ensure high availability across availability domains within a region. In Region 2, the load balancer, application, and database instances are in the passive state.

[Description of the illustration GUID-F9925BC6-56A6-4BF6-A787-9F87B2FCEAF7-default.png](file:///C:\Projects\Solutions\Jira%2030538%20-%20Sylaja%20-%206\E93707_01\html\img_text\GUID-F9925BC6-56A6-4BF6-A787-9F87B2FCEAF7-default.htm)



This architecture supports these components:

* Bastion host: A bastion host is an optional component that you can provision in each availability domain to act as a jump host to access application and database instances. For example, a bastion host in Availability Domain 2 acts as a jump host to access application and database hosts in Availability Domain 2. Bastion hosts in both Availability Domain 1 and Availability Domain 2 are in the active state.
* Load balancer tier: Oracle Cloud Infrastructure Load Balancing instances distribute traffic across the application servers in both the availability domains. Availability Domain 1 hosts the primary load balancer instances. Availability Domain 2 hosts the standby load balancer instances.
* Application tier: Both Availability Domain 1 and Availability Domain 2 contain at least one instance of Web PeopleSoft Internet Architecture (PIA), ES Cluster, application server, and PeopleSoft Process Scheduler on Windows. All instances in the two availability domains in Region 1 of the application tier are in the active state. The application tier instances in Region 2 are in the passive state. To sync the application servers across availability domains and across the regions, use Rsync.

Oracle recommends that you deploy the PeopleSoft multitier setup with shared application binaries. You can create a shared file system to share PeopleSoft application binaries by using Oracle Cloud Infrastructure File Storage.

* Windows client: Use the Windows client to perform administration activities, such as migration and upgrade.
* Database tier: Availability Domain 1 in Region 1 hosts the primary database instances. Availability Domain 2 in Region 1 and Region 2 host the standby database instances. In each availability domain, at least two database instances are set up to ensure high availability. If a database instance goes down in Availability Domain 1, then the second database instance in Availability Domain 1 continues processing requests. If Region 1 goes down, then the database instances in Region 2 process the requests. To replicate a database across regions, use Oracle Active Data Guard in synchronous mode.

If the instances in Region 1 aren’t available, then you must manually switch over to the instances in Region 2. In this scenario, the load balancer and database instances in Region 2 act as the primary load balancer and database instances. The bastion host in Region 2 receives requests, and then forwards the requests to the instances in Region 2. The load balancer distributes the traffic to the Web PIA instances in Region 2. The Web PIA instances route the requests to application instances, and then the application instances forward the requests to the database instances in Region 2 for processing.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | [Previous](file:///C:\Projects\Solutions\Jira%2030538%20-%20Sylaja%20-%206\E93707_01\html\GUID-C464062F-FF7F-4043-B302-76A8CD5AF3A8.htm) | [Next](file:///C:\Projects\Solutions\Jira%2030538%20-%20Sylaja%20-%206\E93707_01\html\GUID-6123C9DB-93D7-42C2-8128-6E357FC64BA0.htm) |  | | [Copyright © Oracle and/or its affiliates. All rights reserved.](file:///C:\Projects\Solutions\Jira%2030538%20-%20Sylaja%20-%206\dcommon\html\cpyr.htm) | |  |  | | --- | --- | |  | [Contents](file:///C:\Projects\Solutions\Jira%2030538%20-%20Sylaja%20-%206\E93707_01\html\toc.htm) | |