ORACLE
PeopleSoft

PeopleSoft Cloud Manager for Oracle Cloud Infrastructure

March 2021

ORACLE

PeopleSoft Cloud Manager for Oracle Cloud Infrastructure

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Contents

Preface

Understanding the PeopleSoft Online Help and PeopleBooks

The PeopleSoft Online Help is a website that enables you to view all help content for PeopleSoft applications and PeopleTools. The help provides standard navigation and full-text searching, as well as context-sensitive online help for PeopleSoft users.

Hosted PeopleSoft Online Help

You can access the hosted PeopleSoft Online Help on the Oracle Help Center. The hosted PeopleSoft Online Help is updated on a regular schedule, ensuring that you have access to the most current documentation. This reduces the need to view separate documentation posts for application maintenance on My Oracle Support. The hosted PeopleSoft Online Help is available in English only.

To configure the context-sensitive help for your PeopleSoft applications to use the Oracle Help Center, see Configuring Context-Sensitive Help Using the Hosted Online Help Website.

Locally Installed Help

If you're setting up an on-premise PeopleSoft environment, and your organization has firewall restrictions that prevent you from using the hosted PeopleSoft Online Help, you can install the online help locally. See Configuring Context-Sensitive Help Using a Locally Installed Online Help Website.

Downloadable PeopleBook PDF Files

You can access downloadable PDF versions of the help content in the traditional PeopleBook format on the Oracle Help Center. The content in the PeopleBook PDFs is the same as the content in the PeopleSoft Online Help, but it has a different structure and it does not include the interactive navigation features that are available in the online help.

Common Help Documentation

Common help documentation contains information that applies to multiple applications. The two main types of common help are:

- Application Fundamentals
- Using PeopleSoft Applications

Most product families provide a set of application fundamentals help topics that discuss essential information about the setup and design of your system. This information applies to many or all applications in the PeopleSoft product family. Whether you are implementing a single application, some combination of applications within the product family, or the entire product family, you should be familiar with the contents of the appropriate application fundamentals help. They provide the starting points for fundamental implementation tasks.

In addition, the *PeopleTools: Applications User's Guide* introduces you to the various elements of the PeopleSoft Pure Internet Architecture. It also explains how to use the navigational hierarchy, components, and pages to perform basic functions as you navigate through the system. While your application or implementation may differ, the topics in this user's guide provide general information about using PeopleSoft applications.

Field and Control Definitions

PeopleSoft documentation includes definitions for most fields and controls that appear on application pages. These definitions describe how to use a field or control, where populated values come from, the effects of selecting certain values, and so on. If a field or control is not defined, then it either requires no additional explanation or is documented in a common elements section earlier in the documentation. For example, the Date field rarely requires additional explanation and may not be defined in the documentation for some pages.

Typographical Conventions

The following table describes the typographical conventions that are used in the online help.

Typographical Convention	***Description***
Key+Key	Indicates a key combination action. For example, a plus sign (+) between keys means that you must hold down the first key while you press the second key. For Alt+W, hold down the Alt key while you press the W key.
. . . (ellipses)	Indicate that the preceding item or series can be repeated any number of times in PeopleCode syntax.
{ } (curly braces)	Indicate a choice between two options in PeopleCode syntax. Options are separated by a pipe (|).
[ ] (square brackets)	Indicate optional items in PeopleCode syntax.
& (ampersand)	When placed before a parameter in PeopleCode syntax, an ampersand indicates that the parameter is an already instantiated object. Ampersands also precede all PeopleCode variables.
⇒	This continuation character has been inserted at the end of a line of code that has been wrapped at the page margin. The code should be viewed or entered as a single, continuous line of code without the continuation character.

ISO Country and Currency Codes

PeopleSoft Online Help topics use International Organization for Standardization (ISO) country and currency codes to identify country-specific information and monetary amounts.

ISO country codes may appear as country identifiers, and ISO currency codes may appear as currency identifiers in your PeopleSoft documentation. Reference to an ISO country code in your documentation

does not imply that your application includes every ISO country code. The following example is a country-specific heading: "(FRA) Hiring an Employee."

The PeopleSoft Currency Code table (CURRENCY_CD_TBL) contains sample currency code data. The Currency Code table is based on ISO Standard 4217, "Codes for the representation of currencies," and also relies on ISO country codes in the Country table (COUNTRY_TBL). The navigation to the pages where you maintain currency code and country information depends on which PeopleSoft applications you are using. To access the pages for maintaining the Currency Code and Country tables, consult the online help for your applications for more information.

Region and Industry Identifiers

Information that applies only to a specific region or industry is preceded by a standard identifier in parentheses. This identifier typically appears at the beginning of a section heading, but it may also appear at the beginning of a note or other text.

Example of a region-specific heading: "(Latin America) Setting Up Depreciation"

Region Identifiers

Regions are identified by the region name. The following region identifiers may appear in the PeopleSoft Online Help:

- Asia Pacific
- Europe
- Latin America
- North America

Industry Identifiers

Industries are identified by the industry name or by an abbreviation for that industry. The following industry identifiers may appear in the PeopleSoft Online Help:

- USF (U.S. Federal)
- E&G (Education and Government)

Translations and Embedded Help

PeopleSoft 9.2 software applications include translated embedded help. With the 9.2 release, PeopleSoft aligns with the other Oracle applications by focusing our translation efforts on embedded help. We are not planning to translate our traditional online help and PeopleBooks documentation. Instead we offer very direct translated help at crucial spots within our application through our embedded help widgets. Additionally, we have a one-to-one mapping of application and help translations, meaning that the software and embedded help translation footprint is identical—something we were never able to accomplish in the past.

Using and Managing the PeopleSoft Online Help

Select About This Help in the left navigation panel on any page in the PeopleSoft Online Help to see information on the following topics:

- Using the PeopleSoft Online Help
- Managing Hosted online help
- Managing locally installed PeopleSoft Online Help

Contact Us

Send your suggestions to psoft-infodev_us@oracle.com. Please include the applications update image or PeopleTools release that you're using.

Follow Us

YouTube

Twitter@PeopleSoft_Info.

PeopleSoft Blogs

LinkedIn

Chapter 1

Getting Started with PeopleSoft Cloud Manager

Understanding PeopleSoft Cloud Manager on Oracle Cloud Infrastructure

PeopleSoft Cloud Manager is an orchestration framework to provision and manage PeopleSoft environments on Oracle Cloud Infrastructure (OCI). The PeopleSoft Cloud Manger can help creating task specific environments that can last as long as the task is needed. PeopleSoft Cloud Manager will enable you to focus more on business and less on infrastructure management by taking away all the complexities involved in acquiring and managing the infrastructure to run PeopleSoft on OCI.

PeopleSoft Cloud Manager is an application available on the Oracle Cloud Marketplace. Any existing PeopleSoft customer can use it by taking advantage of the Oracle Cloud Service resources.

OCI is a set of complementary cloud services that enable you to build and run a wide range of applications and services in a highly available hosted environment.

Common Abbreviations

Term	***Description***
DPK	PeopleSoft Deployment Packages
PCM	PeopleSoft Cloud Manager
PI	PeopleSoft Image
PRP	PeopleSoft Release Patchset
PUM	PeopleSoft Update Manager
OCI	Oracle Cloud Infrastructure
AD	Availability Domain
VCN	Virtual Cloud Network
TDE	Transparent Data Encryption
OCID	Oracle Cloud ID

Minimum Requirements for PeopleSoft Cloud Manager

Listed below are the minimum requirements for using PeopleSoft Cloud Manager:

- Minimum application version for managed environments is 9.1 for Interaction Hub (IH) and 9.2 for all other applications.
- Minimum PeopleTools version for managed environment is 8.55.12. For provisioning COBOL and Elasticsearch, the minimum tools version is 8.55.13.
- Minimum PeopleTools version for Kibana support by Cloud Manager is 8.58.
- COBOL provisioning with PeopleTools is supported from 8.56.09 onward. For PeopleTools 8.58 and above Visual COBOL is the only supported version.
- Minimum shape of Cloud Manager for OCI is VM.Standard 2.1 or VM.Standard.E2.1.

  Note: Based on the tenancy, the availability of shapes may differ.

- Windows middle tier for PeopleSoft must be on PeopleTools 8.57 or above.
- Prepare the tenancy for PeopleSoft applications deployment. As part of preparing the tenancy, the following must be created:

  See Refer to the OBE.Install Cloud Manager tutorials on Oracle Learning Library.

  - At least one compartment for PeopleSoft deployments.
  - An OCI user with sufficient privileges to create and manage resources in the identified compartment.
  - A Virtual Cloud Network (VCN) with required number of subnets and security lists with proper ingress and egress rules.
  - An object storage bucket.

- Oracle Cloud Infrastructure subscriptions.
  - A subscription to Oracle Cloud Infrastructure Compute is mandatory.
  - A subscription to Oracle Cloud Infrastructure Object Storage is mandatory.
  - A subscription to Oracle Database Cloud Service is optional.

PeopleSoft Cloud Manager – An Overview

Cloud Manager provides a framework for customers to provision and administer the life cycle of PeopleSoft environments on OCI. Cloud Manager brings in the agility to rapidly bring up PeopleSoft environments on demand, based on your infrastructure requirements.

Features of PeopleSoft Cloud Manager

PeopleSoft Cloud Manager provides the ability to:

- Provision PeopleSoft environments on OCI.

- Automate migration of on-premise environment to OCI.
- Support lifting and shifting of unicode or non-unicode database.
- Support lifting and shifting of PeopleSoft application environments which have TDE encrypted databases. The on-premise environments must be TDE encrypted before migrating.
- Support lifting and shifting of Transparent Data Encryption, or TDE, and Real Application Clusters, or RAC, for Database Systems.
- Orchestrate deployment of PeopleSoft 9.2 and IH 9.1 applications on OCI.
- Subscription model to auto download application PIs and PRPs.
- Create repeatable deployment templates.
- Self service provisioning of PeopleSoft environments.
- Fully automate deployment which is immune to manual errors and process delays.
- Manage multiple environments from a single page.
- Enable application lifecycle management in Oracle Cloud.
- Clone environments from running instances.
- Access log files through UI for easy troubleshooting.
- View the status of environment provisioning.
- Automated PRP updates for Cloud Manager instance.
- Define and configure web, app domains in topology/template definitions.
- Refresh DB System environments managed by Cloud Manager including PS_APP_HOME, PS_CUST_HOME, and database, or just the database, from a backup.
- Automate PeopleTools upgrade and updates.
- Self update of Cloud Manager to the most current image from the prior image.
- Enable creating or reusing file system service (FSS) and mount target from PeopleSoft Cloud Manager UI.
- Import environments from PeopleSoft environments that are running on Oracle Cloud.
- Can use Zero Downtime Migration (ZDM) to migrate database and middle tier into Cloud Manager.
- Multiple PeopleSoft Client environments are supported.
- Windows middle tier with Process Scheduler to support nVision.
- Database systems support multiple Oracle Database versions.
- Database systems support Exadata shapes.
- Stop and start environment in OCI from Cloud Manager. Customer is not billed for an environment while it is stopped.

- Ability to backup an environment and restore an environment from the backup from Cloud Manager UI.
- Share PS_HOME, PS_APP_HOME and PS_CUST_HOME in multiple middle tiers using File System Service.
- Ability to resume provisioning when a recoverable failure occurs.

Chapter 2

Configuring Cloud Manager

Configuring Cloud Manager

Installation documentation for OCI is posted on the PeopleSoft Cloud Manager Home Page (My Oracle Support DOC ID: 2231255.2), Installation and Implementation tab. PeopleSoft Cloud Manager Home Page

Pages Used to Configure Cloud Manager for OCI

Page Name	*Definition Name*	*Usage*
Cloud Manager Settings Tile	ECL_CMCONFG_FL_GBL (CREF for the tile)	To access the Cloud Manager Settings page.
Cloud Manager Settings page	ECL_CMCFG_OCI_FL	To change the system settings as per requirements in OCI.
Infrastructure Settings page	ECL_OCICFG_OCI_FL	To configure OCI-related settings for environment provisioning and management.
File Server Configuration page	ECL_CMFILESERV_FL	To configure file server as repository for Cloud Manager in OCI.
Manage PUM Connections	ECL_CMUPDATE_FL	To configure a PUM sources for updating the Cloud Manager application.
Manage Updates	ECL_CMSELFUPD_FL	To mange application updates delivered through PeopleSoft IH Updates and PRPs in OCI.
Logs	ECL_CM_FSLOGS_FL	To view Cloud Manager logs.

Cloud Manager Settings Tile

Use the Cloud Manager Settings tile (ECL_CMCONFG_FL_GBL) to access the Cloud Manager Settings page.

Note: Only a Cloud Manager Administrator can view this tile on the Cloud Manager home page.

Navigation

The Cloud Manager Settings tile is delivered as part of the Cloud Manager home page.

Image: Cloud Manager Settings Tile

This example illustrates the Cloud Manager Settings tile.

Configuring Cloud Manager Settings for OCI

Configuring Cloud Manager

The steps involved in Cloud Manager Configuration for OCI are:

- Configuring Cloud Manager settings.
- Configuring Infrastructure settings.
- Configuring File Server.
- Managing Updates.

Cloud Manager Settings Page

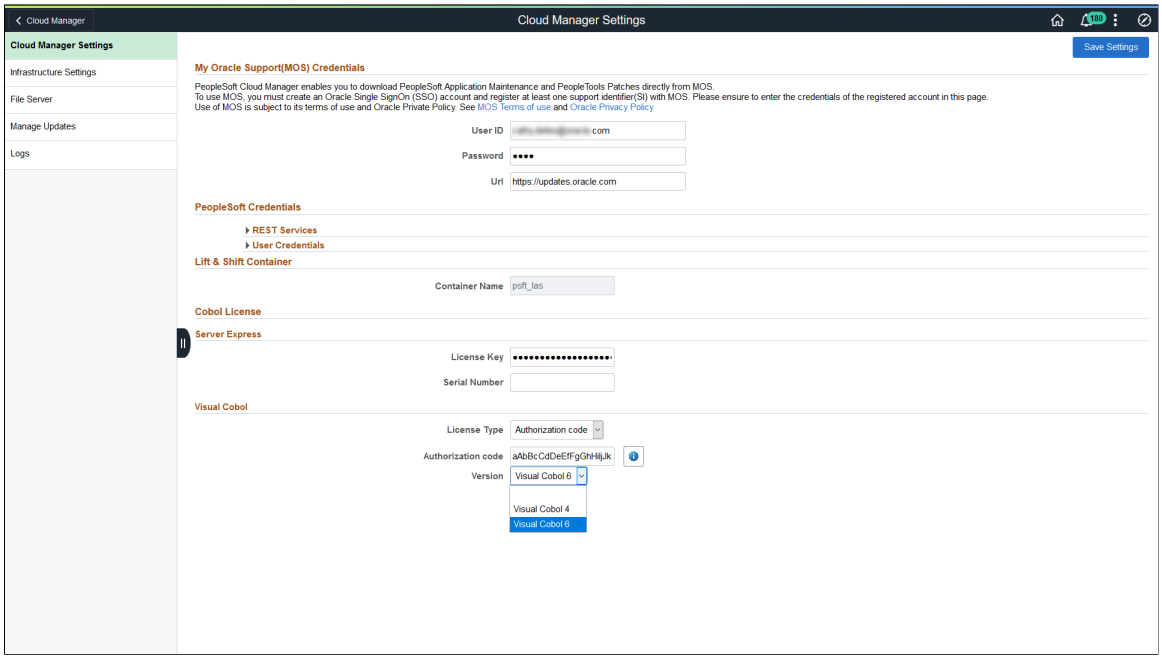
Use the Cloud Manager Settings page (ECL_CMCFG_OCI_FL) to change the system settings as per requirements.

Navigation

Click the Cloud Manager Settings tile on the delivered Cloud Manager Fluid home page. Cloud Manager Settings page is displayed. By default, the details that were provided during Cloud Manager bootstrap process are displayed.

Image: Cloud Manager Settings page

This example illustrates the fields and controls on the Cloud Manager Settings page. You can find definitions for the fields and controls later on this page.



My Oracle Support (MOS) Credentials

This refers to My Oracle Support (MOS) username and password inputs. Using this credential, Cloud Manager downloads the required updates, PIs and PRPs from MOS. The MOS credentials were provided through the Resource Manager Stack.

User ID Enter the user ID for your My Oracle Support account.

URL Enter the URL: https://updates.oracle.com.

Password Enter the password for your My Oracle Support account.

Note: Read the MOS License information. Click the links to understand My Oracle Support terms of use and privacy policy.

PeopleSoft Credentials for REST Services

REST services are standard IB REST services available in the Cloud Manager instance. These REST services are used internally by Cloud Manager modules to send/receive the results of long-running, asynchronous activities.

Important! User credentials must be manually updated on the Cloud Manager instance before updating here. Updating credentials here does not update the Cloud Manager instance.

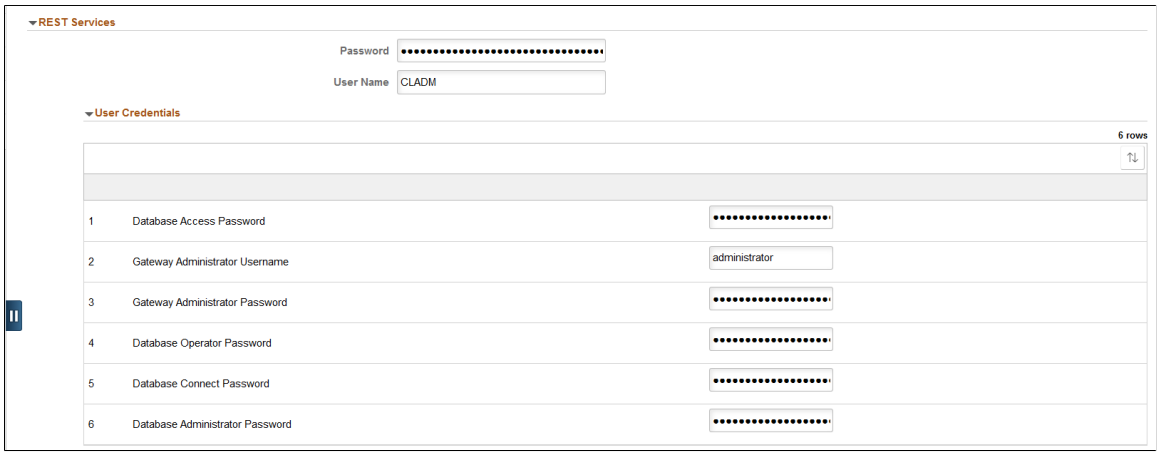
User Name Enter the delivered Cloud Manager Administrator user name.

Password Enter the Cloud Manager Administrator password.

Expand the User Credentials section and enter all the necessary passwords.

Image: REST Services - User Credentials

This example illustrates the fields for REST Services - User Credentials.



Lift and Shift Container

This section refers to the Oracle Cloud Storage Container name in which the lifted DPKs (Lifted DPK means migrated environment from your on premise environment through Lift process) are stored. It is from this container that the list of lifted environments are displayed on the Lift and Shift page.

Container Name Displays the container name. In the current version of Cloud Manager this name cannot be changed.

COBOL License

The Consolidated COBOL DPK contains both Server Express and Visual COBOL. The Consolidated COBOL DPK is included in the PeopleTools DPKs starting with PeopleTools 8.56.16 and PeopleTools 8.57.06. Visual COBOL is only supported for PeopleTools patches that include the Consolidated COBOL DPK.

Starting with PeopleTools 8.58 Visual COBOL is the only supported microfocus compilier.

Use this section to provide COBOL license details. COBOL installation is enabled on the topology by selecting COBOL field value as *Yes* in the Features section of Edit Node modal window. For details on topology, see Enabling Topology with Cobol Feature as Yes. To enable COBOL in the template, the topology for the template must have COBOL enabled. See Configuring Custom Attributes

---

Note: Oracle is the exclusive reseller of the Micro Focus COBOL compiler for use with PeopleSoft applications. Contact your Oracle sales representative for a license.

Server Express

Serial Number Enter your COBOL serial number. For example, PEOPLESOFT-XXXXXX.

License Key Enter your COBOL license key. For example, 010xx xxxxx xxxxx xxxxx xxxx xLA.

Visual Cobol

License Type License Type can be:

- Authorization Code
- File
- Server

License The license depends on the license type:

- Authorization Code

  Enter the authorization code.

- File

  The license file must be copied to the Cloud Manager VM and placed in a location that is accessible to psadm2 user. Enter the path to the license file.

- Server

  Enter the hostname or IP address of the license server. The server must be accessible from the current machine.

Version Select the COBOL version. Visual COBOL 4 and Visual COBOL 6 are supported.

Infrastructure Settings Page

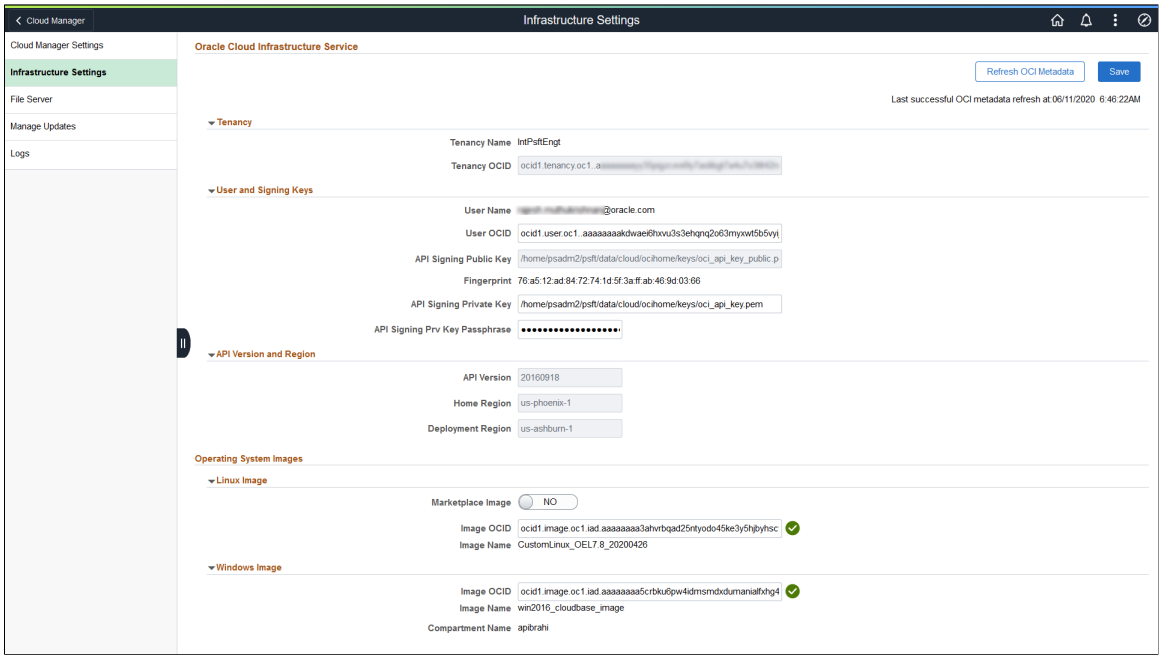
Use Cloud Manager Settings – Infrastructure Settings page (ECL_OCICFG_OCI_FL) to configure OCI related settings for instance provisioning and management.

Navigation

Click the Cloud Manager Settings tile on the delivered Cloud Manager Fluid home page. Cloud Manager Settings page is displayed. On the Cloud Manager Settings page, click the Infrastructure Settings link displayed on the left panel.

Image: Infrastructure Settings page

This example illustrates the fields and controls on the Infrastructure Settings page. You can find definitions for the fields and controls later on this page.



Tenancy OCID

Unique Oracle Cloud Identifier (OCID) for the tenancy. Tenancy is the root compartment that contains all your organization's compartment and other OCI Cloud resources.

If you use the Oracle Cloud Infrastructure API, you will need your tenancy's OCID in order to sign the API requests. You will also use the tenancy ID in some of the IAM API operations. You can find your tenancy's OCID displayed at the bottom of the Oracle Cloud Infrastructure Console pages.

See Locating OCI Credentials.

User OCID

Unique OCID for the user. You can find the user's OCID in the Oracle Cloud Infrastructure Console page showing the user's details.

See Locating OCI Credentials.

API Signing Public Key and **API Signing Private Key**

RSA key pair in PEM format.

Your API requests will be signed with your private key, and Oracle Cloud Infrastructure will use the public key to verify the authenticity of the request.

Note: For details on the creation and usage of the API signing keys, refer the *PeopleSoft Cloud Manager Installation Guide*.

	Important! It is not recommended to modify these values without completely understanding the impact. If in case the public keys are required to be changed, then manually update the public keys for the user using the OCI Console.
API Signing Prv Key Passphrase	Displays the API signing private key encrypted with a passphrase.
API Version	API version is the Rest API version for OCI. The base path of the endpoint includes the desired API version (for example, 20160918).
Home Region	When you sign up for Oracle Cloud Infrastructure, Oracle creates a tenancy for you in one region. This is your home region. Your home region is where your IAM resources are defined. When you subscribe to a new region, your IAM resources are replicated in the new region, however, the master definitions reside in your home region and can only be changed there.
Deployment Region	The region where the PeopleSoft environments will be provisioned by Cloud Manager. Cloud Manager and the file server instance also reside on this same region.
Save	Click the Save button to save your settings.
Refresh OCI Metadata	Once all the Infrastructure settings are entered and saved, click the Refresh OCI Metadata button. When this button is clicked, the Cloud Manager will run a process scheduler job (Process Name: ECL_OCI_SYNC) which will fetch all the OCI-specific metadata required for the Cloud Manager to function properly.

Operating System Image

This refers to OS images in Oracle Cloud that CM uses to provision VMs during environment creation. For details on how windows image gets the path from Oracle Cloud console, refer the *PeopleSoft Cloud Manager Installation Guide*.

For Linux Image, you can either:

- Obtain the Oracle Linux Image customized for PeopleSoft from Marketplace.

  See tutorial *Prepare to Install PeopleSoft Cloud Manager*.

- Create a custom Linux Image for PeopleSoft Cloud Manager.

  See tutorial *Create a Custom Linux Image for PeopleSoft Cloud Manager*.

For Windows Image, you can either:

- Use an Oracle platform image for Microsoft Windows for PeopleSoft Cloud Manager.

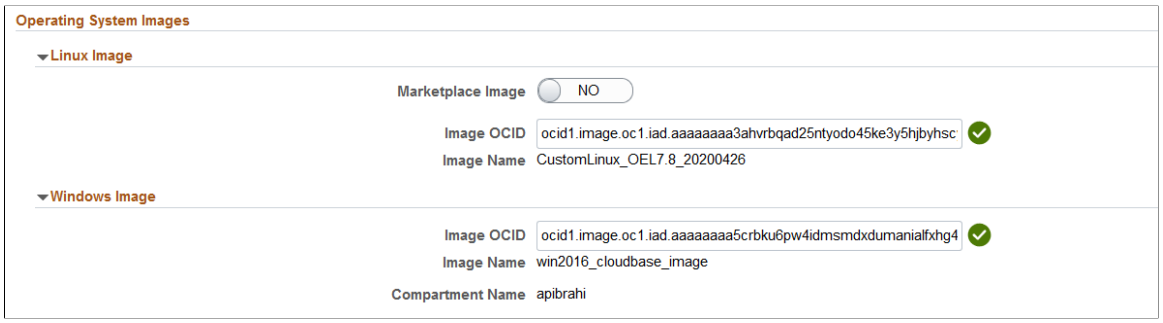
  See tutorial *Prepare to Install PeopleSoft Cloud Manager*.

- Create a custom Windows image for PeopleSoft Cloud Manager in Oracle Cloud Infrastructure.

  See tutorial *Create a Custom Windows Image for PeopleSoft Cloud Manager in Oracle Cloud Infrastructure*.

Image: Operating System Image

This example illustrates the fields and controls on the Operating System Image. You can find definitions for the fields and controls later on this page.



To access the OCID for the Oracle Linux Image and the Windows Image:

1. Sign on to the OCI Console.
2. Select Compute, Custom Images.
3. Select the image (Oracle Linux or Windows).
4. In the details, click the Copy link for the OCID.
5. Paste the OCID in the appropriate Operating System Image.

Linux Image **Image OCID**	Select whether or not the Linux Image was obtained from Marketplace. Enter the OCID for the Linux Image. The image name will be displayed.
Windows Image **Image OCID**	Enter the OCID for the Windows Image. The image name will be displayed.

File Server Page

Use Cloud Manager Settings – File Server page (ECL_CMFILESERV_FL) to configure file server as repository for Cloud Manager.

Use the Cloud Manager File Server page to select or configure a File Storage Service (FSS) file system. If you are upgrading to Image 10, FSS will replace the existing Linux File Server and the contents will be migrated automatically.

See tutorial *Use File Storage Service for PeopleSoft Cloud Manager Repository*.

The following use cases apply while creating the file server:

- Create a new file server with new Mount Target
- Create file system and export with existing Mount Target
- Use existing file system (Mount Target and Export Path)
- Upgrade existing file server to FSS in upgrade environment

The following ports need to be opened in the FSS mount target's subnet to allow NFS connections:

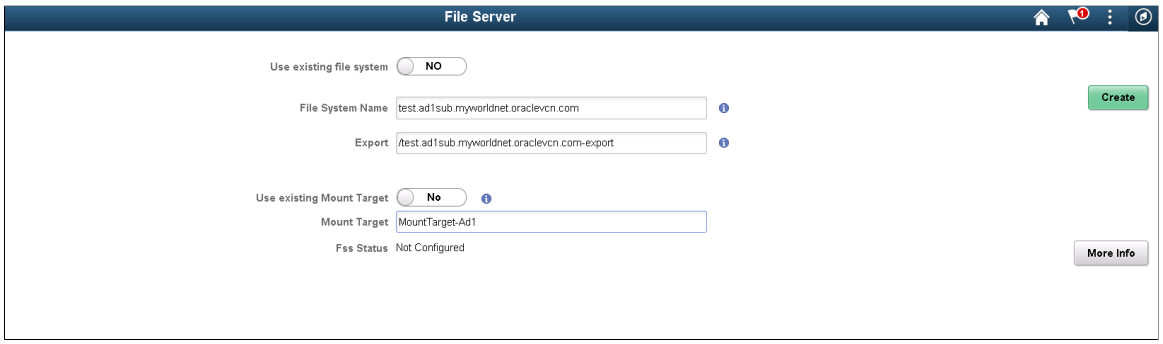
TCP Ports	111
	2048
	2049
	2050
UDP Ports	111
	2048

Navigation

Click the Cloud Manager Settings tile on the Cloud Manager home page. On the Cloud Manager Settings page, click the File Server link displayed on the left panel.

Image: File Server page

This example illustrates the fields and controls on the File Server page. You can find definitions for the fields and controls later on this page.



The File Server settings provides the options to set up a new file system.

By default, options *Use existing file system* and *Use existing Mount Target* are set to No.

Use exiting file system	Set to No when creating a new file system.
File System Name	Name for the file system to be created.
Export Path	Path for instances to mount the file system through mount target.

Use existing Mount Target	Set to No when creating a new file system.
Mount Target	IP address or DNS name that is used in the mount command to connect NFS clients to a file system. A single mount target can export many file systems. By default, you can create two mount targets per account per availability domain.
Create button	Once the inputs are provided, Click the Create button to create the file system, mount target and export path.

Creating a New File System, Mount Target and Export

To create a new File system, mount target and export:

1. Enter the File System Name.
2. Enter the Export Path.
3. Enter the Mount Target.
4. Select No for Use existing file system.
5. Select No for Use existing Mount Target.
6. Click Create.

When the file system becomes available, you can subscribe to your desired download channels in the repository.

Creating New File System and Export with Existing Mount Target

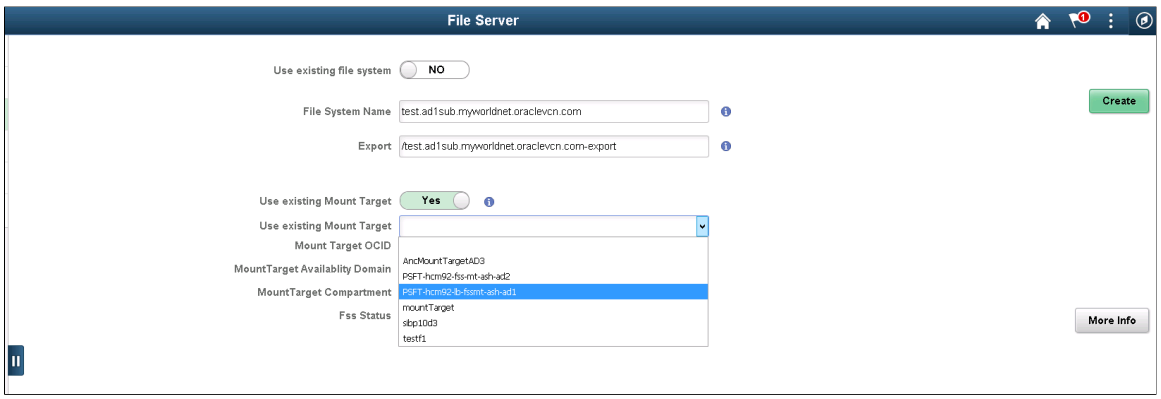
As a mount target can export many file systems, a new File System can be created using an existing Mount Target.

To create a new file system and export with existing mount:

1. Select Infrastructure Settings from the left-side menu and click the Refresh OCI Metadata button.
2. Select File Server from the left-side menu.
3. Select Yes to use existing Mount Target.
4. Select the exiting Mount Target from the drop-down list.
5. Click Create.

Image: Creating New File System and Export with Existing Mount Target

This example illustrates the fields and controls on the File Server page for creating new file system and export with existing Mount Target.



The existing mount is selected from Compartment->Availability Domain->Mount Target.

Using Existing File System

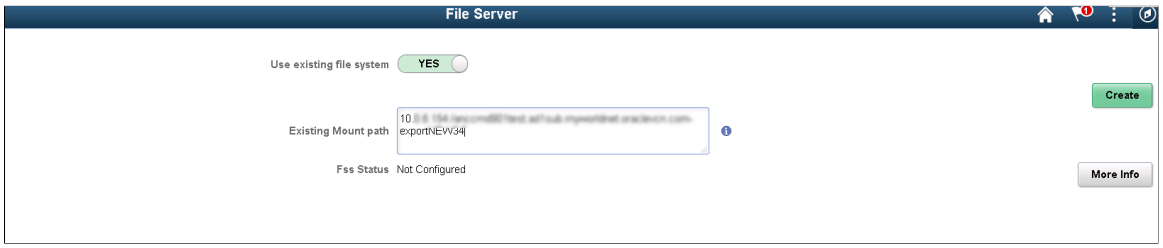
Instead of creating a new file system, an existing file system can be used. Select Use existing file system and enter the export path for the target FSS.

To create a file server from an existing file system:

1. Select Yes to Use existing file system.
2. Enter the Existing Mount path.
3. Click Create.

Image: Using Existing File System

This example illustrates the fields and controls on the File Server page for using existing file system.



Upgrading Existing File Server to FSS in Upgrade Environment

Once Cloud Manager is upgraded to Cloud Manager Image 10, the contents in the existing block volumes based file server need to be migrated to the newly created file systems.

The following actions will not be available until the migration is complete:

- Environment page will not be available.
- Use will not be able to subscribe to new channels.

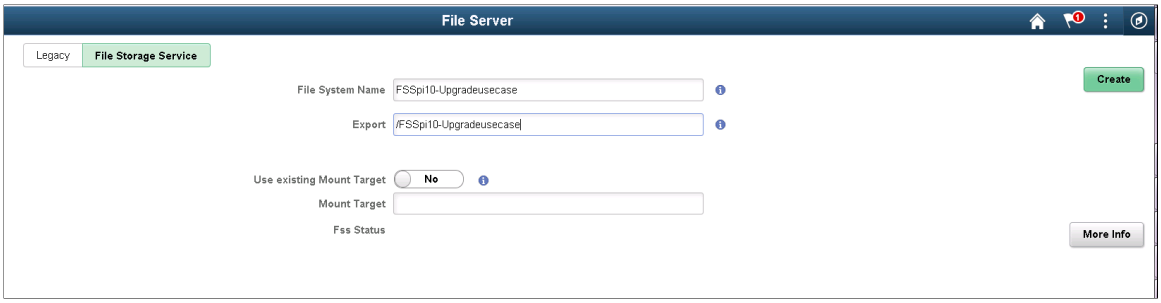
- Shift is not allowed.

There are two options for migrating the old File Server.

- Create a new FSS with new mount target.

  Image: Create FSS with new mount target

  This example illustrates the fields and controls on the File Server page for creating a FSS with new mount target.

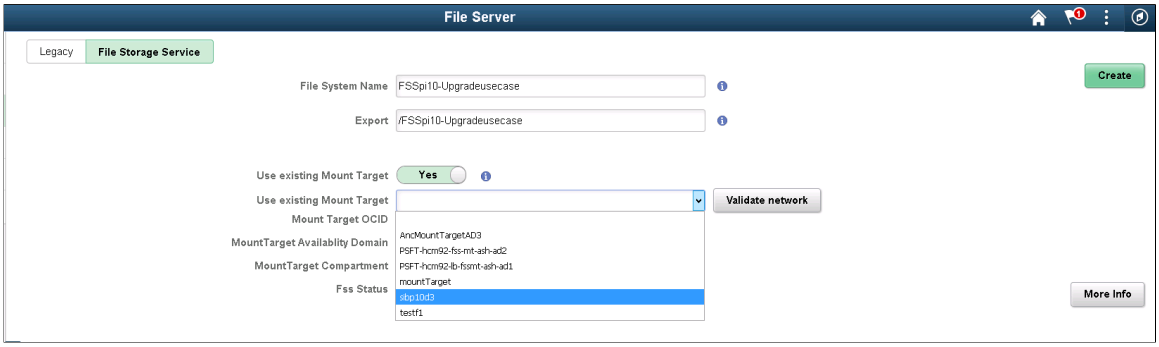


  Enter the File System Name and Export path, then click Create.

- Create FSS using an existing mount target.

  Image: Create FSS using an existing mount target

  This example illustrates the fields and controls on the File Server page for creating a FSS using an existing mount target.

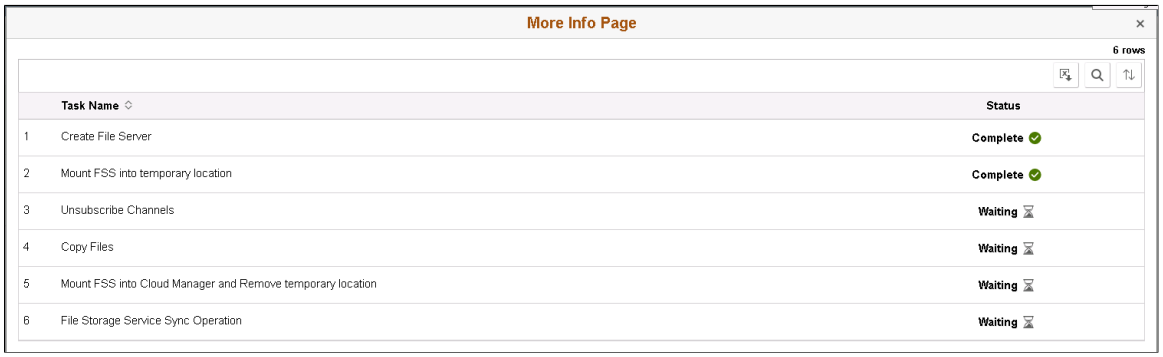


  Select Yes to use Existing Mount Target and select the Mount Target, then click Create.

Once FSS is created Cloud Manager automatically starts the migration process. The progress of the migration can be shown by clicking the More Info button.

Image: More Info- Progress of Migration

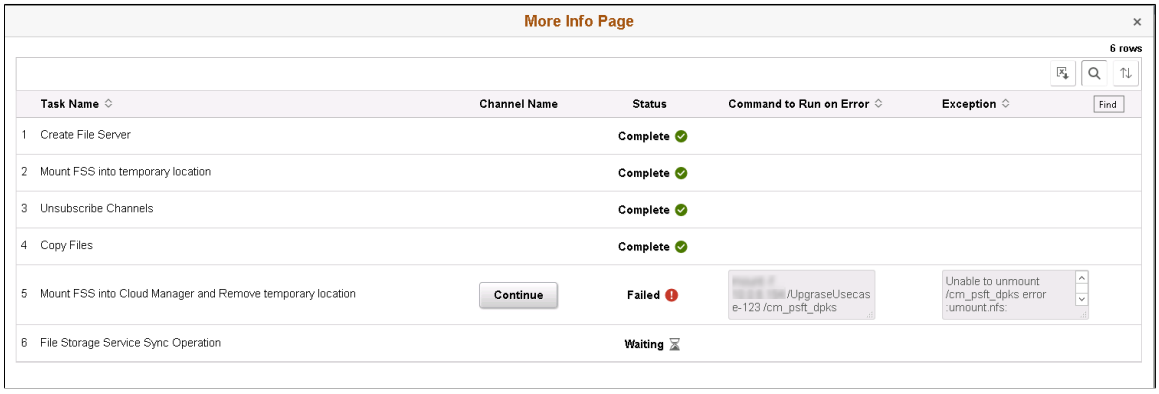
This example illustrates the fields and controls on the More Info - progress of migration.



If a step fails, the error will be displayed. Once the error is corrected, use the Continue button to resume the migration process.

Image: Failed step in FSS migration

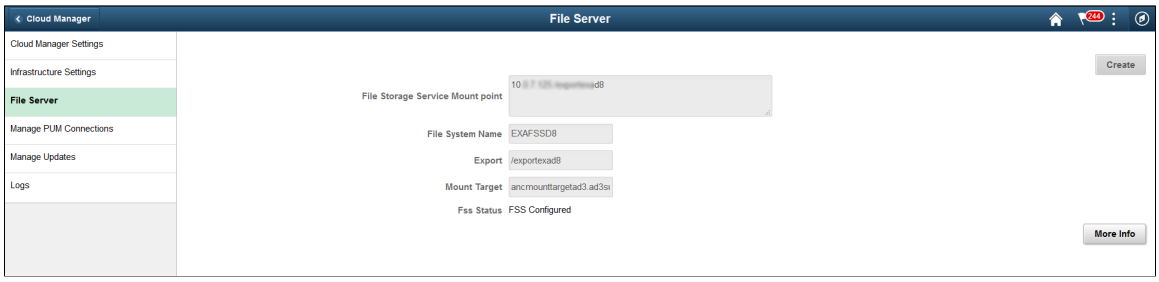
This example illustrates the fields and controls on the More Info page for a failed step.



Completed FSS

Image: Completed File Server page

This example illustrates the fields and controls on the Completed File Server page.



File Storage Service Mount Point IP address or DNS name that is used in the mount command to connect NFS clients to a file system.

File System Name Name of the File System.

Export	Export path.
Mount Target	IP address or DNS name that is used in the mount command to connect NFS clients to a file system. A single mount target can export many file systems. By default, you can create two mount targets per account per availability domain.
FSS Status	File Server status. Different statuses are: Not Configured, FSS Configured, and Failed. • Not Configured: The FSS is not created or configured to store files. • FSS Configured: FSS is created and is ready to store files. • Failed: FSS creation failed. Check the More info page to correct the errors and continue. Reset option can also be used to re-create the FSS.
More Info	Select to view the progress of the migration. More Info contains the list of tasks that can be continued or retried in case of a failure or error.

Manage Updates Page

Use the Manage Updates page to apply Cloud Manager updates delivered through PeopleSoft IH Updates and PRPs.

Note: This feature is meant for the Cloud Manager application update only.

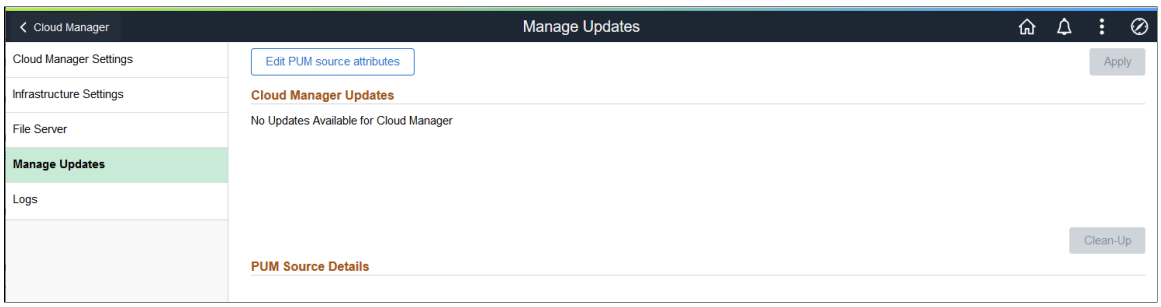
Navigation

Click the Cloud Manager Settings tile on the delivered Cloud Manager Fluid home page. The Cloud Manager Settings page is displayed. On the Cloud Manager Settings page, click the Manage Updates link displayed on the left panel.

For information on updating Cloud Manager see Updating Cloud Manager Overview.

Image: Manage Updates page

This example illustrates the fields and controls on the Manage Updates page when no updates are available.



Configuring My Settings

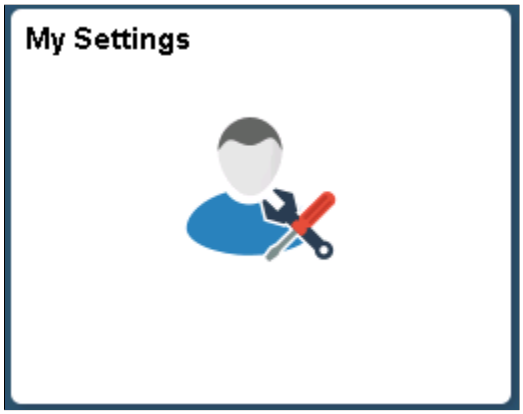
Use the My Settings tile (ECL_INFO_HOME_FL_GBL) to access My Settings page.

Navigation

My Settings tile is delivered as part of the Cloud Manager home page.

Image: My Settings tile

This example illustrates the My Settings tile.



My Settings Page

Use the My Settings page (ECL_INFO_HOME_FL) to enter or edit the public SSH key. The SSH key provided here can be used to input user's own SSH keys or any administrators SSH keys to help manage or troubleshoot issues by connecting over SSH.

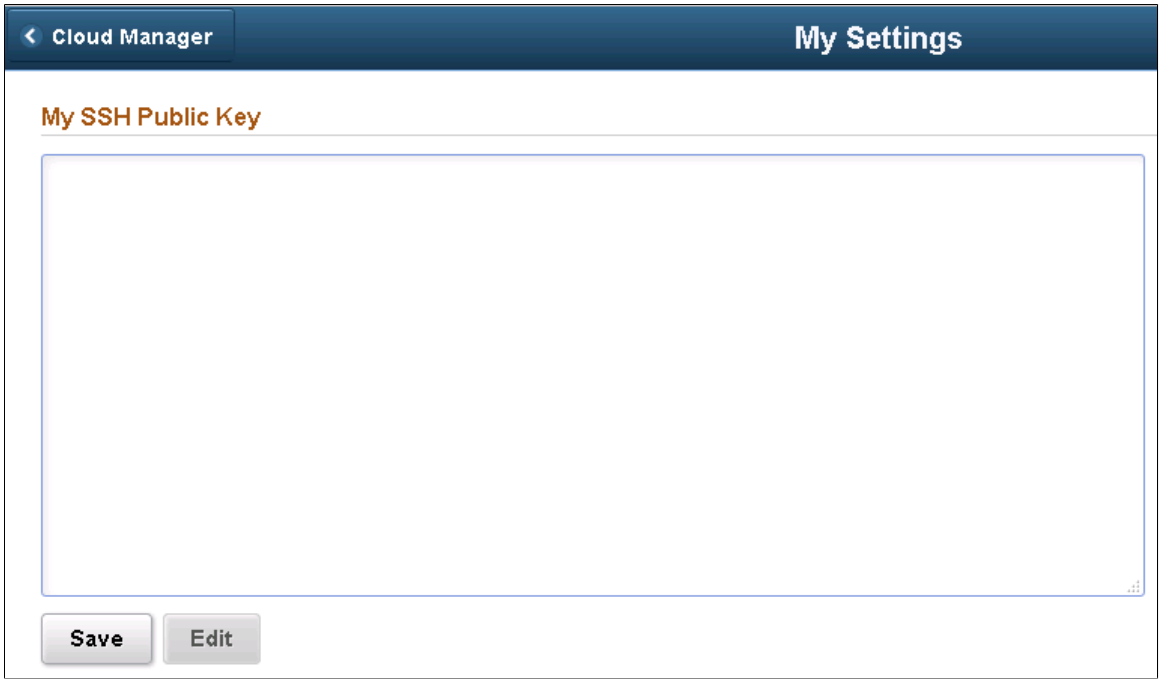
Note: The SSH key will be automatically added into all environments that will be created by the user after adding this key here.

Navigation

Click the My Settings tile on the delivered Cloud Manager Fluid home page. The My Settings page is displayed.

Image: My Settings page

This example illustrates the fields and controls on the My Settings page for the tablet.



My SSH Public Key Enter the SSH public key value.

Click Save to save the details.

Note: To edit existing key details, click the Edit button and replace the text; then click Save.

Chapter 3

Provisioning Environment In PeopleSoft Cloud Manager

Managing Repository

Cloud Manager provides an easy way to automatically download and manage PeopleSoft Application Update Images (PIs), PeopleSoft Release Patchsets (PRPs), PeopleTools Product Patches and PeopleSoft Custom Images. Cloud Manager uses the file server to store downloaded artifacts from MOS. To streamline and automate downloads of various PeopleSoft application images and PRPs, Cloud Manager has introduced the concept of Subscription Channels. Each PeopleSoft application has an associated Channel, which an administrator can choose to subscribe in order to download the latest PIs and PRPs for that particular PeopleSoft application. Cloud Manager is delivered with channels for PeopleSoft applications, which are available after you complete the installation and configuration. An administrator can subscribe to multiple channels and download all necessary PIs and PRPs.

Cloud Manager uses an application called Download Manager to download updates from MOS, which is invoked through process scheduler in asynchronous mode every time a channel is subscribed.

On the Repository tile, Administrators can:

- Subscribe to release channels for latest PeopleSoft application updates.
- Manage downloaded PeopleSoft Images and PRPs.

Pages Used to Manage Cloud Manager Repository as an Administrator

Page Name	*Definition Page*	*Usage*
Repository Tile	ECL_REPOSITORY_FL_GBL (CREF for tile)	Access the various features such as, Channel Subscriptions and Download History, and functions such as, downloading logs and deleting downloads.
My Downloads Page	ECL_REPO_AMYDLS_FL	View the PRPs and PIs downloaded. New entries are added as soon as new artifacts are downloaded.
Download Subscriptions Page	ECL_REPO_BCHNL_FL	Create download channels and subscribe them to initiate downloads. You can also use predefined download channels to initiate downloads.
Download History Page	ECL_REPO_BDLHIS_FL	View the history of downloads, such as PIs and PRPs downloaded.

Page Name	*Definition Page*	*Usage*
Logs Page	ECL_REPO_MLOG_FL	View the download manager logs.
Upload Custom Scripts Page	ECL_UPLD_CUST_SCR	Upload Custom Scripts

Repository Tile

Use the Repository tile to access the following features and functions:

- View downloaded artifacts
- Channel subscriptions
- Download history
- Download logs
- Filter and delete downloads
- Manage custom scripts

Navigation

The Repository tile (ECL_REPOSITORY_FL_GBL) is delivered as part of the Cloud Manager home page.

Image: Repository Tile

This example illustrates the Repository Tile.

My Downloads Page

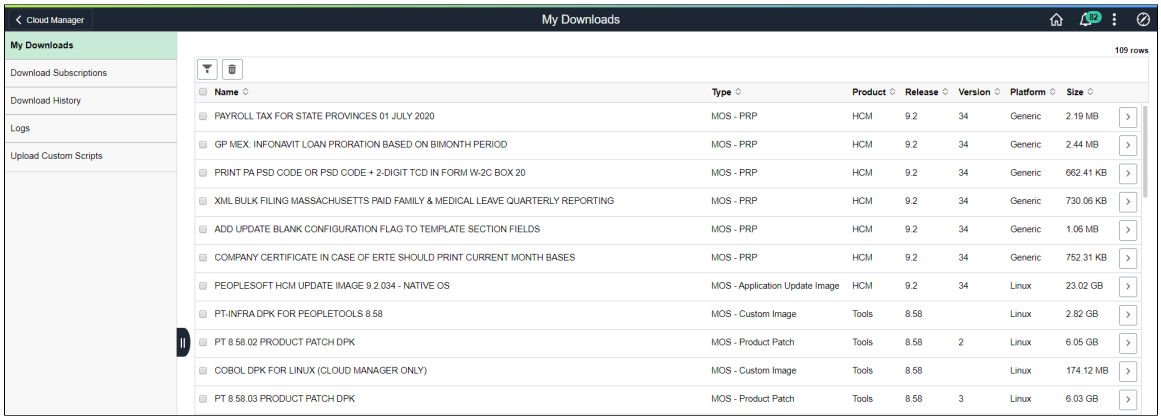
Use the My Downloads page (ECL_REPO_AMYDLS_FL) to view the artifacts downloaded. New entries are added as soon as new artifacts are downloaded.

Navigation

Click the Repository tile on the delivered Cloud Manager Fluid home page. My Downloads page is displayed by default.

Image: My Downloads page

This example illustrates the fields and controls on the My Downloads page. You can find definitions for the fields and controls later on this page.



Note: Clicking an item in the My Downloads page displays additional details of the downloaded artifact.

	Use the Filter icon to refine the search results based on search criteria.
	Use the Delete icon to delete downloaded PIs and PRPs. Select the check box corresponding to the row you want to delete, and then click Delete button.
Name	Name of the downloaded artifact.
Type	Indicates the artifact type such as PI, PRP, Custom Image, and so on.
Product	Indicates the PeopleSoft application product pillar.
Release	Indicates the PeopleSoft application release.
Version	Indicates the application PI version.
Platform	Indicates the Operating System platform, such as Linux, or Windows.
Size	Total size of the PI or PRP.

Download Subscriptions Page

Use the Download Subscriptions page (ECL_REPO_BCHNL_FL) to subscribe to download channels and initiate downloads.

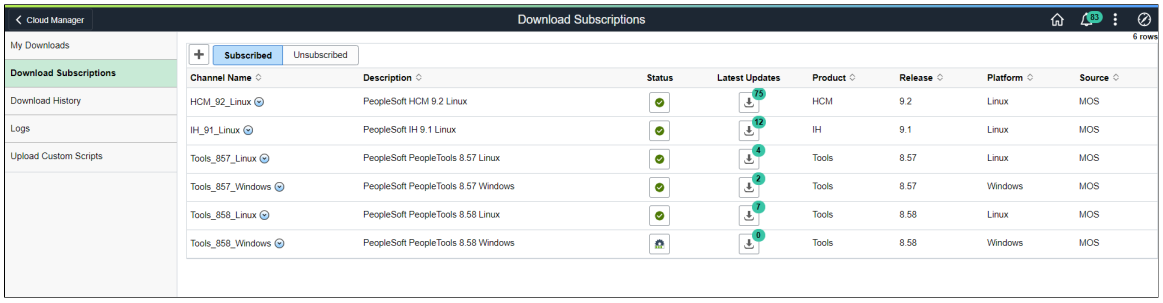
Note: Cloud Manager delivers default channels and those channels are available in the unsubscribed list of the Download Subscriptions page.

Navigation

Click the Repository tile on the delivered Cloud Manager Fluid home page. Select the Download Subscriptions tab in the left panel of the Cloud Manager home page.

Image: Download Subscriptions page

This example illustrates the fields and controls on the Download Subscriptions page. You can find definitions for the fields and controls later on this page.



To subscribe or unsubscribe channel, click the Related Actions button corresponding to the channel name. If you select the Subscribe option, Cloud Manager starts monitoring for any new PIs or PRPs and downloads them from My Oracle Support. If you select the Unsubscribe option, Cloud Manager will no longer monitor or download latest PIs or PRPs.

When a release channel is subscribed, Cloud Manager invokes the download manager application, which connects to MOS and downloads latest updates for the release channel. Please note that artifacts, such as Update Images, are large in size and can take a few hours to download. User can view the status of active downloads from the Download History page.

Subscribed tab

Click this tab to view a list of subscribed channels.

When you select the Related Action to subscribe to a channel, that channel will be added to the Subscribed tab.

Note: This operation will renew the channel subscriptions for all channels present in the Subscribed tab. This means that Cloud Manager will check for updates and download them for all channels present in the Subscribed tab.

Unsubscribed tab

Click this tab to view a list of unsubscribed channels. By default, newly created download channels are listed under the Unsubscribed tab.

Status

Status will indicate current state.

- Success

The Success icon indicates the download was successful. No further action is necessary.

- In-progress

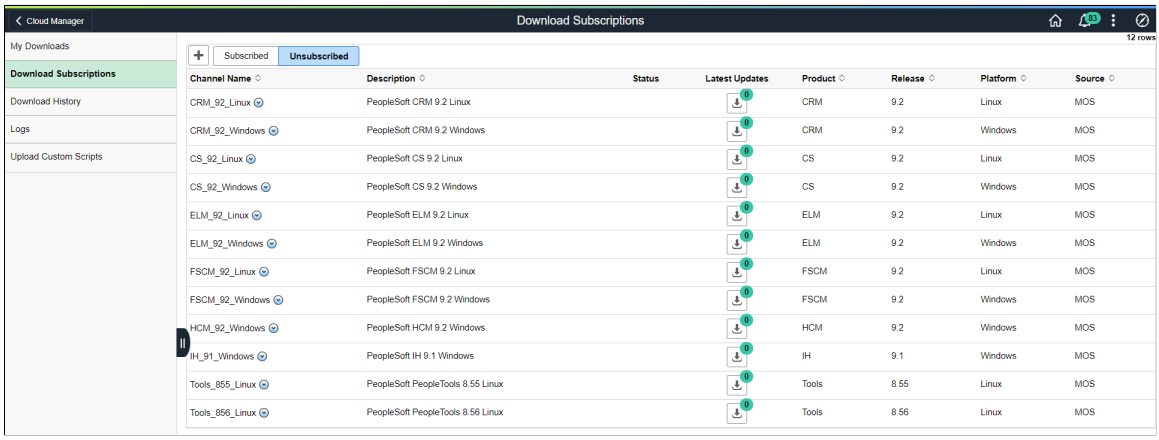
The In-progress icon indicates the update is downloading. Click on the icon to view the status of the download.

- Error

The Error icon indicates the download failures. Click the icon to open the Download Error page.

Image: Download Subscriptions – Unsubscribed page

This example illustrates the fields and controls on the Download Subscriptions – Unsubscribed page. You can find definitions for the fields and controls later on this page.



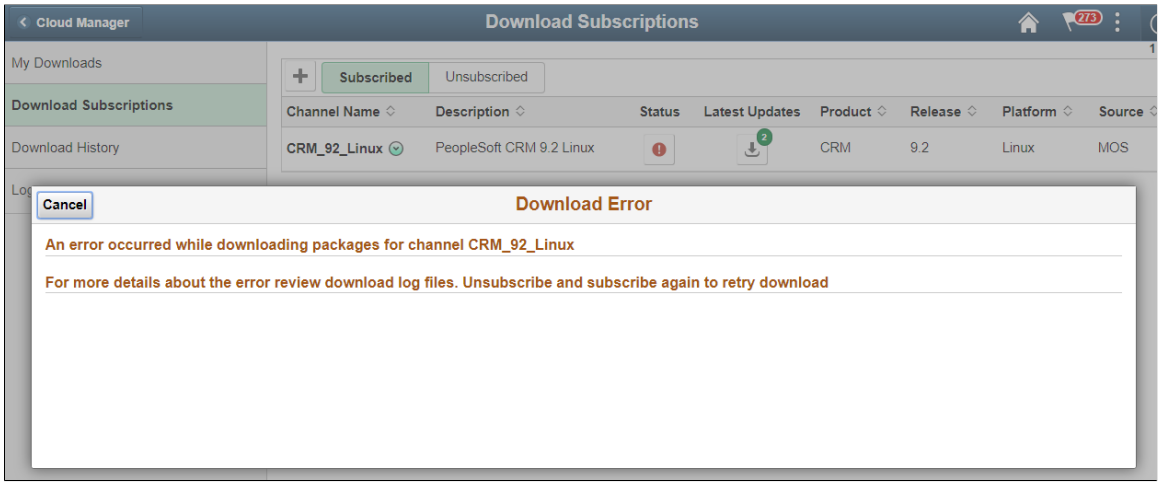
Use the action button to subscribe to a channel.

Download Error Page

Click the failed icon on the Download page to view the Download Error popup page. There are two types of error popup pages, one for standard errors and another for invalid password. The invalid password popup only applies to password protected downloads.

Image: Download Error page

This example illustrates the fields and controls on the Download Error page. You can find definitions for the fields and controls later on this page.



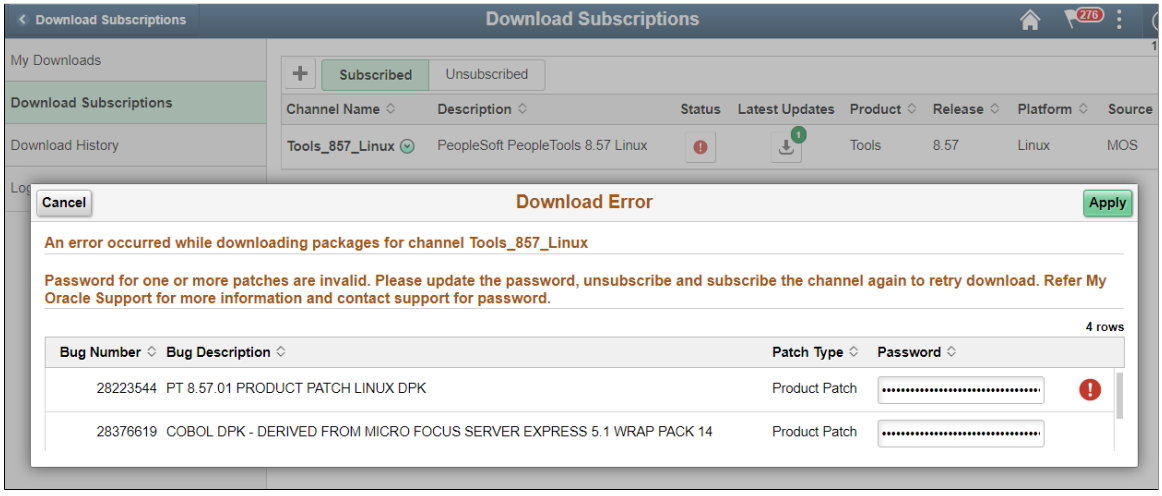
The download error message will indicate the error and direct the user to review the download log files. Error could be due to issues occurring during the download, such as network connection disruption (unable to reach MOS) or if there is no space available on the file server to save downloads.

Password Protected Subscription Password Error

When you subscribe to the a password protected download channel, the DownloadAssist file is downloaded from MOS to Cloud Manager. The DownloadAssist file contains the password required to download the packages.

Image: Download Error for Password Error

This example illustrates a Download Error page displaying a password error.



This message will only appear if Cloud Manager is unable to retrieve the password due to an error in MOS. If this does occur, the user will need to request the password from Support and update it manually on this page.

If the issue is due to an expired password, user can do a unsubscribe to the channel and then re-subscribe to the channel. Any password changes will be updated in the DownloadAssist file that is posted in MOS. On re-subscribing to a channel, the new password should get automatically updated in Cloud Manager.

If a re-subscribing doesn't solve the problem, then there could be issues in Cloud Manager that is failing to retrieve and update the password automatically or an unforeseen issue in MOS which is not allowing the download of the DownloadAssist file. In such a scenario, the user is expected to get the password from support and update the same on the Download Error page.

Note: The next scheduled download will renew the subscription and include any password changes in the DownloadAssist file. See Changing Download Interval

---

Downloading PeopleTools Patches

Cloud Manager can download previous PeopleTools patch releases for the PeopleTools channel. But for Application channels, only latest patches get downloaded.

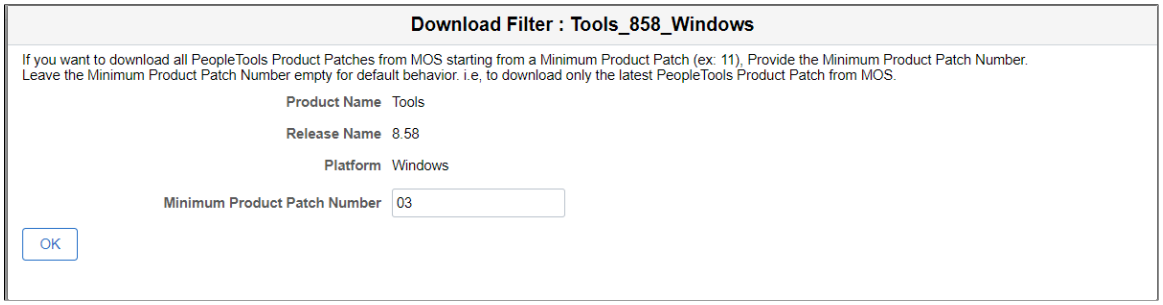
In case of Tools channel subscription, you are presented with a modal window for selecting the patch version you want to download.

Navigation

Click the Unsubscribed tab. Select any Tools channel. Click the Related Options menu and select Subscribe.

Image: Download Filter Modal Window

This example illustrates the fields and controls in Download Filter modal window.



Enter the required product patch version in the Minimum Product Patch Number field. For example, if user enters 11 in this field, then CM will download tools patches 8.55.11, 8.55.12, 8.55.13 up to the latest.

Download History Page

Use the Download History page (ECL_REPO_BDLHIS_FL) to view the history of downloads.

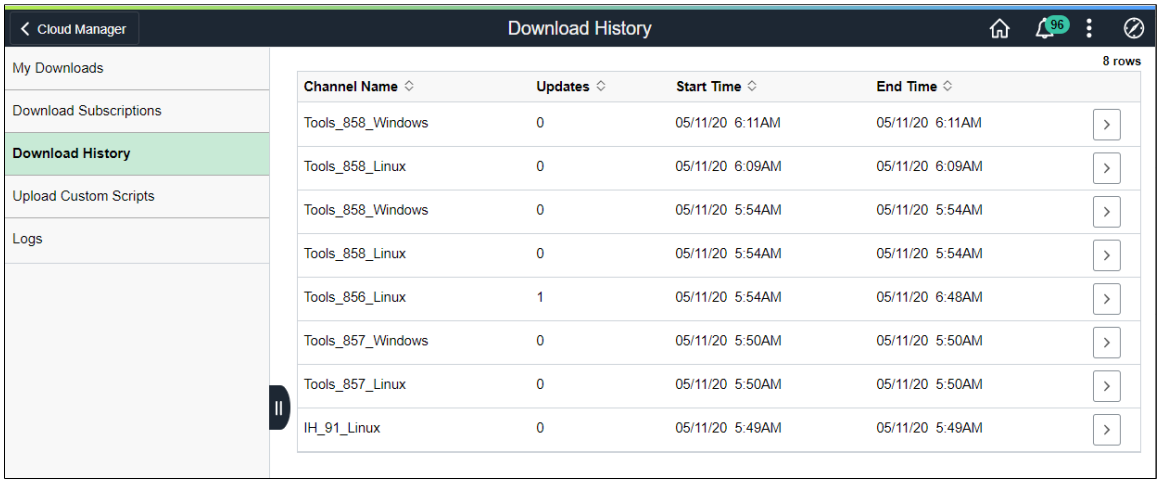
Note: The entries in Download History page are updated based on the download interval. Clicking an entry in the Download History page displays the current state of the download channel (that is, a list of files already downloaded, another list of files in the download queue and those that are currently downloading).

Navigation

Click the Repository tile on the delivered Cloud Manager Fluid home page. Select the Download History tab in the left panel of the Cloud Manager home page.

Image: Download History page

This example illustrates the fields and controls on the Download History page. You can find definitions for the fields and controls later on this page.



Channel Name Name of the download channel.

Updates Number of updates downloaded.

Start Time and **End Time** Indicates the time when downloads are started/finished for the release channel.

Logs Page

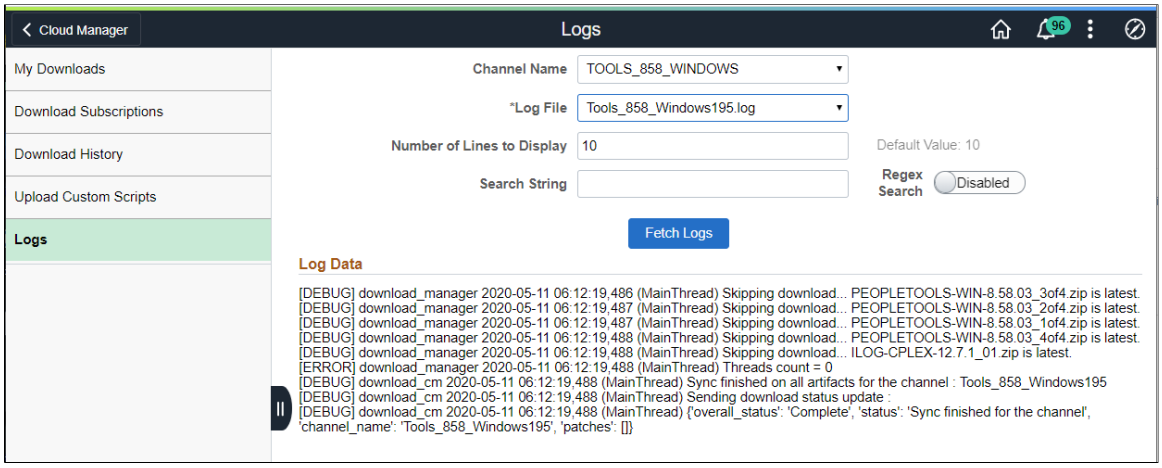
Use the Logs page (ECL_REPO_MLOG_FL) to view the download logs corresponding to the subscribed channels. It displays download logs for all the files that get downloaded.

Navigation

Click the Repository tile on the delivered Cloud Manager Fluid home page. Select the Logs tab in the left panel of the Cloud Manager home page.

Image: Logs page

This example illustrates the fields and controls on the Logs page. You can find definitions for the fields and controls later on this page.



Channel Name	Name of the subscribed channel.
Log File	Log files are generated when a channel is subscribed. Select an appropriate log file in this field.
Number of Lines to Display	Indicates how many lines of the selected log file to be displayed.
Search String	Used to search for specific keywords in the log file. When user inputs a keyword, such as "ERROR" as an example, then only those lines are displayed which has an Error string in it. Here, only the specified number of lines are displayed.
Regex Search	Enables advanced searching, where a user can provide Unix style regular expressions.
Fetch Logs button	Click this button to fetch log data based on the input provided by the user in the Logs page.
Log Data	Data from the logs.

Re-synchronizing Repository Data with Downloaded List

Sometimes even after subscribing to a channel, you may not able to see some of the downloaded patches in Repository > My Downloads page. The logs may show that the downloads are being skipped. This indicates a situation where the patches are already downloaded but their metadata is not synced with Cloud Manager. In such situations re-sync the downloaded patches metadata with Cloud Manager using the following steps.

1. Go to Repository > Download Subscriptions page and unsubscribe all channels that are currently subscribed.
2. Navigate to PeopleTools > Process Scheduler > System Requests page and run the process "ECL_REPODM".

3. Once the process finishes execution, you should be able to see the missing patches in Repository > My Downloads page.

Subscribing Channels using the Cloud Manager Repository

This section details the process flow for subscribing to channels using the Cloud Manager Repository.

Note: Cloud Manager has a process scheduler recurring job defined, which invokes the download manager for all the subscribed release channels once a week. This will make sure that latest updates for all the subscribed release channels are downloaded every week without any user interaction.

Prerequisites

The administrator needs to define My Oracle Support credentials prior to subscribing channels using the Cloud Manager Repository. For this, perform the following:

1. Select the Cloud Manager Settings tile.
2. Edit the value in the User ID field and My Oracle Support password field in the My Oracle Support (MOS) Credentials section.
3. Click Save Settings to save the details.
   For details on the Cloud Manager settings, see Cloud Manager Settings Page.

Note: This is a one-time setup.

Perform the following steps to subscribe to channels using the Cloud Manager Repository tile:

1. Click the Repository home page available on the Cloud Manager home page.
2. Select Download Subscriptions on the left panel. The Download Subscriptions page is displayed.
3. Click Unsubscribed.
4. To subscribe to the release channel, perform the following:
   a. Click the Related Actions button corresponding to the channel name.
   b. Select Subscribe action. If there are any new updates, then the system starts downloading the new updates.

Changing Download Interval

By default, Cloud Manager polls My Oracle Support for new updates every week. The recurrence definition for download channel subscriptions is **CloudManager Repository Update**. To modify the download schedule to meet your organizational needs, modify the recurrence pattern to a pattern that meets your needs.

For example, if you want to poll for updates on alternate days, you would perform the following:

1. In Cloud Manager, navigate to PeopleTools, Process Scheduler, Recurrences.
2. Select the recurrence CloudManager Repository Update.

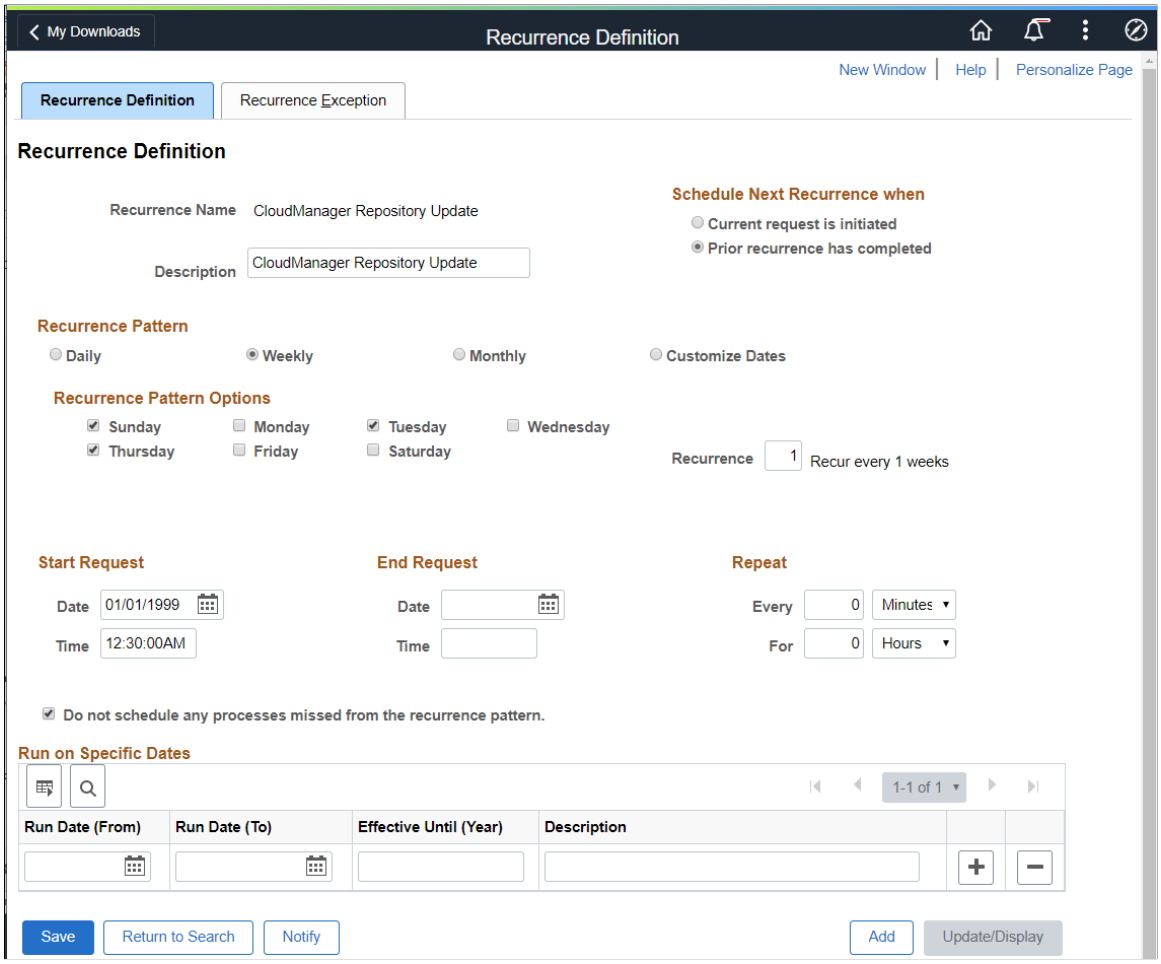
3. Select Recurrence Pattern to *Weekly*.
4. Select the alternating days as in Monday, Wednesday, and Friday or Sunday, Tuesday, Thursday.

   Note: It is recommended to select alternate days.

5. Save the page.

Image: Recurrence Definition – CloudManager Repository Update

This example illustrates the fields and controls on the Recurrence Definition – Cloud Manager Repository Update where the occurrence is set to alternate days.



For more information on setting up recurring schedules, see Product documentation for *PeopleTools : Process Scheduler,* “Defining PeopleSoft Process Scheduler Support Information”, Defining Recurrence Definitions.

Upload Custom Scripts Page

Starting with Cloud Manager Image 8 custom scripts can be run before or after provisioning a PeopleSoft environment.

Note: After a PeopleTools upgrade, you must edit the webserver property (configuration.properties) file to add or modify the HttpRepositoryPath as shown here: `HttpRepositoryPath=/opt/oracle/psft/customscripts`

This table lists the script types and which tiers they can run on.

Script Type	***Where you can run the script***
Python	Full Tier Middle Tier Database Tier PeopleSoft Client ELK Stack Database as a service (DBaaS)
Shell	Full Tier Middle Tier Database Tier ELK Stack Database as a service (DBaaS)
Batch	PeopleSoft Client

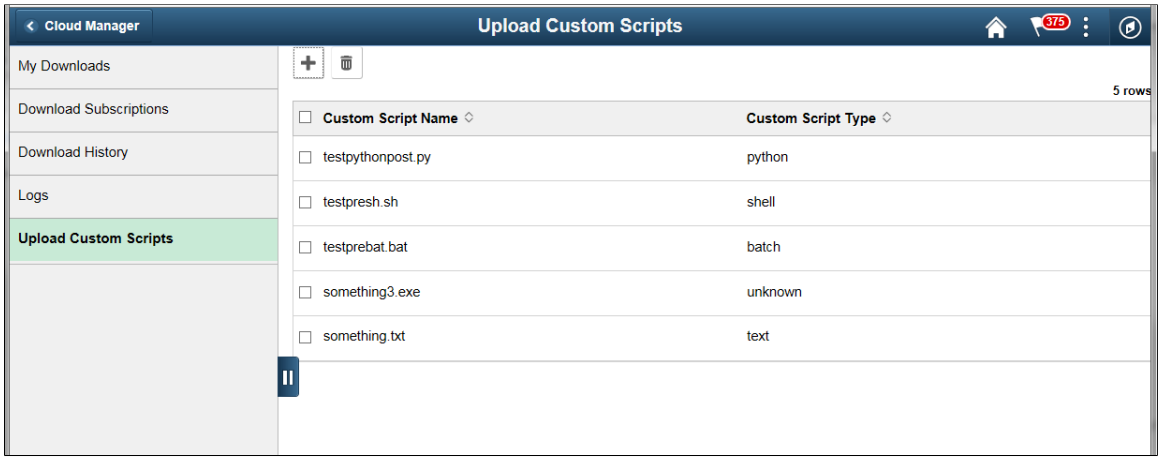
Scripts can call other scripts or multiple scripts from within the scripts and execute them. For example, a shell script can invoke multiple shells, Python or other scripts. You can also upload any kind of supporting files that are used by the scripts.

To upload a custom file:

1. From Cloud Manager homepage, select the Repository tile.
2. Select Upload Custom Scripts.
3. Click the Add icon.
4. The File Attachment pop up appears where you can choose files from your device by clicking on My Device option available.
5. Once you have selected the file, the Upload option appears.
6. Click the Upload button to upload the file to Cloud Manager.
7. When upload is complete, click Done to complete the process.

Image: Upload Custom Scripts page

This example illustrates the fields and controls on the Upload Custom Scripts page. You can find definitions for the fields and controls later on this page.



Environment Variables Allowed in Custom Scripts

Custom scripts provide an ability to extend Cloud Manager's provisioning flow. During provisioning orchestration, Cloud Manager provides access to following environment variables inside the custom scripts.

BASHOPTS

BASH_LINENO

BASH_SOURCE

MAIL PATH

PIPESTATUS

PPID

PSFT_ACCESS_ID

PSFT_ACCESS_PWD

PSFT_ADMIN_PWD

PSFT_APP_DOMAINS

PSFT_APP_TYPE

PSFT_COBOL_SETUP

PSFT_CONNECT_ID

PSFT_CONNECT_PWD

PSFT_CUSTOMIZATION

PSFT_CUSTOMIZATION_DATA

PSFT_DB_INSTANCE_TYPE

PSFT_DB_IS_ML

PSFT_DB_NAME

PSFT_DB_PORT

PSFT_DB_SERVICE

PSFT_DB_TYPE

PSFT_ELASTIC_SEARCH

PSFT_EM_AGENT

PSFT_ENV_TYPE

PSFT_ES_ADMIN_PASSWD

PSFT_ES_HOSTNAME

PSFT_ES_PORT

PSFT_ES_PROXY_PASSWD

PSFT_GW_ADMIN_USER

PSFT_GW_ADMIN_USER_PWD

PSFT_INFRA_AVAILDOMAINPRIMARY

PSFT_INFRA_COMPARTMENT_ID

PSFT_INFRA_HOST

PSFT_INFRA_HOST_OS

PSFT_INFRA_PRIVATE_IP

PSFT_INFRA_PUBLIC_IP

PSFT_INFRA_REGION

PSFT_INFRA_SSH_PRIVATE_KEY_PATH

PSFT_INFRA_SUBNET_ID

PSFT_INFRA_TENANCY_ID

PSFT_INFRA_VCN

PSFT_OPR_ID

PSFT_OPR_PWD

PSFT_PIA_DOMAINS

PSFT_PI_IMAGE

PSFT_PI_NUMBER

PSFT_POST_PROVISION_CUST_SCRIPT

PSFT_PRCS_DOMAINS

PSFT_PRCS_PRCS01_APPENG

PSFT_PRCS_PRCS01_APPLICATION_ENGINE

PSFT_PRCS_PRCS01_COBOL_SQL

PSFT_PRCS_PRCS01_MAXAPIAWARE

PSFT_PRCS_PRCS01_MSTRSRV

PSFT_PRCS_PRCS01_OPTIMIZATION_ENGINE

PSFT_PRCS_PRCS01_PSAESRV_MAX_INSTANCES

PSFT_PRCS_PRCS01_PSAESRV_MIN_INSTANCES

PSFT_PRCS_PRCS01_PSDSTSRV_MAX_INSTANCES

PSFT_PRCS_PRCS01_PSDSTSRV_MIN_INSTANCES

PSFT_PRCS_PRCS01_SQR_PROCESS

PSFT_PRCS_PRCS01_SQR_REPORT

PSFT_PRCS_PRCS01_XML_PUBLISHER

PSFT_PRE_PROVISION_CUST_SCRIPT

PSFT_PSFT_BASE PSFT_WEBLOGIC_ADMIN_PWD

PSFT_WEBLOGIC_ADMIN_USER

PSFT_WEBPROFILE_USER_PWD

PSFT_WEB_WEBSERVER01_AUTH_TOKEN_DOMAIN

PSFT_WEB_WEBSERVER01_PEOPLESOFT01_APPSERVER_CONNECTIONS

PSFT_WEB_WEBSERVER01_WEBSERVER_HTTPS_PORT

PSFT_WEB_WEBSERVER01_WEBSERVER_HTTP_PORT

PWD

PYTHONPATH

SHELLOPTS

SHLVL

SUDO_COMMAND

How to Access Environment Variables in or from Custom Scripts

This section shows some examples of using the environment variables.

Example for Python:

```
os.environ['PSFT_ACCESS_ID'] = ''xyz"
```

Example for Shell:

```
$PSFT_ACCESS_ID=xyz
```

Example for Batch:

```
%PSFT_ACCESS_ID% = xyz
```

Sample Batch File

This sample batch file will print the PATH and PSFT_DB_NAME and store it in a file.

```
set file=C:\temp\script_batch.log

@echo off

@echo Starting the provisioning script > %file%

@echo The value for variable PATH is:  >> %file%

@echo %PATH% >> %file%

@echo The value for variable PSFT_DB_NAME is:  >> %file%

@echo %PSFT_DB_NAME% >> %file%

@echo Ending the provisioning script >> %file%
```

Sample Python Script

This sample python script will print the PATH and PSFT_DB_NAME and store it in a file.

```
import os, time

millis = int(round(time.time() * 1000))

file_name = '/tmp/post-provision_python_{}.log'.format(millis)

f = open(file_name, 'w+')

f.write('Starting post-provisioning script')

f.write('The variable PATH value is: {}\n'.format(str(os.environ.get('PATH'))))

f.write('The variable PSFT_DB_NAME value is: {}\n'.format(str(os.environ.get('PSFT_⇒
DB_NAME'))))

f.write('Ending post-provisioning script')

f.close()
```

Sample Shell Script

This sample python script will print the PATH and PSFT_DB_NAME and store it in a file.

```
now=$(date +%d%m%Y%H%M%S)
file=/tmp/prov_$now.log

echo "Starting the provisioning script" > $file

echo "The value for variable PATH is: " >> $file

echo $PATH >> $file

echo "The value for variable PSFT_DB_NAME is: " >> $file

echo $PSFT_DB_NAME >> $file

echo "Ending the provisioning script" >> $file
```

Managing Topology

Topology defines the infrastructure layout that will be created on Oracle Cloud by Cloud Manager. Essentially, a topology defines a set of nodes, which is an abstraction of a virtual machine. While defining a node, you can set the values for node attributes, such as OS, VM shape, disk capacity, and PeopleSoft components to be installed.

The PeopleSoft administrators create topologies for PeopleSoft applications as per their organization requirements. By default, the Cloud Manager is delivered with the following topologies:

- Lift and Shift
- Lift and Shift - DBaaS
- PUM Fulltier

Note: Users are not allowed to delete lift and shift topologies that are used for lift and shift process.

Pages Used to Manage Topology as an Administrator

Page Name	*Definition Name*	*Usage*
Topology Tile	ECL_TOPOLOGY_FL	To access the Topology landing page.
Topology Page	ECL_TOPO_COMP_FL	To create new topologies, edit or clone existing topologies.
Topology Definition Page	ECL_TOPO_COMP_FL	Create a new topology.

Topology Tile

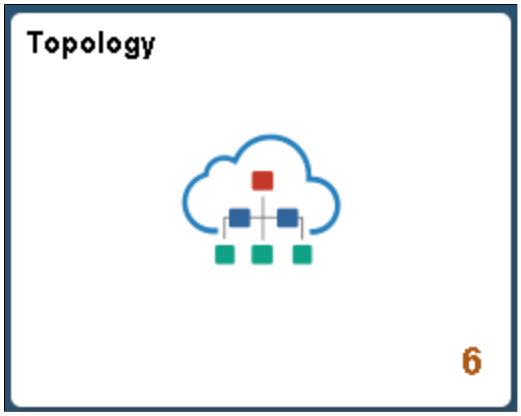
Use the Topology tile to access the Topology landing page.

Navigation

The Topology tile is delivered as part of the Cloud Manager home page.

Image: Topology Tile

This example illustrates the Topology Tile.



Topology Page

Use the Topology page (ECL_TOPOLOGY_FL) to perform the following:

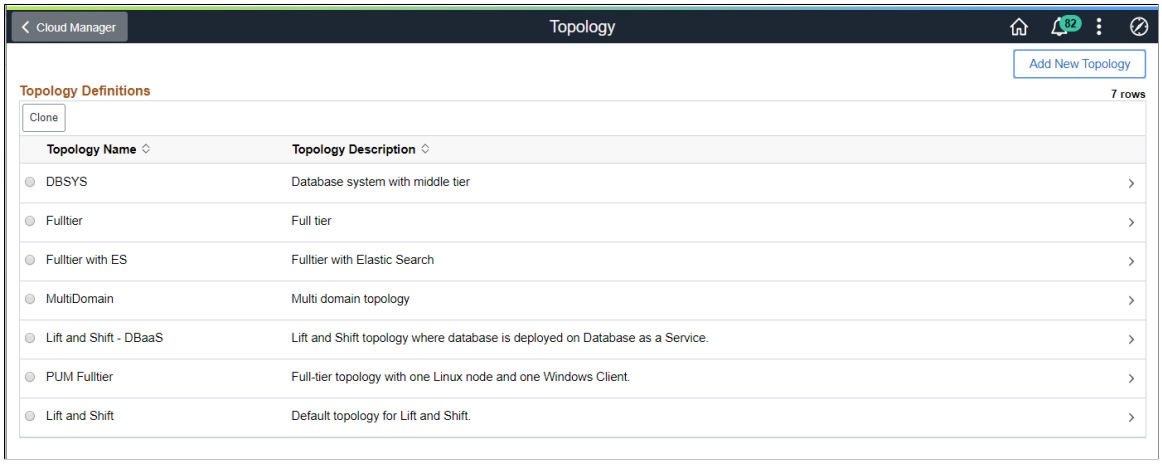
- Create a new topology
- Edit an existing topology
- Clone an existing topology
- Delete an existing topology

Navigation

Click the Topology tile on the delivered Cloud Manager home page. The Topology page is displayed.

Image: Topology Page

This example illustrates the fields and controls on the Topology page. You can find definitions for the fields and controls later on this page.



Topology Name Name of the topology.

Topology Description	Description for the topology.

Creating a New Topology

To create a new topology:

1. Click the Add New Topology button available on the upper-right corner of the Topology page.
2. In the Topology Definition page, enter the topology name and the corresponding description.
3. Click the Add Node button to create a node. This opens the Add Node page. Use the Add Node page to set the values for node attributes like OS, sizing parameter, disk to be attached, and the PeopleSoft component to be installed.
4. Click Save to save the details.

Validation Rules for Topology

The following are the set of current validation rules for topology:

If there is a full tier node, then you:

- Cannot have another full tier node.
- Cannot have a mid-tier node.
- Cannot have a database node.
- Cannot have a Database as a Service node.

If there is a mid-tier node, then you:

- Cannot have a full tier node.
- Must have either a Database as a Service node or a database node.

If there is a database node, then you:

- Cannot have another database node.
- Cannot have a Database as a Service node.
- Cannot have a full tier node.

If there is a Database as a Service node, then you:

- Cannot have another Database as a Service node.
- Cannot have database node.
- Cannot have a full tier node.

Apart from this, user may have a Windows Client Node in all the above mentioned cases and an optional ELK Stack Node.

Topology Definition Page

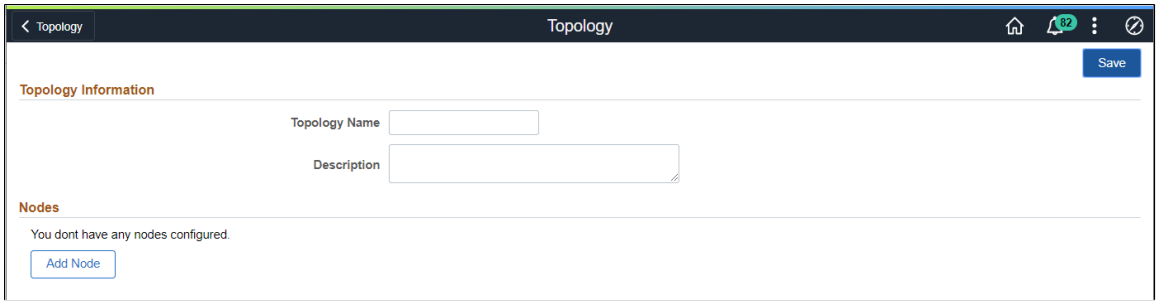
Use the Topology Definition page (ECL_TOPO_COMP_FL) to create a new topology.

Navigation

Click the Add New Topology button on the upper-right corner of the Topology page to access the Topology Definition page.

Image: Topology Definition page

This example illustrates the fields and controls on the Topology Definition page.

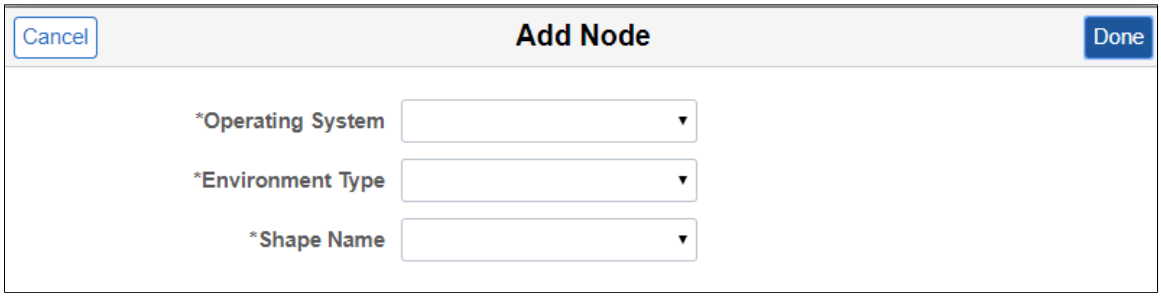


Add Node Page

Use Add Node page to add nodes for creating a topology.

Image: Add Node page

This example illustrates the fields and controls on the Add Node page. You can find definitions for the fields and controls later on this page.



Operating System Select the operating system (Linux or Windows) used to create the topology.

Environment Type Select the PeopleSoft software components to be deployed on the node.

The following environment types are available for Linux operating system:

- DB Systems: Database systems are dedicated instances running Oracle Linux, optimized for running one or more Oracle databases. A DB System is a Database Service resource. Cloud Manager supports provisioning of databases

on OCI DB Systems. CM provisions 1 and 2 node Database systems on virtual machines.

The shape for DB systems can be BM (Bare metal), VM or Exadata.

See Adding DB Systems Node

- Database Tier: Deploys the PeopleSoft database on a compute node.
- ELK Stack: Sets up Elasticsearch (ES) and optionally Kibana on the node.

  See Creating ELK Stack Node
- Full Tier: Deploys Database, Appserver, Webserver and Process Scheduler on the node. Additional features available for Fulltier include COBOL, Kibana, and Elasticsearch.
- Middle Tier: Deploys Appserver, Webserver and Process Scheduler on the node. If Process Scheduler is selected, you can add the COBOL feature.

  See Adding Middle Tier Nodes

The following environment types are available for Windows operating system:

Note: For applying PeopleTools patch to an environment, it is mandatory to have a PeopleSoft client or a Windows middle tier node defined.

- PeopleSoft Client: Deploys Windows client components on the node.
- Middle Tier: Deploys Windows client with process scheduler. Optionally you can add nVision.

  See Creating Windows Middle Tier Nodes

Shape Name

Select the required VM shape.

For DB systems, BM shapes, VM shapes as well as Exadata are supported.

Note: The Exadata DB System must already exist on OCI. When you select Exadata, the environment (shift) will create the databases within the Exadata DB system.

For non-DB system nodes, the list of VM shapes depends on the custom Linux and Windows image that is specified in the "Infrastructure Settings" page. In OCI, whenever a user creates a

custom Linux or Windows image, a set of shapes get associated with that image. CM shows that set of shapes, when end-user creates or modifies the nodes in a topology.

Note: The list of shapes will not appear until you do a Refresh of OCI Metadata after configuring the Operating System images in the Settings page. Some shapes may not be available in new tenancies.

Disk Space (GB)

Select the amount of disk space attached to the machine.

Note: Assume that if the lifted DPK is K size, then the disk size should be 2.5 times K.

Note: For DB System, only a limited set of pre-defined disk sizes are supported. The allowed disk sizes are:

- 256 GB
- 512 GB
- 1024 GB
- Multiples of 1024 GB

Note: For BM or Exadata DB system shapes, this field is not visible.

Adding DB Systems Node

Available shapes for Database Systems are:

- BM (Bare metal)
- VM
- Exadata

Note: Before performing an environment shift, you must modify the Lift and Shift - DBaaS topology with the required size and capacity of the database.

Database System Node on Exadata

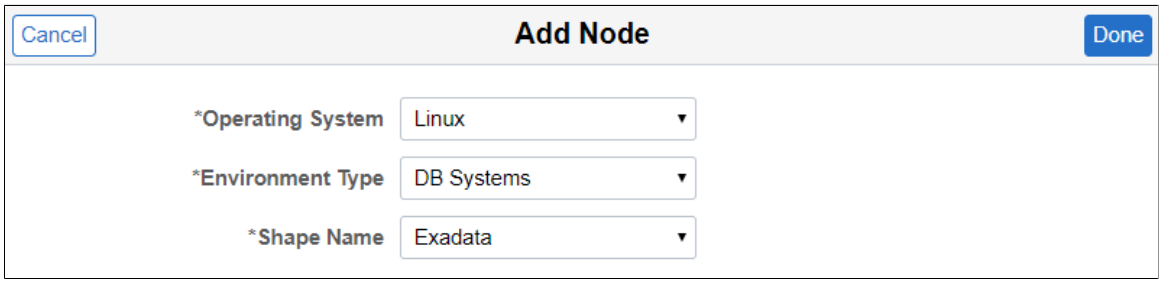
When you select the shape name as Exadata , you are instructing Cloud Manager to create the environment (shift) with the databases on your existing Exadata DB System on OCI.

When you select Exadata for the DB Systems, disk space is not displayed.

Important! Exadata database is a RAC system which supports multiple nodes, you need to add Cloud Manager SSH public key on all nodes. See Administering Oracle Database Exadata Cloud Service

Image: Add Node page for DBS

This example illustrates the fields and controls on the Add Node page for DB systems on Exadata.

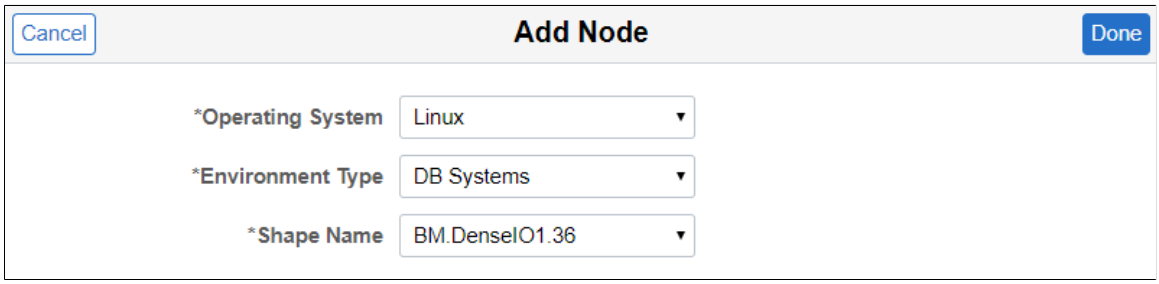


Database System Node on Bare Metal

When you select a bare metal shape for the DB Systems, disk space is not displayed.

Image: Add Node page for DB Systems on Bare Metal

This example illustrates the fields and controls on the Add Node page for database systems on Bare Metal.

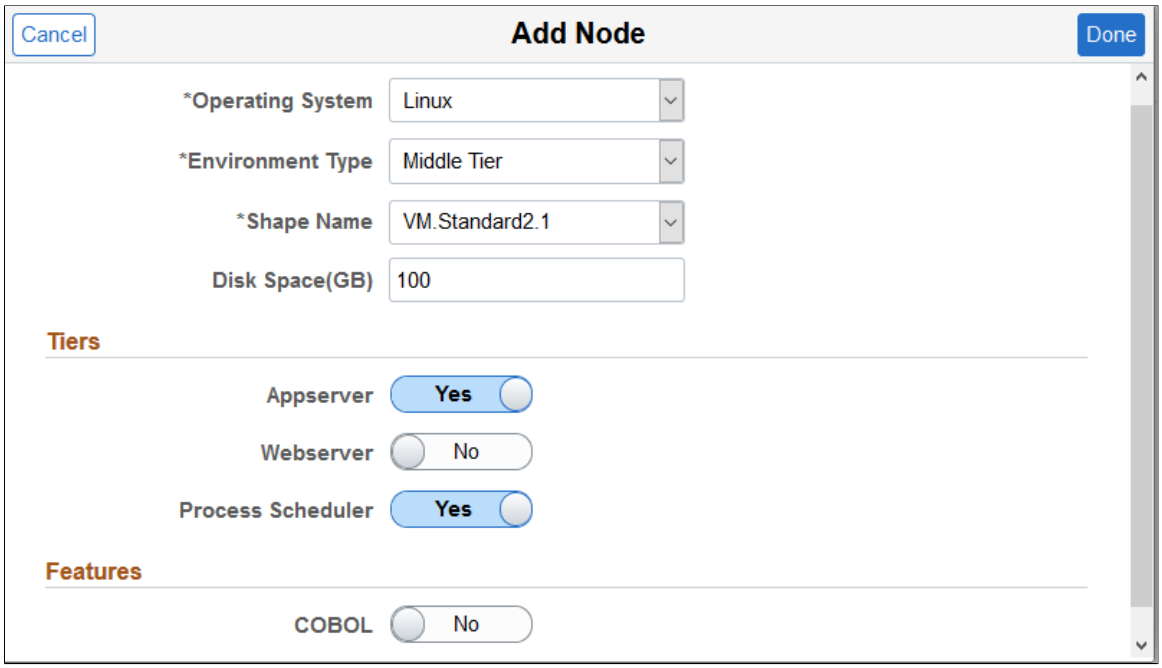


Adding Middle Tier Nodes

When you add a middle tier node, the tiers section is displayed.

Image: Add Node page for Middle Tier

This example illustrates the fields and controls on the Add Node page for Middle Tier. You can find definitions for the fields and controls later on this page.



Select the tier or tiers for this node.

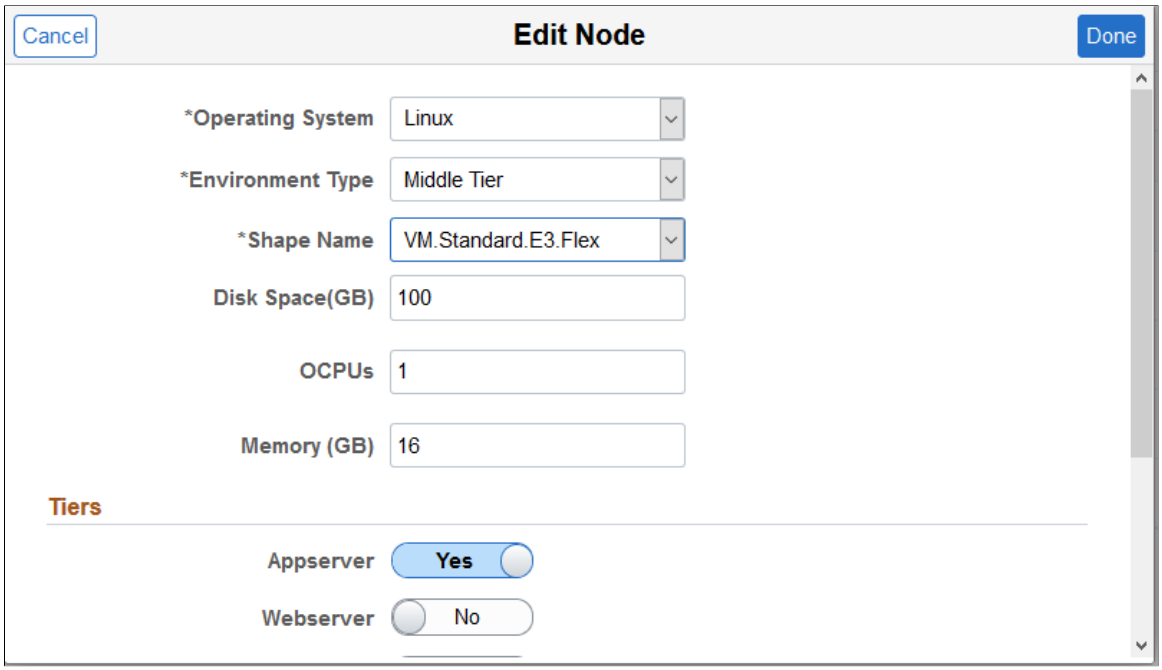
This table lists the supported combinations for the tiers:

Application Server	*PIA*	*Process Scheduler*
Yes	Yes	Yes
Yes	No	Yes
Yes	No	No
No	Yes	No
No	No	Yes

The VM.Standard.E3.Flex shape is also available for Linux Middle Tier and Fulltier nodes.

Image: Add Node page for VM.Standard.E3.Flex shape

This example illustrates the fields and controls on the Add Node page for VM.Standard.E3.Flex shape. You can find definitions for the fields and controls later on this page.



OCPUs Select from 1 to 64 OCPUs.

Memory (GB) For each OCPU, you can select up to 64 GB of memory, with a maximum of 1024 GB total.

The minimum amount of memory allowed is either 8 GB or a value matching the number of OCPUs, whichever is greater.

Creating ELK Stack Node

Note the following regarding Elasticsearch and Kibana:

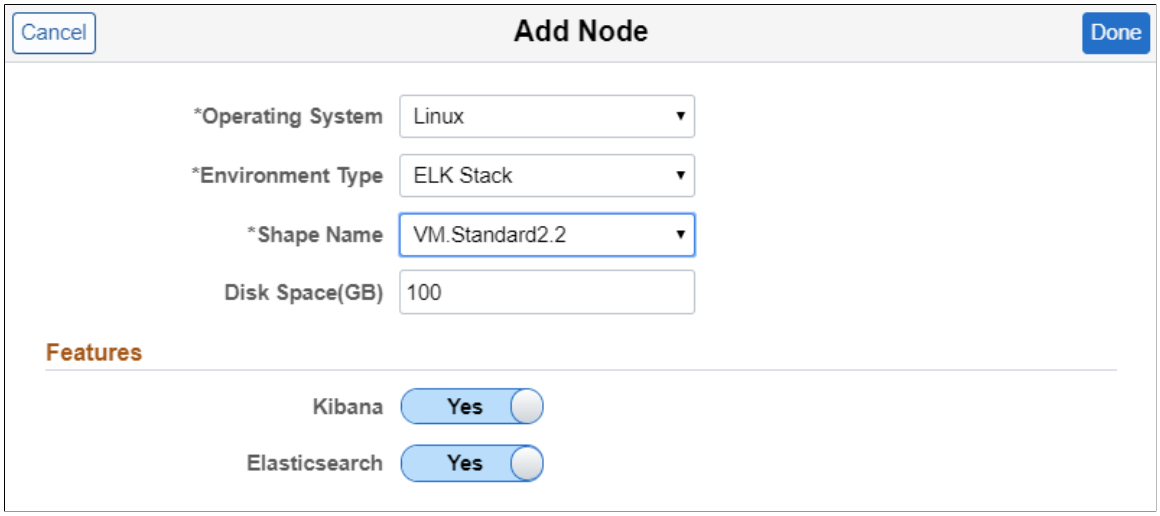
- Elasticsearch node configuration is automatically done by Cloud Manager.

  For information on how to deploy and configure Elasticsearch refer Elasticsearch Home Page on My Oracle Support (Doc ID 2205540.2).

- Kibana is only available with PeopleTools 8.58 or higher.
- In order to provision Kibana, Elasticsearch must be selected.
- For environments configured with Elasticsearch, Kibana will be automatically installed as part of the PeopleTools upgrade to 8.58.

Image: Add Node page for ELK Stack

This example illustrates the fields and controls on the Add Node page for ELK Stack.



Creating Windows Middle Tier Nodes

Starting with Cloud Manager Image 10, you can create multiple Windows middle tier nodes. You can use either a custom Windows image or an OCI platform image. The image is selected on the Infrastructure Settings page.

Prerequisites

- Configure the Windows Image in Infrastructure Settings.

  See Infrastructure Settings Page

- Subscribe to the Windows channel for your application.

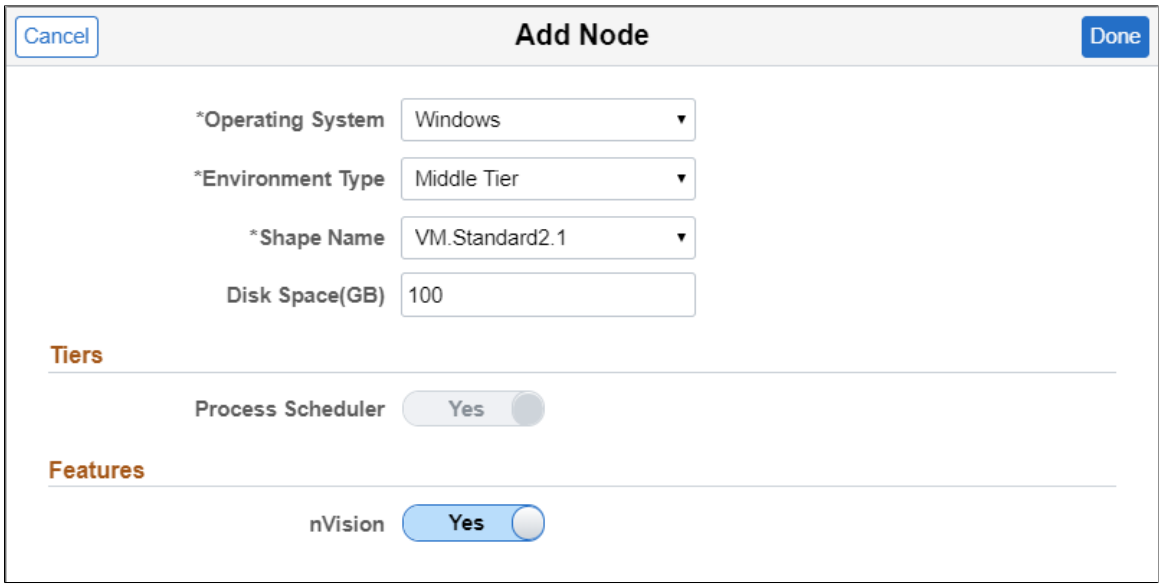
  See Download Subscriptions Page

Use the Add Node page to create a new Windows node.

This is an example of an existing Windows Node.

Image: Example Windows Node

This example illustrates the fields and controls on the Add Node page with Windows Operating System selected. You can find definitions for the fields and controls later on this page.



Operating System	Windows.
Environment Type	Middle Tier
Shape Name	Select the required VM shape.
Disk Space (GB)	Select the amount of disk space attached to the machine.
Tiers	Only Process Scheduler domain is supported for Windows middle tier Node. Windows Process Scheduler is required for running nVision reports.
Features	The nVision feature can be set either on or off.

Creating Multi Domain and Multi Middle Tier Node Configurations

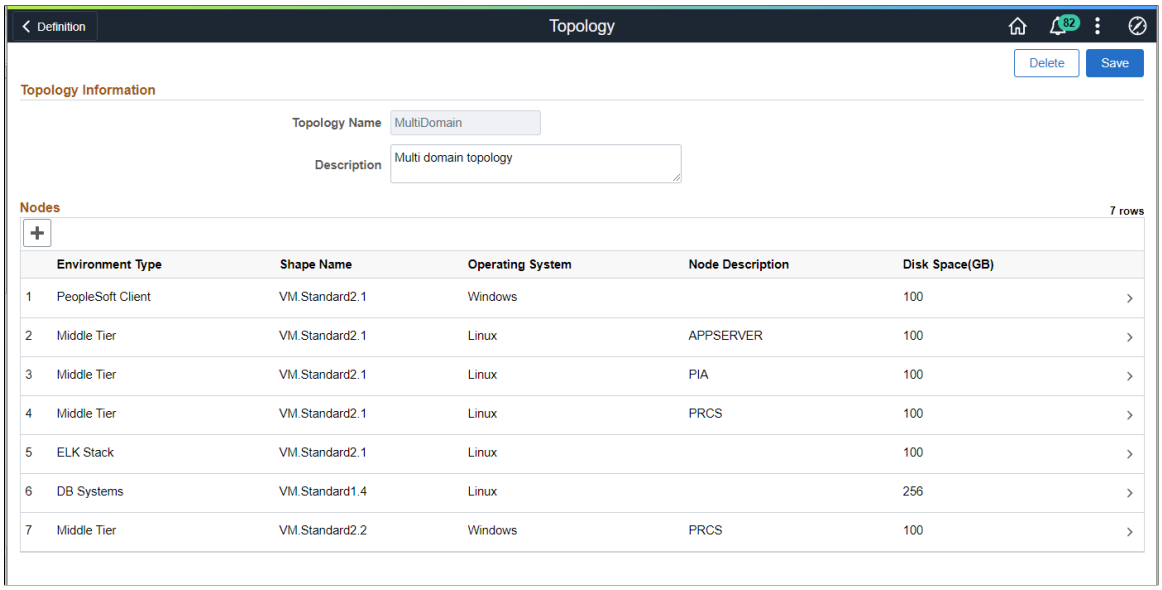
Cloud Manager Image 8 and above supports both horizontal and vertical elasticity by allowing multi node and multi domain configuration for the PeopleSoft environment.

Cloud Manager supports multiple middle tier and PIA domains on single node as well on multiple nodes. It also provides an option to enable Integration Broker in one application domain in an environment. This Domain Configuration feature extends the existing provisioning environment feature in Cloud Manager.

See Configuring AppServer Tier Domain Settings.

Image: Example Multi Domain Topology

This example illustrates the fields and controls on the Topology page for a topology with multiple middle tiers.

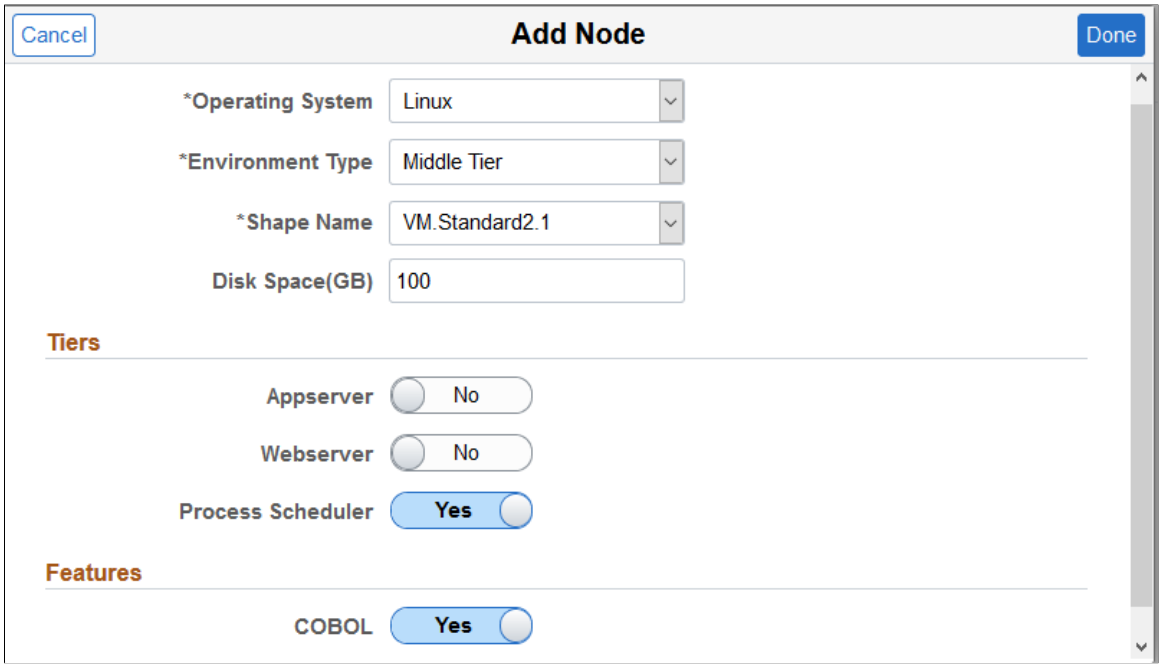


Enabling Topology with Cobol Feature as Yes

COBOL can only be enabled in the node only when environment type is Full Tier or Middle Tier with Process Scheduler enabled.

Image: Example Middle Tier node with Process Scheduler enabled

This example illustrates a middle tier node with Process Scheduler enabled.



Note: Process Scheduler must be enabled in order to enable COBOL.

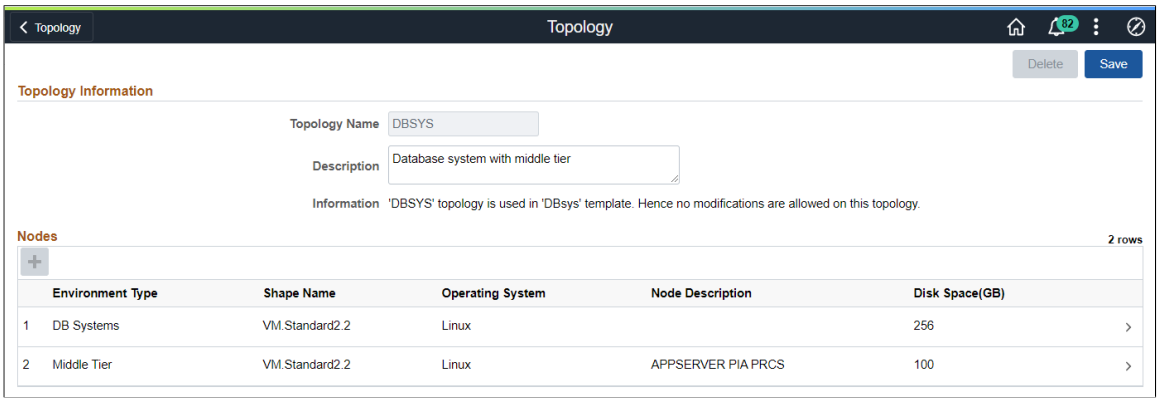
Editing an Existing Topology

To edit an existing topology, perform the following:

1. Click any existing topology in the Topology page. This displays the Topology Definition page of the topology which you want to edit.

   Image: Topology Definition – Edit page

   This example illustrates the fields and controls on the Topology Definition – Edit page. You can find definitions for the fields and controls later on this page.



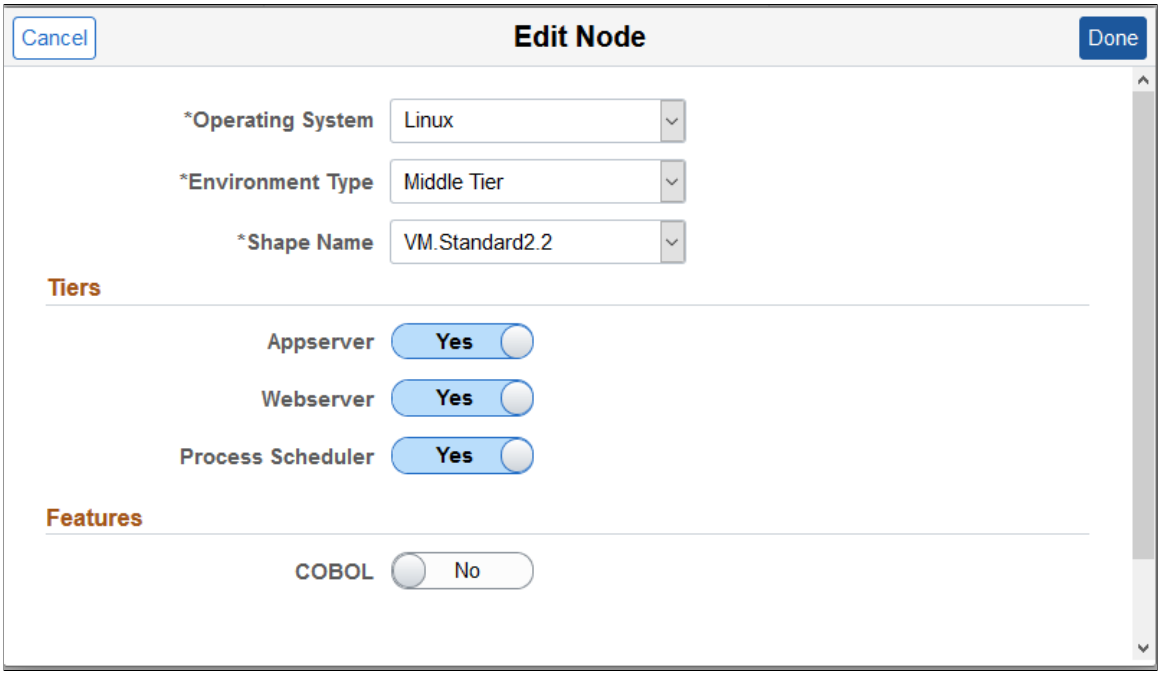
2. You can edit the description, if required.
3. Click + to add new nodes.

   See Add Node Page

4. To edit any node attribute value, click on any node row. This displays the Edit Node window.

Image: Edit Node window

This example illustrates the fields and controls on the Edit Node window.



5. Edit the fields as per requirement.
6. Click Done to save the edited details.

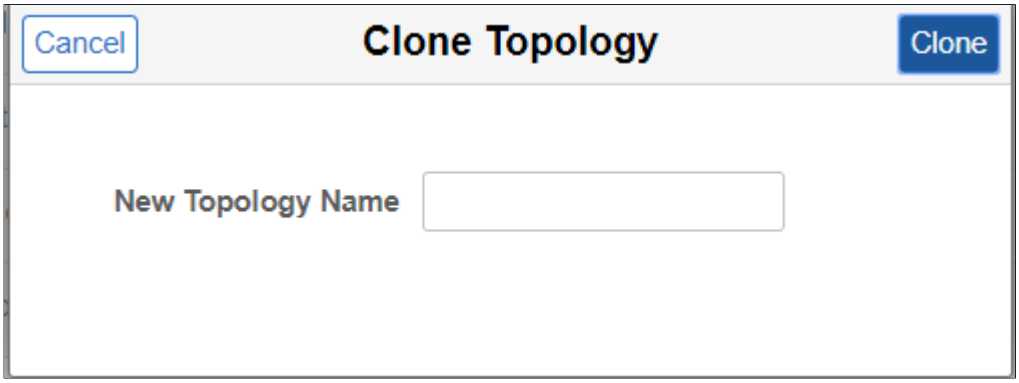
Cloning an Existing Topology

To clone an existing topology, perform the following:

1. Select the radio button corresponding to a topology that you want to clone.
2. Click Clone button in the Topology page. This displays the Clone Topology window.

Image: Clone Topology window

This example illustrates the fields and controls on the Clone Topology window.



3. Enter a new topology name and click Clone. The new topology is added to the topology list.

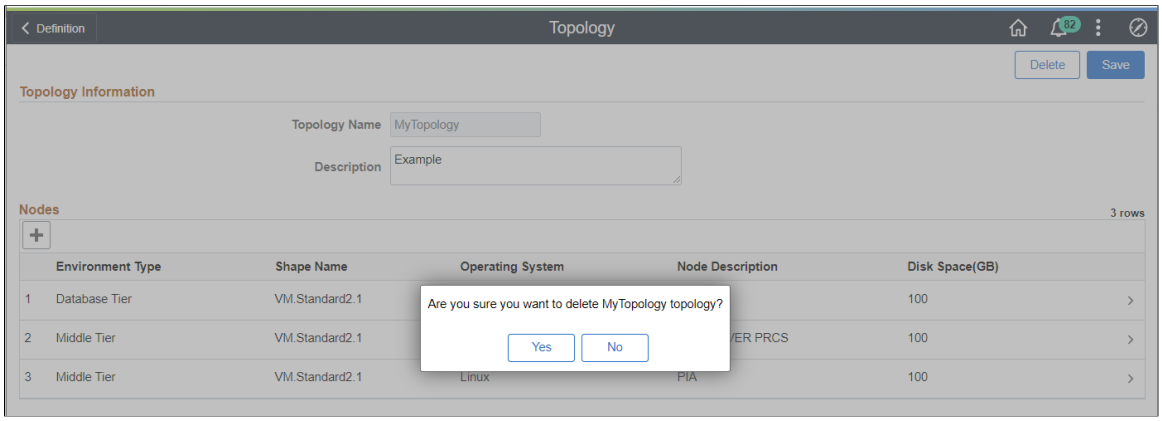
Deleting an Existing Topology

To delete an existing topology, perform the following:

1. Click any existing topology in the Topology page. This displays the Topology Definition page of the topology.
2. Click Delete, to delete the topology.

Image: Example Delete Topology page

This example illustrates the fields and controls on the Example Delete Topology page.



Managing Template

An environment template is a repeatable blueprint that is used to deploy PeopleSoft environments using Cloud Manager. A template defines the topology to be used when deploying the PeopleSoft application DPK, which gets downloaded to the Repository. A template also defines environment attributes to enable streamlined deployments. Access to templates can be managed by defining security attributes of the templates.

Pages Used to Manage Environment Templates as a PeopleSoft Administrator

Page Name	*Definition Name*	*Usage*
Environment Template Tile	Understanding Governance FrameworkECL_TEMPLATE_LP_FL_GBL (This is the CREF for the tile.)	Access the Environment Template landing page.
Environment Template Page	ECL_TEMPLATE_FL	Create new templates or edit, delete or clone existing templates.

Page Name	*Definition Name*	*Usage*
Environment Template – General Details Page	ECL_TEMPL_GEN_FL	Enter the template name, description, and selecting a database.
Environment Template – Select Topology Page	ECL_TEMPL_TOP_FL	Select the topology that you have already defined.
Environment Template – Security and Policies Page	ECL_TEMPL_SEC_FL	Associate zones in which the environment is created, the roles that have access to the template, and policies that will be auto-enabled for the environment.
Environment Template – Summary Page	ECL_TEMPL_REV_FL	Displays the summary of the environment template that the user is about to create.

Environment Template Tile

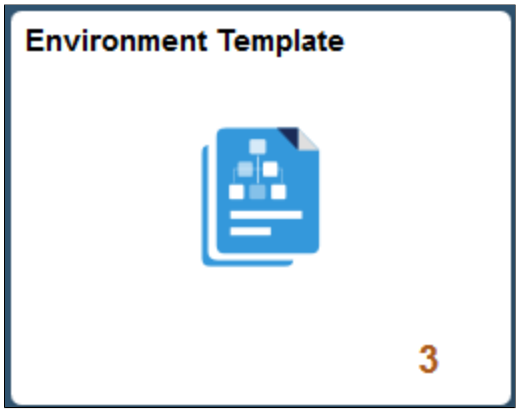
Use the Environment Template tile (ECL_TEMPLATE_LP_FL_GBL) to access Environment Template landing page.

Navigation

The Environment Template tile is delivered as part of the Cloud Manager home page.

Image: Environment Template Tile

This example illustrates the Environment Template Tile.



Environment Template Page

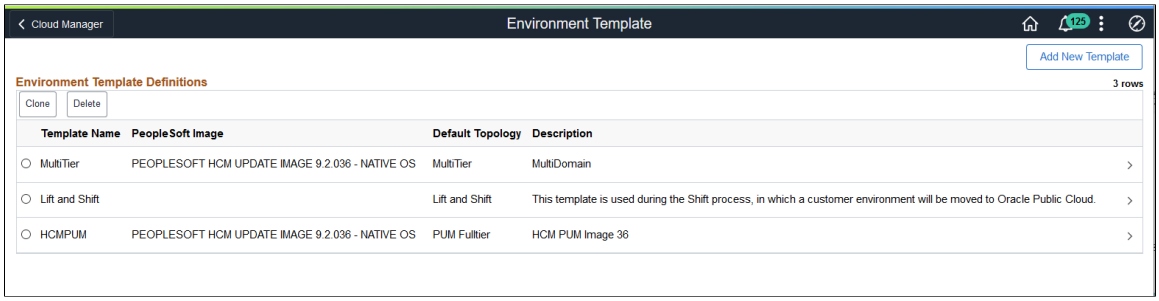
Use the Environment Template page (ECL_TEMPLATE_FL) to create a new template, and edit, delete or clone an existing template.

Navigation

Click the Environment Template tile on the delivered Cloud Manager Fluid home page. The Environment Template page is displayed by default.

Image: Environment Template page

This example illustrates the fields and controls on the Environment Template page. You can find definitions for the fields and controls later on this page.



Note: The Lift And Shift template is the default template displayed in the Environment Template page with no database associated with it.

Template Name	Name of the template.
Database	Indicates the PeopleSoft application DPK that gets installed when the template is deployed.
Default Topology	Default topology associated with the template.
Description	Add a description for the template.

Edit/Delete/Clone an Existing Template

User can edit, delete or clone the existing templates using the Environment Template landing page.

Note: It is recommended to recreate the existing templates to ensure that the new custom attributes are available in the template.

- To edit an existing template details, click a row and modify the details as per requirement.
- To delete an existing template, select the radio button corresponding to the template which you want to delete and click the Delete button. Users cannot delete a template, if it is already used for defining an environment.
- To clone an existing template, select the radio button corresponding to the template which you want to clone and click the Clone button available on the Environment Template landing page. The Clone Template modal window is displayed, wherein you can enter the new template name and click the Clone button. The new template is added to the template list.

Default Environment Templates

A default template is provided for Lift and Shift, which is used during environment shifting by default. This Lift and Shift template and its associated topology must be modified such that it is suitable for the environment being shifted. The Lift and shift topology is fixed in terms of number of nodes, but the shape and disk space parameters can be modified. For any environment to be provisioned in Cloud Manager, the administrator creates a template and a user uses that template to provision. In case of Lift and Shift, a default template is provided out of the box and there is no need to create any templates. When

an administrator creates an environment on the Lift and Shift page, the process automatically chooses the default Lift and Shift template. This Lift and Shift template must be modified to suit the environment being shifted. For more details, see Understanding the Lift and Shift Process.

Creating a Template

Use the Environment Template wizard to create a new template using a step by step guided process.

By default, the create template guided process involves the following steps:

1. Entering general details.

   See Environment Template – General Details Page

2. Selecting topologies.

   See Environment Template – Select Topology Page

3. Defining security and policies.

   See Environment Template – Security and Policies Page

4. Submitting the details.

   See Environment Template – Summary Page

Environment Template – General Details Page

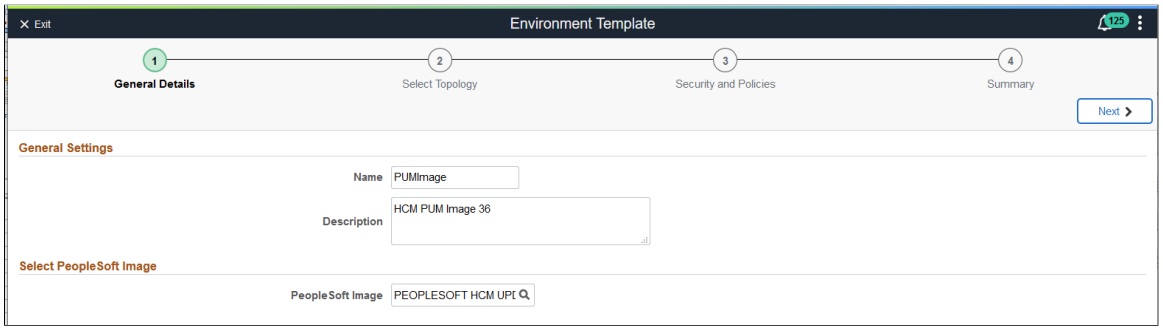
Use the Environment Template – General Details page to enter the template name, description, and select a database.

Navigation

Click the Add New Template button on the Environment Template landing page.

Image: Environment Template – General Details page

This example illustrates the fields and controls on the Environment Template – General Details page. You can find definitions for the fields and controls later on this page.



Name Name of the template which you want to create.

Description Add a description for the template.

PeopleSoft Image Select a PeopleSoft application DPK from the list of DPKs available in the Repository.

Environment Template – Select Topology Page

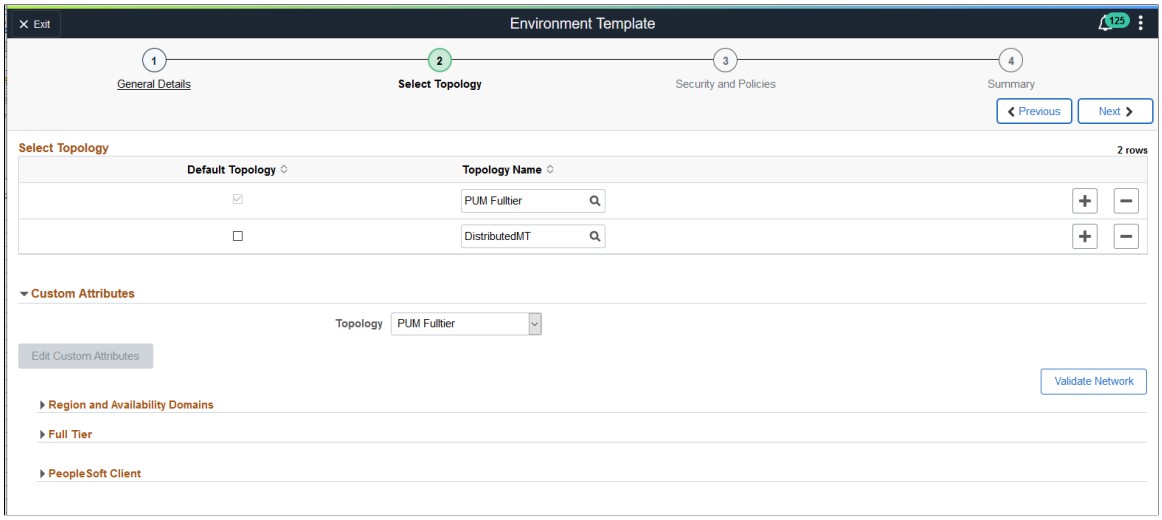
Use the Environment Template – Select Topology page to select the topology that you have already defined. You may edit the default attributes associated with the selected topology.

Navigation

- Click Next in the Environment Template – General Details page.
- Click Step 2, Select Topology, at the top of the page to navigate to the Environment Template – Select Topology page in the guided process.

Image: Select Topology page

This example illustrates the fields and controls on the Select Topology page. You can find definitions for the fields and controls later on this page.



Default Topology Users can mark one of the topology associated with the template as the default topology. During the environment creation process using a template, you can override this default topology and select any other topology associated with that template. If you don't want to override, then the default topology will get used automatically.

Click + to add more topologies. A new row of empty fields appears below the existing record. You can configure the fields based on the requirements.

Note: Be sure to select the topology under the Override Topology section and then continue with the template creation.

Topology Name Select the required topology that you want to include in the template.

Note: While selecting a topology, the custom attributes associated with the selected topology is displayed. It is possible to override the default attributes based on the requirements.

Configuring Custom Attributes

1. Expand the Custom Attributes section.
2. Select the required topology.
3. Enter the required attributes and click Next.

Note: Cloud Manager allows users to add customization during template creation under Edit Custom Attributes section. This customization can be added only to middle tier and database tier. The customization will be available to users when they select this template. This facilitates the user to define custom attribute values for the environment being deployed.

4. After entering the required attributes, click the Validate Network button to ensure your infrastructure settings are correct and the network is valid.

   This validates whether the port is open for an incoming/outgoing connection across different subnets and VCN. The connection can be:

   a. From Cloud Manager to VM

   b. From VM to Cloud Manager

   c. From VM to VM

   Some of the validations are based on user input (Jolt Port, WSL Port, Database Server Port, HTTP PIA Port, HTTPS PIA Port).

   The following implicit validations are performed:

From	***To***
Every subnet	Cloud Manager subnet: NFS ports TCP - 2049, 111, 892, 32803
Cloud Manager subnet	Every subnet (including itself) except Windows VM subnet: ssh port 22
Cloud Manager subnet	Windows VM’s subnet : WinRM TCP Ports 5985, 5986
Cloud Manager subnet	Windows VM’s subnet: CIFS ports TCP 445, 139, 138, 137

The following sections must be configured in every template.

- Region and Availability. See Configuring Region and Availability Domains
- Network for node. See Configuring Network Settings
- Network Security Groups (optional) for node. See Configuring Network Security Group Settings

- Fault domain for the node. See Configuring the Fault Domain

  Note: DB Systems node does not have fault domain setting.

- Advanced section. See Configuring Advanced Section

  Note: Add Node operation and ELK nodes do no include an Advanced section.

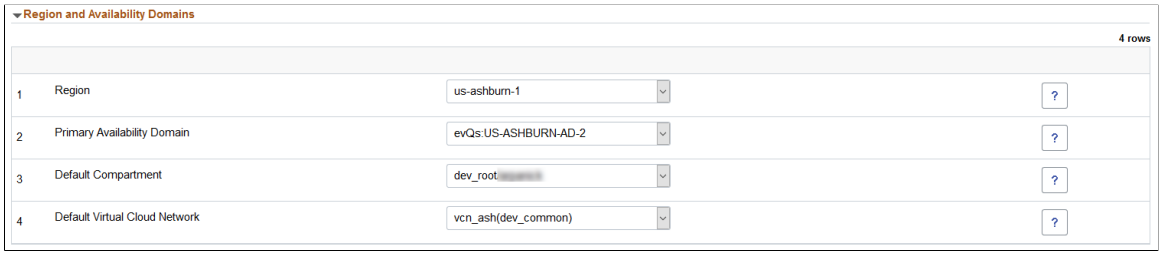
The General Setting and Domain Settings depend on the type of node.

- Fulltier. See Configuring Full Tier Template Settings
- DB Systems. See Configuring DB Systems Settings
- Web Server. See Configuring Web Server Tier Settings
- Application Server. See Configuring AppServer Tier Domain Settings
- Process Scheduler. See Configuring Process Scheduler General Setting and Configuring Process Scheduler Domain Settings
- Windows. See Configuring Windows Middle Tier General Settings
- Database Tier. See Configuring Database Tier
- ELK Stack. See Configuring ELK Stack General Settings

Configuring Region and Availability Domains

Image: Region and Availability Domains section

This example illustrates the fields and controls on the Region and Availability Domains section. You can find definitions for the fields and controls later on this page.



Region 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.

Note: Cloud Manager will provision and manage environments only in the region where it is deployed. See Infrastructure Settings Page.

Primary Availability Domain Availability domain in OCI.

Default Compartment Compartments allow you to organize and control access to your cloud resources. A compartment is a collection of related

resources (such as instances, virtual cloud networks, block volumes) that can be accessed only by certain groups that have been given permission by an administrator.

Select a default compartment, this compartment will be used for all tiers in the template.

Note: You must use a compartment that is directly under the root compartment. Nested compartments, that is, lower-level subcompartments, are not supported for Cloud Manager, or for environments that you provision with Cloud Manager.

Default Virtual Cloud Network

Virtual Cloud Network within OCI. A virtual cloud network is a virtual version of a traditional network—including subnets, route tables, and gateways on which your instances run.

Select the default Virtual Cloud Network, this will be the default VCN used for all tiers in the template.

For details on setting up the OCI environment, refer to the OBE Installing PeopleSoft Cloud Manager in Oracle Cloud Infrastructure.

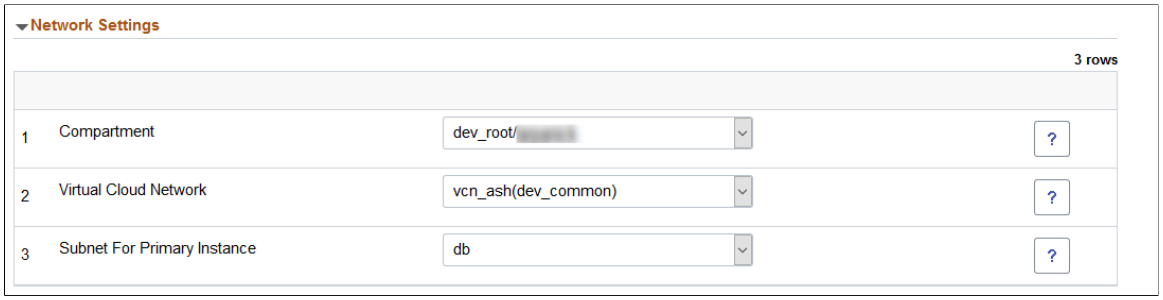
Note: In OCI, the templates will not have any default values for Region and Availability Domains section. All templates must be updated with these settings before using it for deployment using the Create Environment Page.

Configuring Network Settings

Each node in the template must be configured for subnet where it will run. The compartment and VCN default to the values entered in the Region and Availability Domain section, these values can be changed to run in a different compartment or VCN. For more information on VCN peering see the tutorial *Use Multiple VCNs, Multiple Compartments, or Network Security Groups with PeopleSoft Cloud Manager (Optional)*.

Image: Network Setting section

This example illustrates the fields and controls on the Network Setting section. You can find definitions for the fields and controls later on this page.



Compartment

The default compartment is displayed, you can select a different compartment for the network.

Virtual Cloud Network	The default VCN is displayed, you can select a different VCN for this node.
Subnet For Primary Instance	Select the subnet where this node will run.

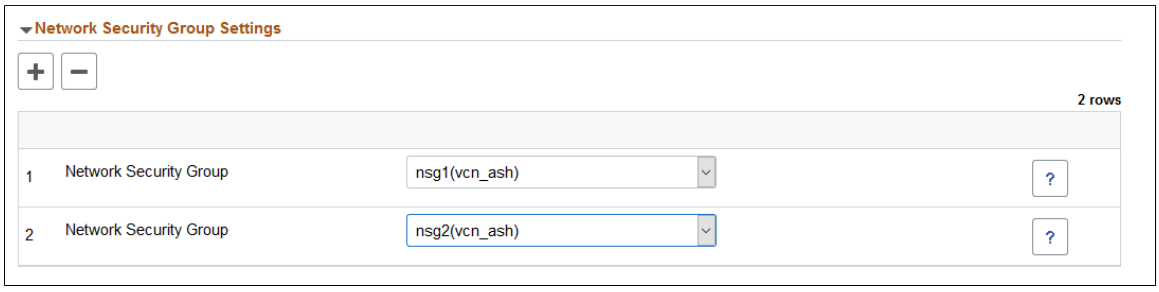
Configuring Network Security Group Settings

Cloud Manager supports Network Security Groups (NSG). Network Security Groups are set up outside of Cloud Manager. Up to 5 Network Security Groups can be assigned to a node.

See tutorial *Network Security Groups with PeopleSoft Cloud Manager (Optional)*.

Image: Network Security Group Settings section

This example illustrates the fields and controls on the Network Security Group Settings section.



Configuring the Fault Domain

Each availability domain in OCI contains three fault domains for high availability. OCI randomizes the availability domains by tenancy to help balance capacity in data centers.

Use the Fault Domain Settings section to select which fault domain to use for a specific node. Select the fault domain from the drop down list, only fault domains in the availability domain for the node are listed and available.

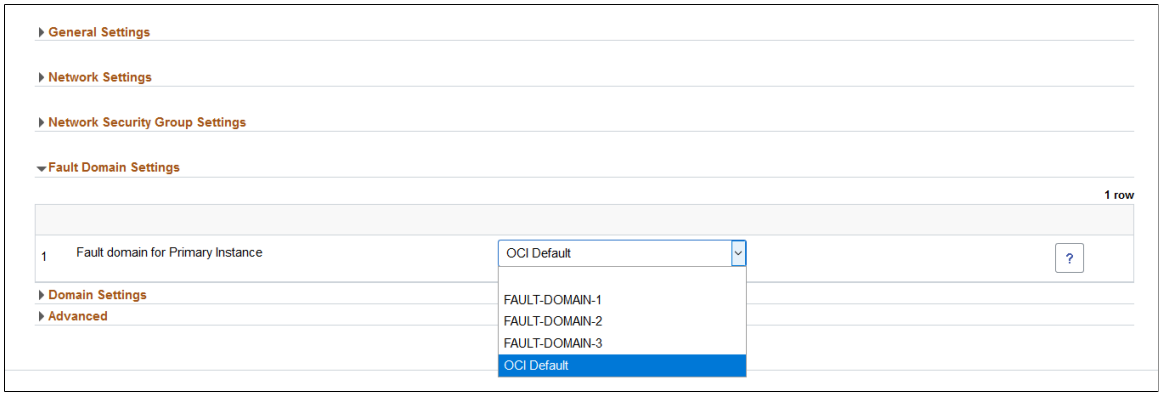
If OCI Default is selected , OCI randomly selects the fault domain to use and customer is not aware of which fault domain is being used.

Note: DB Systems node does not have fault domain settings.

For more information on faults domains see Regions and Availability Domains.

Image: Fault Domain section

This example illustrates the fields and controls on the Fault Domain section.



Configuring Advanced Section

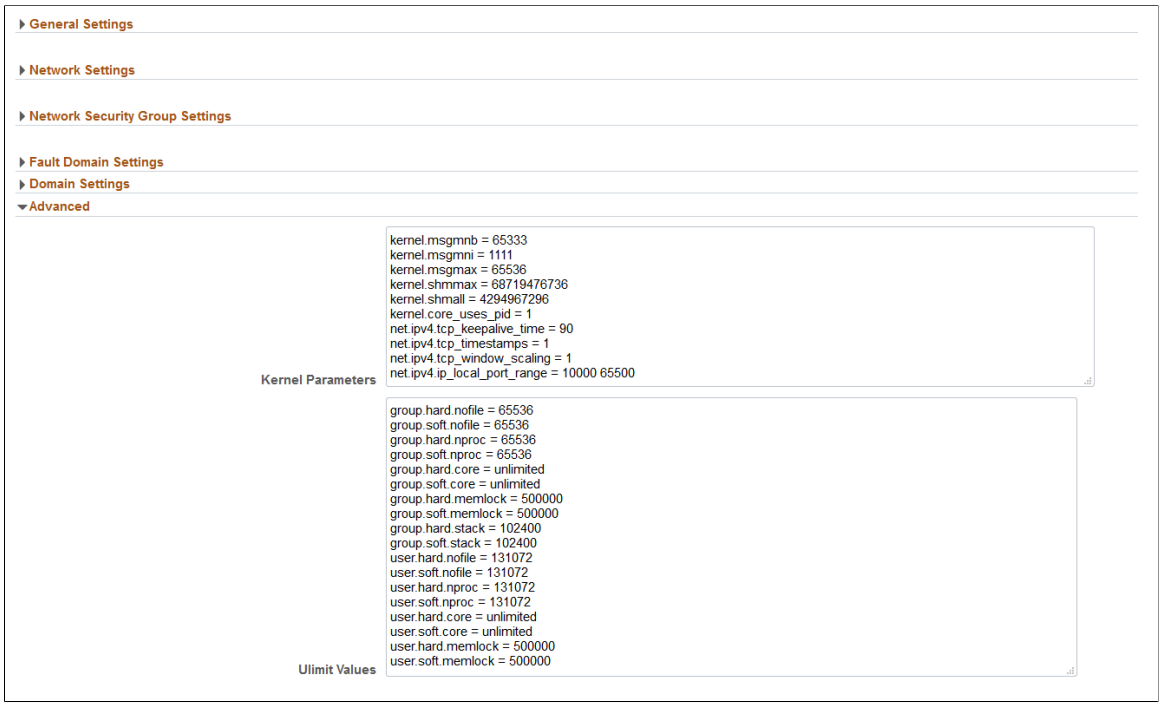
The Advanced section contains kernel parameters and Ulimit values. Expert administrators have the option to change these values.

Important! No validation is performed on these fields. Only Operating system experts should change these values.

Note: Add Node operation and ELK nodes do not include an Advanced section.

Image: Advanced section

This example illustrates the fields and controls on the Advanced section.



Ulimits

This input field allows you to set ulimit values for the Linux node. Each line of the input represents one ulimit entry. The format to be used for each line is as follows:

```
[user|group].[soft|hard].<limit name> = <value>
```

The left-hand side of the expression represents a ulimit, and the right hand expression is a value of that ulimit. They are separated by a = sign.

user or group — The key word “user” represents a limit for a Linux user, and the key word “group” represents a limit for a user group. Exactly which users and groups are added to the Linux configuration files is internally determined by the environment deployment process. You cannot set those actual user/group names here.

soft or hard — The keyword “soft” denotes the limit a process can use. It can later be increased by the corresponding user/group.

The keyword “hard” denotes the maximum limit to which the soft limit can be raised to.

limit name — This is the name of the limit. Please refer to table below for the list of names

value — This is either a numeric value or the string “unlimited”. Please refer to table below for a list of values and the units in which they have to be expressed

This table lists the ulimit names.

Name	***unit***
cpu	Seconds
fsize	Blocks
data	Kilobytes
stack	Kilobytes
core	Blocks
rss	Kilobytes
nofile	Number of file descriptors
as	Kilobytes
nproc	Number of processes
memlock	Kilobytes

Name	*unit*
lock	Number of locks
sigpending	Number of queued signals
nice	Nice level (an integer)
rtprio	Realtime priority (an integer)
rttime	Number

Kernel Parameters

The kernel parameters input field can be used for setting Linux kernel parameters. Each line represents one Linux parameter. The format of each line should be as follows:

```
<kernel parameter name> = <value>
```

The list of all kernel parameters can be found from the main page of the Linux sysctl command.

Configuring Full Tier Template Settings

Example Full Tier Node with ELK Stack and COBOL

Based on the topology selected, the full tier contains the appropriate settings for the node. The examples in this section display full tier topology that includes ELK Stack and COBOL.

Image: Full Tier - General Settings (1 of 2)

This example illustrates the fields and controls on the Full Tier - General Settings (1 of 2). You can find definitions for the fields and controls later on this page.

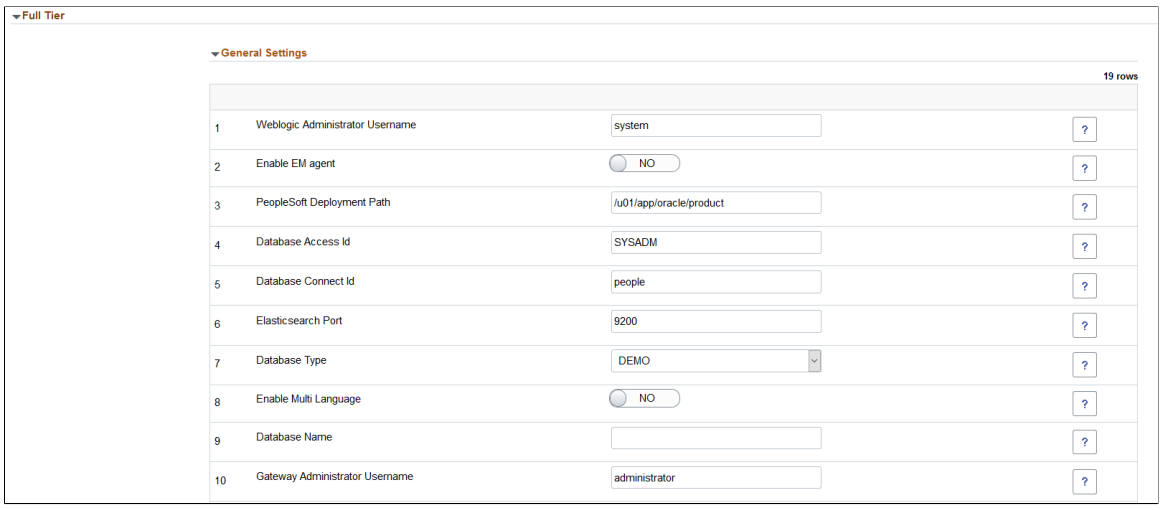
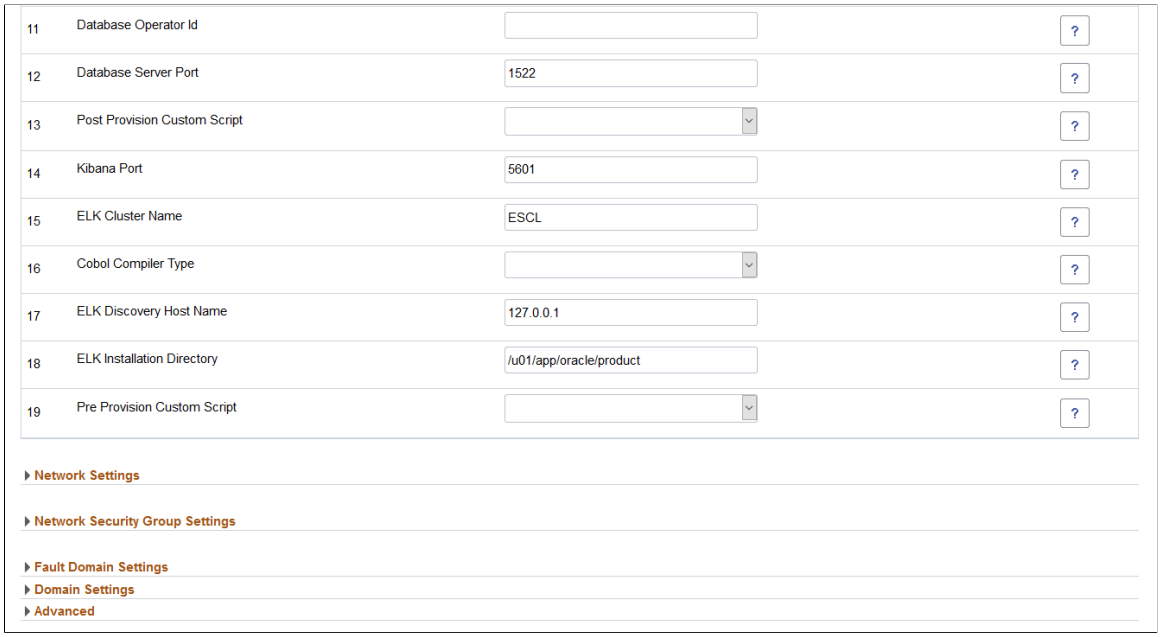


Image: Full Tier - General Settings (2 of 2)

This example illustrates the fields and controls on the Full Tier - General Settings (2 of 2). You can find definitions for the fields and controls later on this page.



Elasticsearch Port Elasticsearch port.

Weblogic Administrator Username User name of the Weblogic administrator. This is used for accessing WebLogic console.

PeopleSoft Deployment Path Location where the PeopleSoft application is deployed.

Database Access ID Access Id for the database.

Database Connect ID Connect Id for the database.

Enable EM Agent Select either Yes or No to enable or disable EM agent.

Elasticsearch Port Elasticsearch port.

Database Type Select the required database type. Available database types are DEMO or SYS.

Enable Multi Language Select either Yes or No to enable multi language support.

Database Name Name of the database.

Gateway Administrator Username User Id of gateway administrator.

Database Operator ID Database Operator ID.

Database Server Port Listener port number.

COBOL Compiler Type If COBOL is enabled in the selected topology, you must select the Cobol compiler type, Server Express or Visual COBOL.

Note: Server Express is not supported for PeopleTools 8.58 and onward.

Note: The COBOL license must be configured on the Cloud Manager Settings page. See Cloud Manager Settings Page

ELK Discovery Host Name	Host names for any nodes that are already members of a cluster. Host names (or IP/DNS) are required for letting each Elasticsearch server know where it can ping and find other Elasticsearch servers during booting up.
ELK Installation Directory	ELK Installation Directory
Pre Provision Custom Script	Select an uploaded script to execute prior to provisioning the environment. See Upload Custom Scripts Page
Post Provision Custom Script	Select an uploaded script to run post provisioning. See Upload Custom Scripts Page
Kibana Port	Kibana port.
ELK Cluster Name	ELK cluster name.

Domain Settings Section

Full tier includes Web Server, Appserver and Process Scheduler.

Web Server Settings	For Web Server setting see Configuring Web Server Tier Settings.
Appserver Setting	For App Server Setting see Configuring AppServer Tier Domain Settings.
Process Scheduler Settings	For Process Scheduler Setting see Configuring Process Scheduler Domain Settings.
Process Scheduler Server Definition Parameters	For Process Scheduler Setting see Configuring Process Scheduler General Setting.

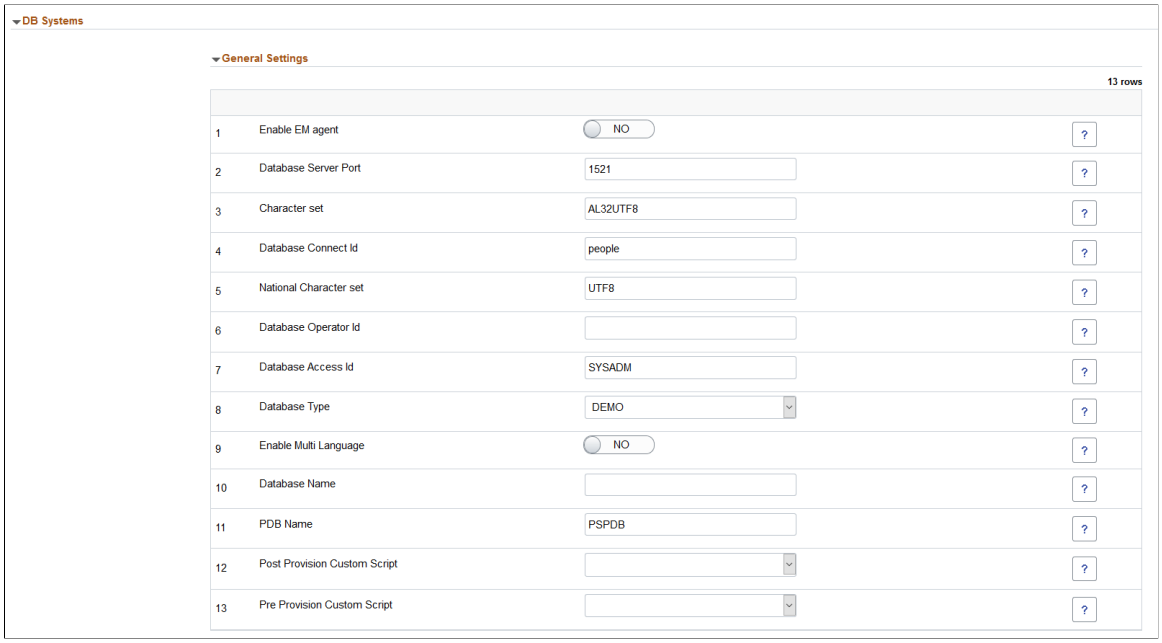
Configuring DB Systems Settings

DB Systems General Settings

The DB System options differ depending on whether the database system is on a VM, bare metal, or Exadata.

Image: DB Systems – General Settings

This example illustrates the fields and controls on the DB Systems – General Settings. You can find definitions for the fields and controls later on this page.



Enable EM Agent Select Yes to enable Environment Management agent for creating the infrastructure that is required to deploy an EM agent.

Database Server Port Listener port number.

Character Set The character set for the database.

Database Connect ID Access ID for the database.

National Character Set The national character set for the database.

Database Operator ID Default database operator ID.

Database AccessID Access ID for the database.

Database Type Select the required database type. Available database types are DEMO or SYS.

Enable Multi Language Select either Yes or No to enable multi language support.

Database Name Name of the database.

PDB Name Name of the Pluggable Database.

Pre Provision Custom Script Select an uploaded script to execute prior to provisioning the environment.

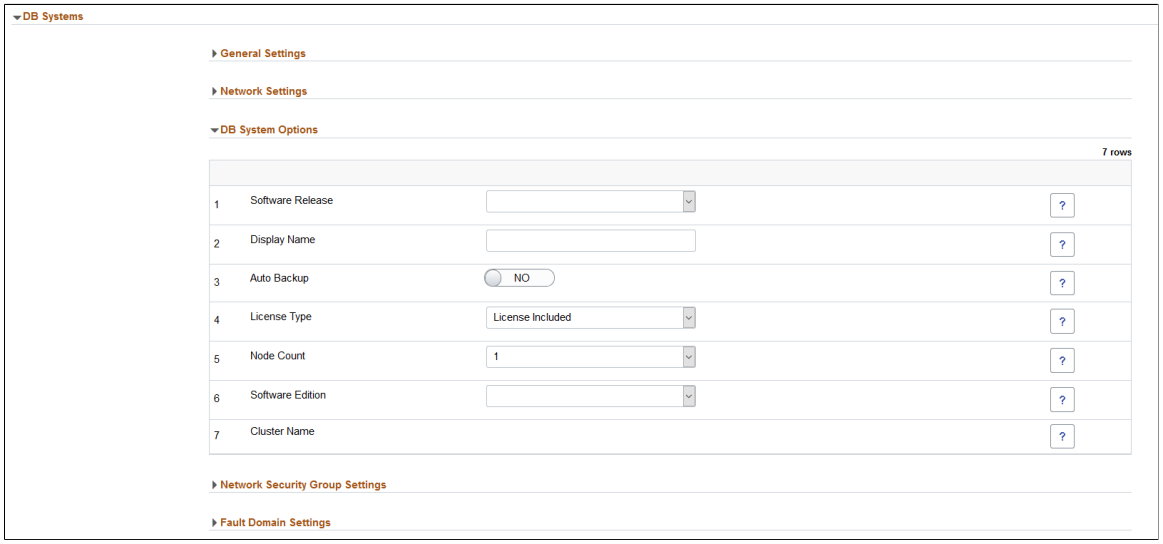
See Upload Custom Scripts Page

Post Provision Custom Script Select an uploaded script to run post provisioning.

See Upload Custom Scripts Page

Image: DB System Options section for VM

This example illustrates the fields and controls on the DB System Options section for VM. You can find definitions for the fields and controls later on this page.



Software Release

Oracle database release version. Select the software release from the drop down list.

Staring in Image 10, the following software releases are supported in DBS.

- 12.1
- 12.2
- 18c
- 19c

The database release version must be chosen based on the database version in PeopleSoft Image or customer's lifted database version.

Display Name

Display name for the DB system. The name doesn't need to be unique. An Oracle Cloud Identifier (OCID) will uniquely identify the DB system.

Auto Backup

Displays whether automatic incremental backups for this database is enabled or disabled.

License Type

The type of license you want to use for the DB system. Your choice affects metering for billing. License included means the cost of the cloud service includes a license for the Database service. Bring Your Own License (BYOL) means you are an Oracle Database customer with an Unlimited License Agreement or Non-Unlimited License Agreement and want to

use your license with Oracle Cloud Infrastructure. This removes the need for separate on-premise licenses and cloud licenses.

Node Count

The number of nodes in the DB system. The number depends on the shape you select. You can specify 1 or 2 nodes for virtual machine DB systems, except for VM.Standard2.1 and VM. Standard1.1, which are single-node DB systems.

Note: Some shapes may not be available in new tenancies.

Note: Except 1.1 and 2.1, all other shapes seem to be supported for RAC (2-node DB system).

Software Edition

The database edition supported by the DB system.

Cluster Name

A unique cluster name for a multi-node DB system. The name must begin with a letter and contain only letters (a-z and A-Z), numbers (0-9) and hyphens (-). The cluster name can be no longer than 11 characters and is not case sensitive.

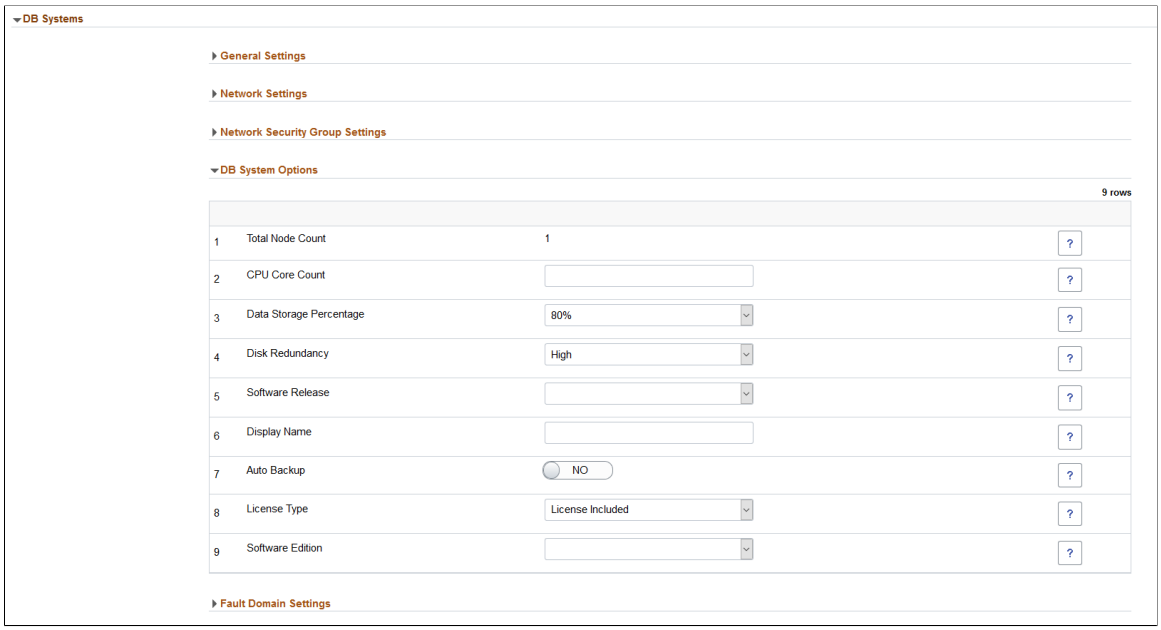
Fault domain

Select the fault domain for the database node, if the DB System contains 2 nodes, you will be able to configure the fault domain for each node.

Example Database Systems on Bare Metal

Image: DB System Options for Bare Metal

This example illustrates the fields and controls for DB System Options for Bare Metal . You can find definitions for the fields and controls later on this page.



Total Node Count

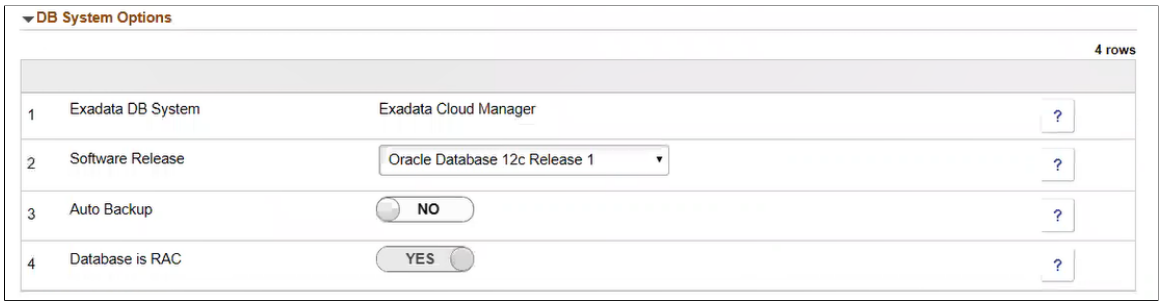
The number of nodes in the DB system. Only single node DB systems are supported for BM shapes.

CPU Core Count	Number of CPU cores enabled on the database system. Cloud Manager does not validate the core count, therefore you must use the correct core count for the BM shape selected in the topology configuration or the deployment may fail.
Data Storage Percentage	Percentage assigned to DATA storage including user data and database files. The remaining percentage is assigned to RECO storage including database redo logs, archive logs, and recovery manager backups. Accepted values are 40% and 80%.
Disk Redundancy	Type of redundancy configured for the database system. Normal is 2-way redundancy. High is 3-way redundancy. Allowed values are High and Normal
Software Release	Oracle database release version. The database release version must be chosen based on the database version in PeopleSoft Image or customer's lifted database version.
Display Name	Display name for the DB system. The name doesn't need to be unique. An Oracle Cloud Identifier (OCID) will uniquely identify the DB system.
Auto Backup	Displays whether automatic incremental backups for this database is enabled or disabled.
License Type	The type of license you want to use for the DB system. Your choice affects metering for billing. License included means the cost of the cloud service includes a license for the Database service. Bring Your Own License (BYOL) means you are an Oracle Database customer with an Unlimited License Agreement or Non-Unlimited License Agreement and want to use your license with Oracle Cloud Infrastructure. This removes the need for separate on-premise licenses and cloud licenses.
Software Edition	The database edition supported by the DB system.
Fault Domain	Select the fault domain for the database node, if the DB System contains 2 nodes, you will be able to configure the fault domain for each node.

Example Database System on Exadata

Image: Database System Options on Exadata

This example illustrates the fields and controls on the database system options on Exadata. You can find definitions for the fields and controls later on this page.



Exadata DB System Displays a list of Exadata DB systems that are available in your availability domain. If there is only one Exadata DB System, the value is auto-populated.

Software Release Oracle database release version. The database release version must be chosen based on the database version in PeopleSoft Image or customer's lifted database version.

Auto Backup Displays whether automatic incremental backups for this database is enabled or disabled.

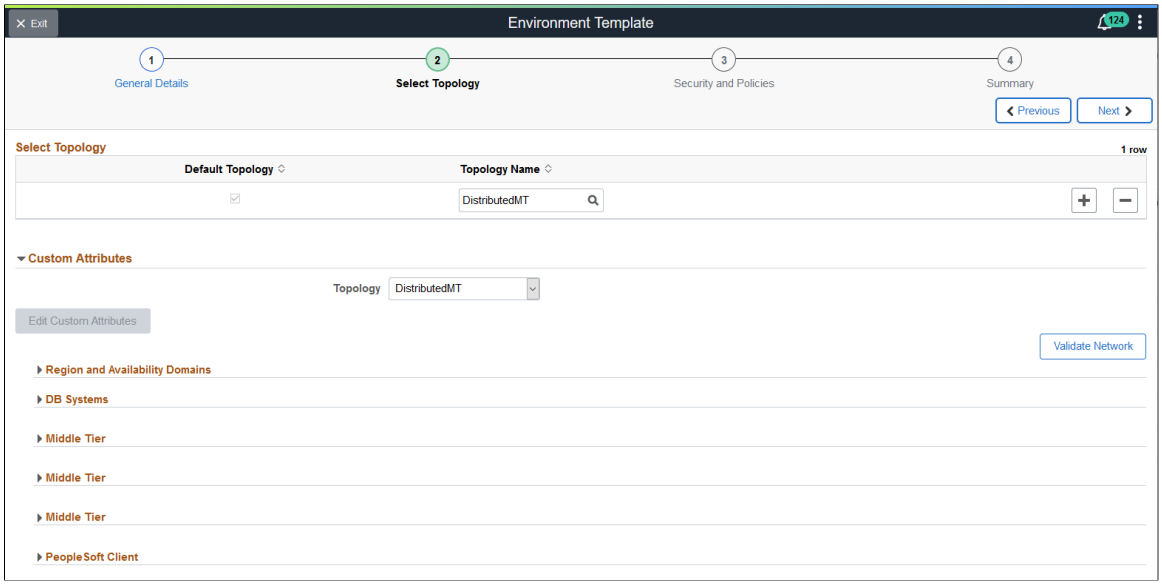
Database is RAC Displays whether database is RAC.

Configuring Distributed Middle Tier Environment Template Settings

For templates using a topology with multiple middle tiers, you will configure the custom attributes for each middle tier.

Image: Custom Attributes section

This example illustrates the fields and controls on the Custom Attributes section showing multiple middle tiers.

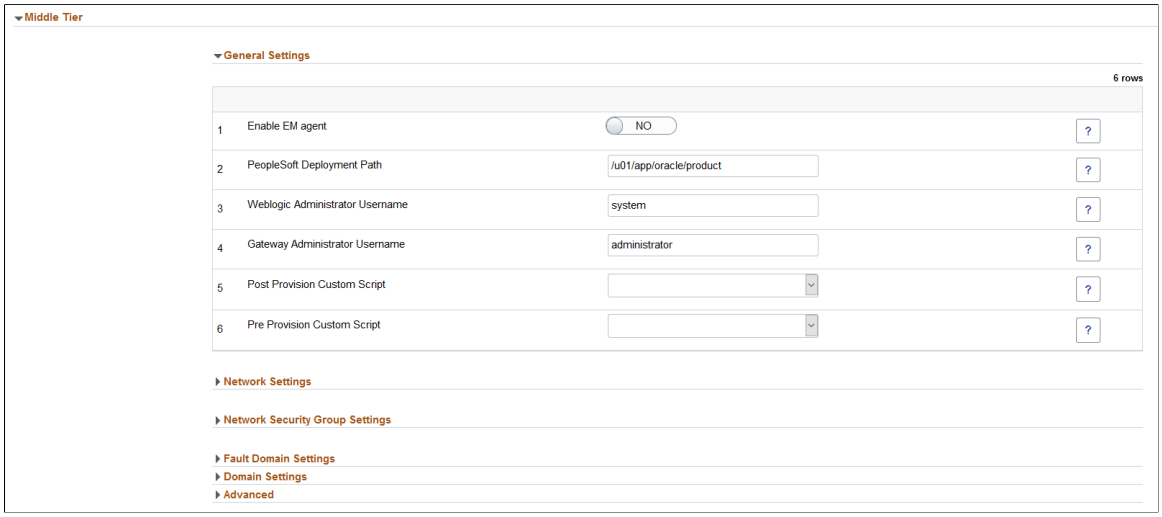


Configuring Web Server Tier Settings

General Settings

Image: Middle Tier - General Settings for Web Server

This example illustrates the fields and controls on the Middle Tier - General Settings for Web Server. You can find definitions for the fields and controls later on this page.



Enable EM Agent Select either Yes or No to enable or disable EM agent.

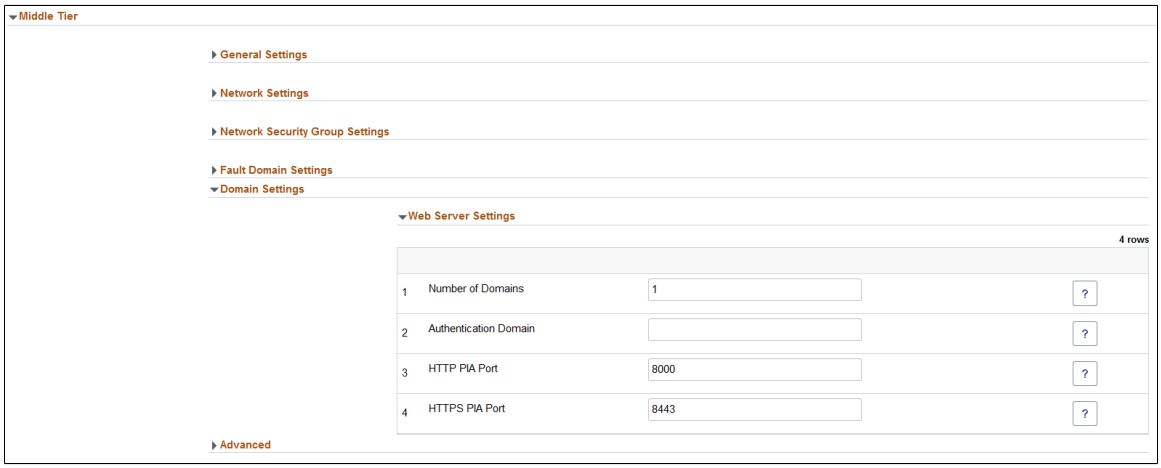
Weblogic Administrator Username User name of the Weblogic administrator. This is used for accessing the Weblogic console.

PeopleSoft Deployment Path	Location where the PeopleSoft application is deployed.
Gateway Administrator Username	User Id of gateway administrator.
Pre Provision Custom Script	Select an uploaded script to execute prior to provisioning the environment. See Upload Custom Scripts Page
Post Provision Custom Script	Select an uploaded script to run post provisioning. See Upload Custom Scripts Page

Domain Settings

Image: Middle Tier - Domain Settings for Web Server

This example illustrates the fields and controls on the Middle Tier - Domain Settings for Web Server. You can find definitions for the fields and controls later on this page.

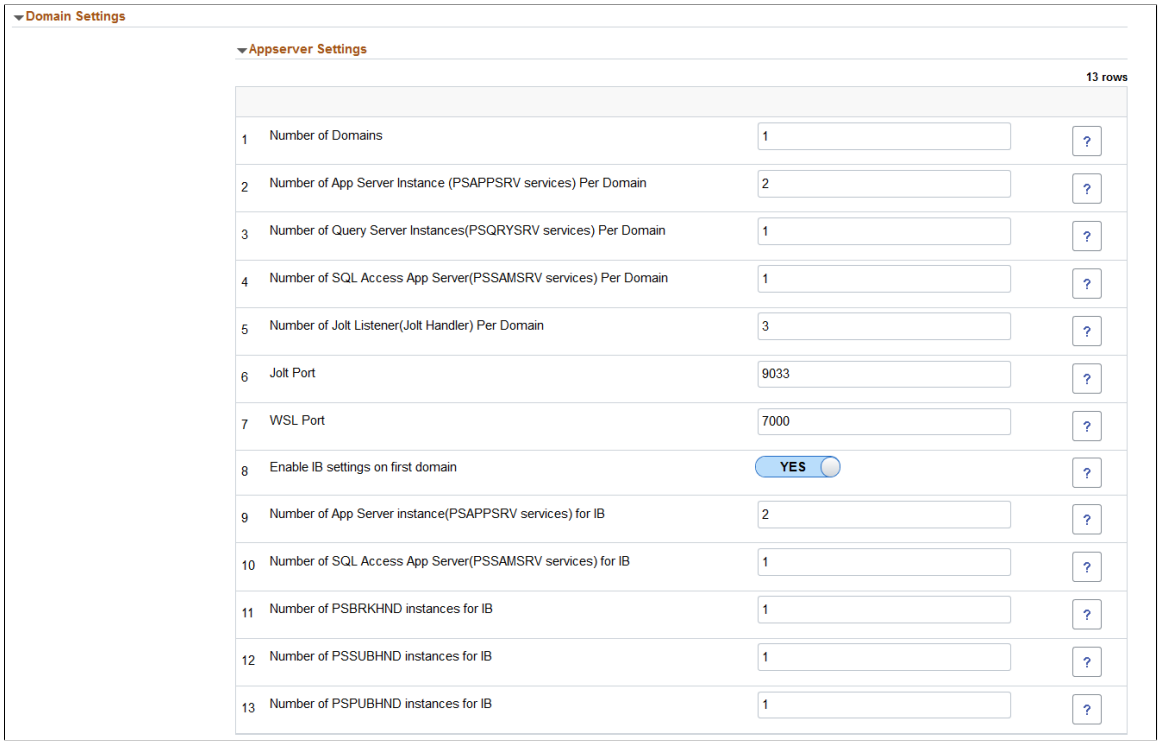


Number of Domains	Enter the number of web server domains. Number of domains can be 1 to 5.
Authentication Domain	The domain in which the portal is running and across which the single sign-on authentication token is valid.
HTTP PIA Port	There will be as many ports, equal to the given number of domains, separated by comma.
HTTPS PIA Port	There will be as many ports, equal to the given number of domains, separated by comma.

Configuring AppServer Tier Domain Settings

Image: Domain Settings for Appserver

This example illustrates the fields and controls on the Domain Settings for Appserver. You can find definitions for the fields and controls later on this page.



Number of Domains Number of application server domains. Number of domains can be 1 to 5.

Number of App Server Instance Per Domain Number of PSAPPSRV instances required. This configuration is applied to all App Server domains.

Number of Query Server Instances Per Domain Number of PSQRYSRV instances required. This configuration is applied to all App Server domains.

Number of SQL Access App Server(PSSAMSRV) Per Domain Number of PSSAMSRV instances required. This configuration is applied to all App Server domains.

Number of Jolt Listener per Domain Number of Jolt Listener per Domain.

Jolt Port There will be as many ports, equal to the given number of domains, separated by comma.

WSL Port There will be as many ports, equal to the given number of domains, separated by comma.

Enable IB Domain on first Domain If Yes is selected IB will be enabled in the first App Domain.

Number of App Server Instance (PSAPPSRV services) for IB Number of App Server Instance (PSAPPSRV services) for IB.

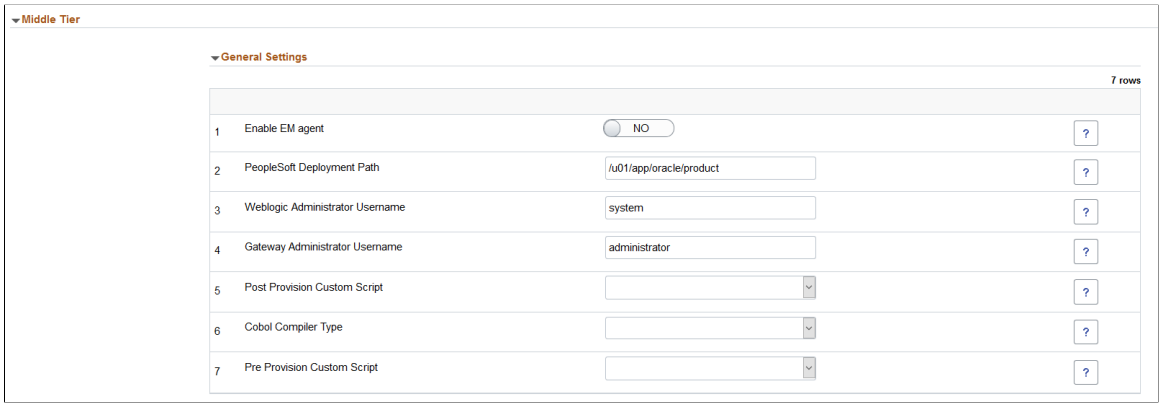
Number of SQL Access App Server (PSSAMRSRV services) for IB	Number of SQL Access App Server (PSSAMRSRV services) for IB
Number of PSBRKHND instances for IB	Number of PSBRKHND instances for IB
Number of PSSUBHND instances for IB	Number of PSSUBHND instances for IB
Number of PSPUBHND instances for IB	Number of PSPUBHND instances for IB

Configuring Process Scheduler General Setting

If the middle tier is Process Scheduler and COBOL is enabled in the topology, the General Setting will include COBOL Complier Type.

Image: Process Scheduler Middle Tier - General Settings

This example illustrates a Process Scheduler middle tier node, where COBOL is enabled in the topology.



COBOL Compiler Type If COBOL is enabled in the selected topology, you must select the COBOL compiler type, Server Express or Visual COBOL.

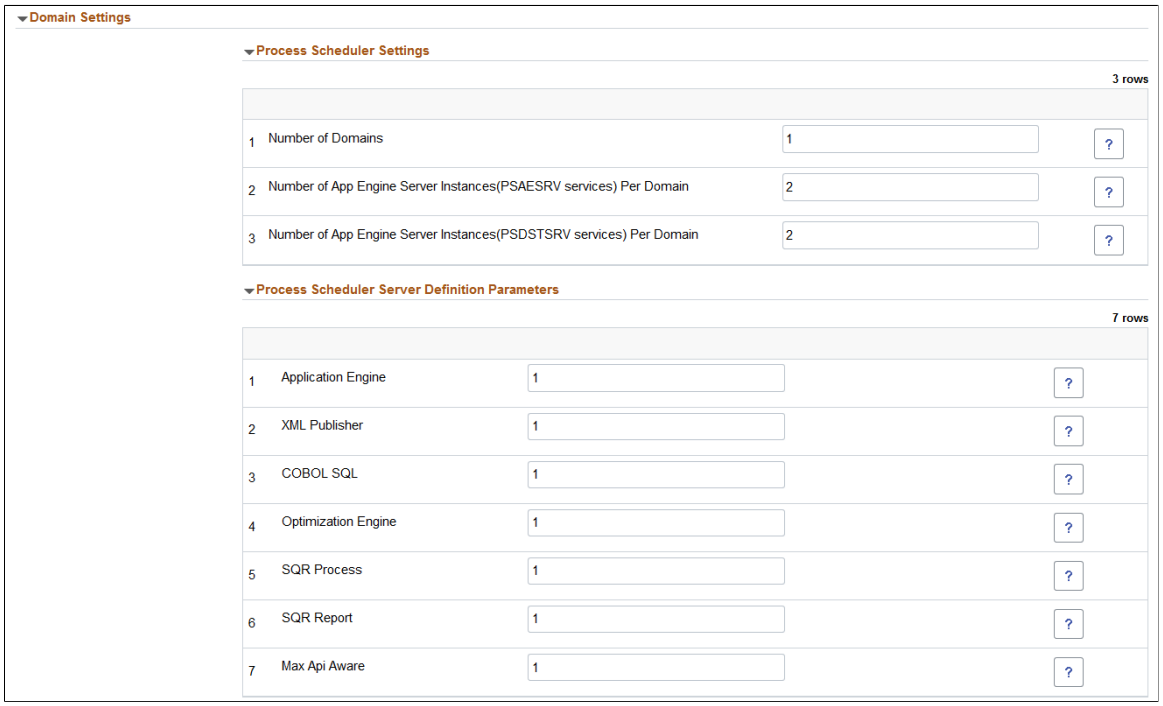
Note: Server Express is not supported for PeopleTools 8.58 onwards.

Note: The COBOL license must be configured on the Cloud Manager Settings page. See Cloud Manager Settings Page

Configuring Process Scheduler Domain Settings

Image: Domain Settings for Process Scheduler Settings and Process Scheduler Server Definition Parameters

This example illustrates the fields and controls on the Domain Settings for Process Scheduler Settings and Process Scheduler Server Definition Parameters. You can find definitions for the fields and controls later on this page.



Process Scheduler Settings

Number of Domains Number of process scheduler domains.

Number of App Engine Server Instances(PSAESRV services) Per Domain Number of application engines required.

Number of App Engine Server Instances(PSDSTSRV services) Per Domain Number of application servers required.

Process Scheduler Server Definition Parameters

Application Engine Number of application engine processes.

XML Publisher Number of XML publishers.

COBOL SQL Number of COBOL SQL processes.

Optimization Engine Number of optimization engines.

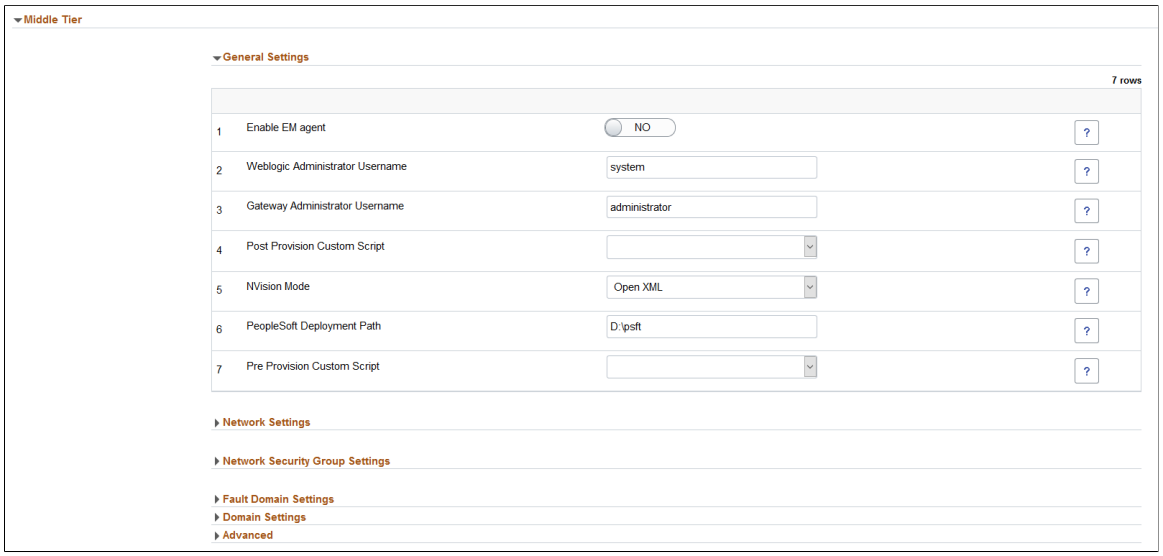
SQR Process Number of SQR processes.

SQR Report	Number of SQR reports.
Max Api Aware	Number of Max Api Aware.

Configuring Windows Middle Tier General Settings

Image: General Settings for Windows Middle Tier

This example illustrates the fields and controls on the General Settings for Windows Middle Tier. You can find definitions for the fields and controls later on this page.



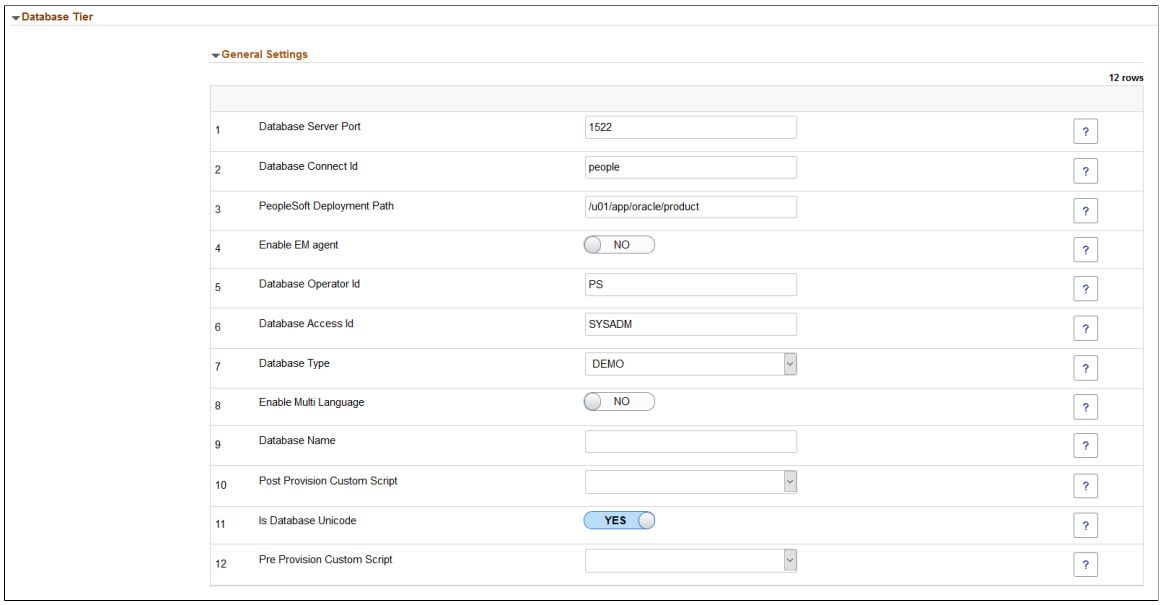
Enable EM Agent	Select either Yes or No to enable or disable EM agent.
WebLogic Administrator Username	User name of the WebLogic administrator. This is used for accessing WebLogic console.
Gateway Administrator Username	User ID of Gateway.
Pre Provision Custom Script	Select an uploaded script to execute prior to provisioning the environment. See Upload Custom Scripts Page
Post Provision Custom Script	Select an uploaded script to run post provisioning. See Upload Custom Scripts Page
NVision Mode	Select either OpenXML or Excel.
PeopleSoft Deployment Path	Location where the PeopleSoft application is deployed.

Configuring Database Tier

The database tier includes general settings and subnet settings.

Image: Database Tier – General Settings

This example illustrates the fields and controls on the Database Tier – General Settings. You can find definitions for the fields and controls later on this page.



Database Server Port Listener port number.

Database Connect ID Connect Id for the database.

PeopleSoft Deployment Path Location where the PeopleSoft application is deployed.

Enable EM agent Select Yes to enable Environment Management agent for creating the infrastructure that is required to deploy an EM agent.

Database Operator ID Default database operator ID.

Database Access ID Access ID for the database.

Database Type Select the required database type. Available database types are DEMO or SYS.

Enable Multi Language Select either Yes or No to enable multi language support.

Database Name Name of the database.

Pre Provision Custom Script Select an uploaded script to execute prior to provisioning the environment.

See Upload Custom Scripts Page

Post Provision Custom Script Select an uploaded script to run post provisioning.

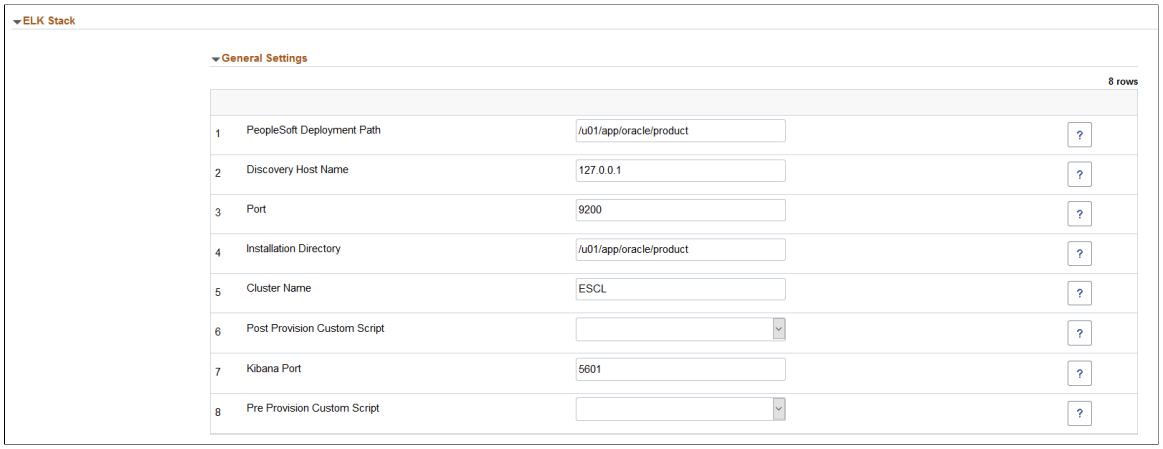
See Upload Custom Scripts Page

Is Database Unicode Select either Yes or No.

Configuring ELK Stack General Settings

Image: General Settings for ELK Stack Tier

This example illustrates the fields and controls on the General Settings for ELK Stack Tier. You can find definitions for the fields and controls later on this page.



Cluster Name The name of the Elasticsearch cluster.

PeopleSoft Deployment Path Location where the PeopleSoft application is deployed.

Discovery Host Name The host name for any nodes that are already members of a cluster.

Port Elasticsearch port.

Installation Directory The path to install Elasticsearch and/or Kibana.

Pre Provision Custom Script Select an uploaded script to execute prior to provisioning the environment.

See Upload Custom Scripts Page

Kibana Port Kibana port

Post Provision Custom Script Select an uploaded script to run post provisioning.

See Upload Custom Scripts Page

Environment Template – Security and Policies Page

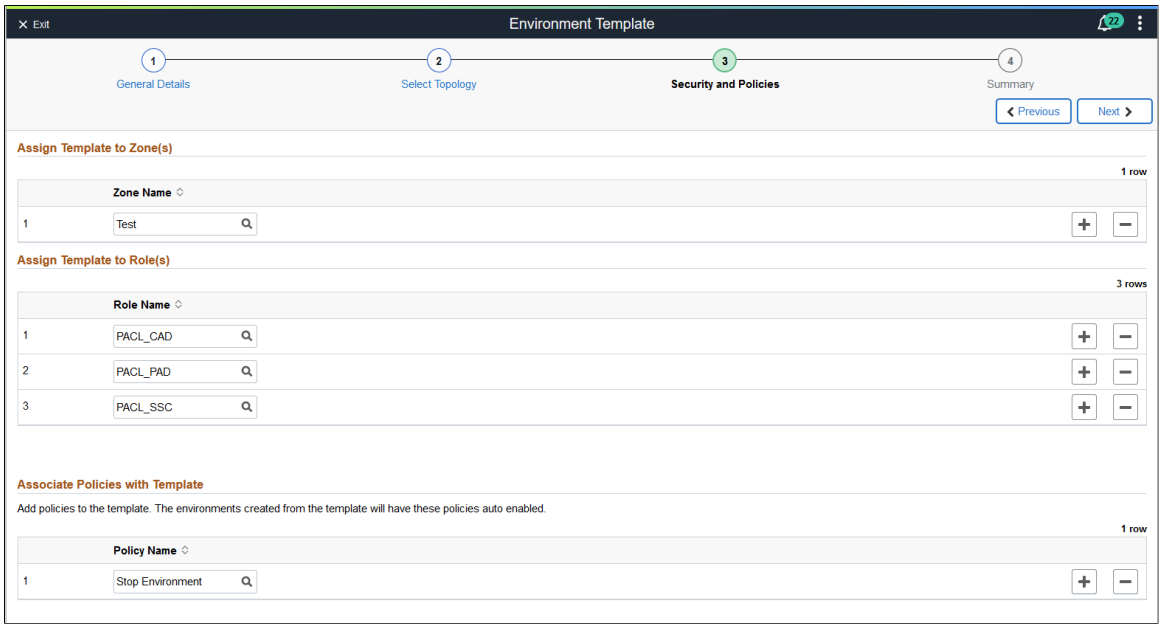
Use the Environment Template – Security and Policies page to associate the zone in which the environment is created, the role that will have access to the template and policies associated with the template.

Navigation

- Click Next on the Select Topology step.
- Click Step 3, Security and Policies, at the top of the page to navigate to the Environment Template – Security and Policies page in the guided process.

Image: Environment Template – Security and Policies page

This example illustrates the fields and controls on the Environment Template — Security and Policies page. You can find definitions for the fields and controls later on this page.



Zone Name Indicates the zone in which the environment is created.

Role Name Indicates the roles that have access to the template for creating environments. Only the users belonging to the role specified will be able to access the template while creating environment.

The delivered Cloud Manager roles are:

- Cloud Administrator (PACL_CAD)
- Cloud PeopleSoft Administrator (PACL_PAD)
- Self-Service User (PACL_SSC)

Policy Name Select policies for this template. The environments created from the template will have these policies auto enabled.

See Using Policy Editor.

Environment Template – Summary Page

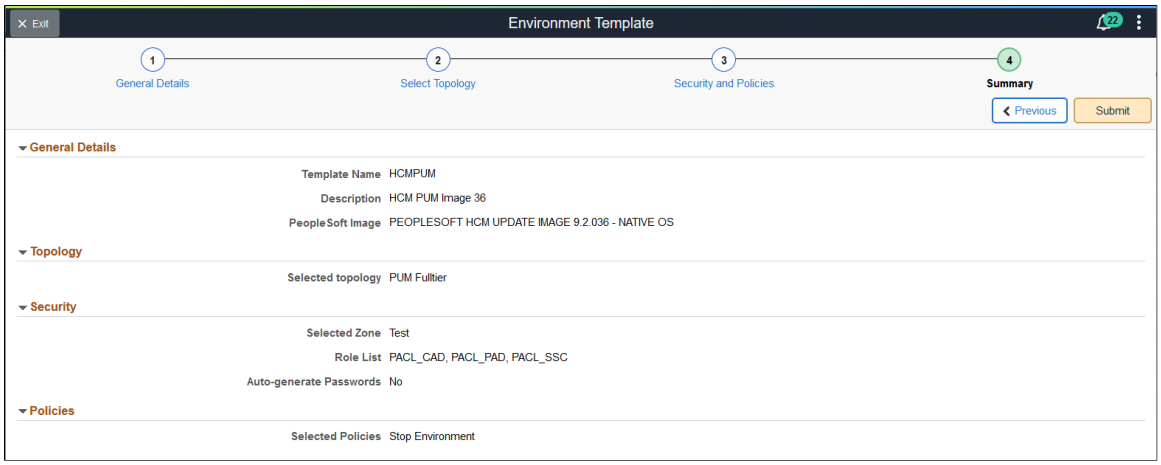
Use the Environment Template – Summary page (ECL_TEMPL_REV_FL) to review and submit the template details.

Navigation

- Click Next on the Security and Policies step.
- Click step 4, Summary, at the top of the page to navigate to the Environment Template – Summary page in the guided process.

Image: Environment Template – Summary page

This example illustrates the fields and controls on the Environment Template – Summary page. You can find definitions for the fields and controls later on this page.



The details provided in all the pages in the Environment Template wizard is displayed here.

Submit Click this button to submit the details for template creation.

Managing Environments

Cloud Manager provisions PeopleSoft environments on-demand with just a few clicks. The entire provisioning process is automated. At the end of provisioning, a ready-to-use environment is available within a short time. The environments can be created by a three step process:

1. Create Topology
2. Create Template
3. Create Environment

Note: Prior to creating an environment, ensure that the required DPKs are already downloaded in the Repository.

An administrator defines a template for creating an environment. The topology is encapsulated inside the template. Users can select a template, override topologies, change any attributes, if needed and provision PeopleSoft environments on demand.

Users are allowed to perform actions on a running environment, such as stop, view details, create new template from it, and so on. For details, see the Actions on the Environment section under the Create Environment Page.

Note: Also, you must ensure to tune the servers, database, and PeopleSoft system for optimum performance once the deployment is completed.

Pages Used to Manage Environments Tile as an Administrator

Page Name	*Definition Name*	*Usage*
Environments Tile	ECL_ENVPROV_FL_GBL (CREF for tile)	Access the Environments landing page.
Environments Page	ECL_ENVPRO_FL	Access the Environments landing page.
Create Environment Page	ECL_ENV_ADD_SCF	Create a new environment.
Environment Details Page	ECL_ENV_DET_FL	Access more details of the environment from one location.
Manage Attributes Page	ECL_ENV_RESET_FL	Update Cloud Manager with environment attributes, if a user modifies it outside Cloud Manager.
Manage PUM Connections Page	ECL_SA_MANAGEPM_FL	Manage PUM connections.
Apply PeopleTools Patch Page	ECL_ENV_PTCHUPD_FL	Apply latest patches.
Upgrade PeopleTools Page	ECL_ENV_UPGD_FL	Update PeopleTools version (major version changes).
Policies Page	ECL_POLICY_ENVS	Associate policies with the environment name.
Logs Page	ECL_ESEARCH_FL	View logs of all operations such as create, delete, actions performed on the environment, and the like.

Environments Tile

Use Environments tile (ECL_ENVPROV_FL_GBL) to access the Environments landing page.

Navigation

The the Environments tile is delivered as part of the Cloud Manager home page.

Image: Environments tile

This example illustrates the Environments tile.

Environments Page

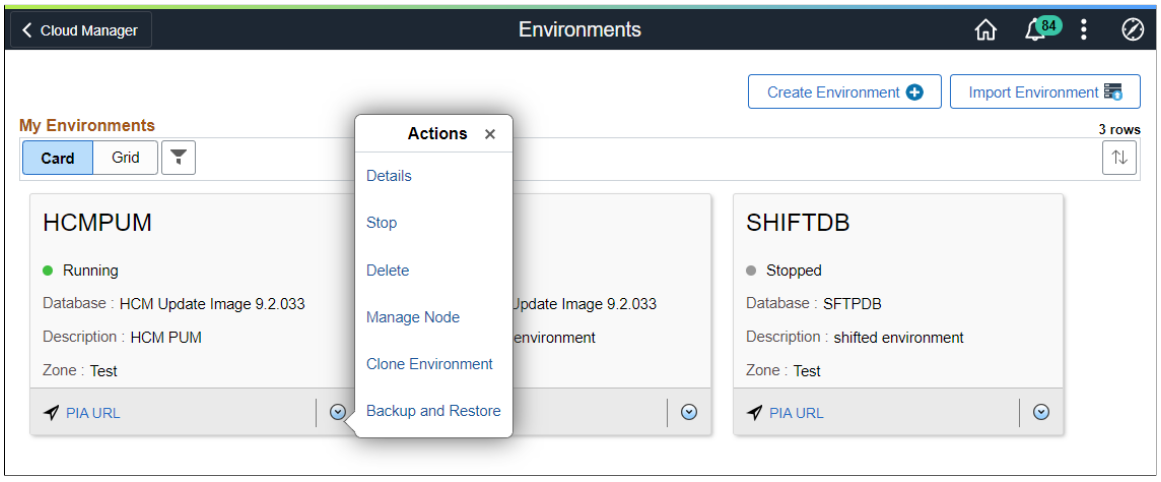
Use the Environments page (ECL_ENVPRO_FL) to access the Environments landing page.

Navigation

Click the Environment tile on the delivered Cloud Manager Fluid home page. The Environments page is displayed.

Image: Environments page

This example illustrates the fields and controls on the Environments page. You can find definitions for the fields and controls later on this page.



Name Name of the environment.

Note: Length of Environment name and identity domain name should not exceed 20 characters in OCI.

Status Status of the environment provisioned through Cloud Manager.

The different statuses associated with the environment are:

	• Initiating • Provisioning • Failed • Stopping • Starting • Running • Deleting • Applying PeopleTools Patch. • Upgrading PeopleTools. • Refreshing • Restoring • Infra Creation Complete
Description	Description of the environment.
Zone	Zone in which the environment is deployed.
PIA URL	Indicates the URL used to connect to the provisioned environment.
Create Environment button	Click this button to access the Create Environment page, where you can create new environments.
Related Actions button	Click this button to perform different actions for managing the environment as a whole. .
Import Environment button	Click this button to import a database system environment. See Importing Environment

Actions on the Environment

You can perform a variety of actions on the environment by using the Related Actions button corresponding to each environment. The actions can be:

- Details: Select this option to view environment details and to perform additional actions on the environment such as performing a health check, applying a PeopleTools patch, viewing logs, and managing PUM connections.
- Start: Select this option to start all the instances and then all the domains within them.
- Stop: Select this option to stop all domains and shutdown all the instances. In case of database, only compute database instances are shutdown.
- Delete: Select this option to remove the environment.

- Manage Node: Select this option to scale environment up or down.
- Clone Environment: Select this option to clone an existing environment.
- Refresh: Select this option to refresh the database or the database, ps app home and ps cust home.

  This option is only available for DBaaS environments.
- Backup and Restore: Select this option to backup or restore an environment.
- Deploy: Select this option to continue deploying an environment that has paused after infrastructure creation.

Create Environment Page

Use the Create Environment page (ECL_ENV_ADD_SCF) to create a new environment.

Important! Before creating an environment in OCI, ensure that the template is updated with OCI-specific Infrastructure Settings such as region, compartment, VCN and subnet settings.

Note: Deploying a PI image requires a Windows image which is updated with latest Windows updates and patches must be used. If the Windows image is not on the latest updates and patches the provisioning of PeopleSoft Client will fail. Refer to the OBE. Install Cloud Manager tutorials on Oracle Learning Library.

Navigation

Click the Create Environment button on the Environments landing page.

Image: Create Environment page

This example illustrates the fields and controls on the Create Environment page. You can find definitions for the fields and controls later on this page.

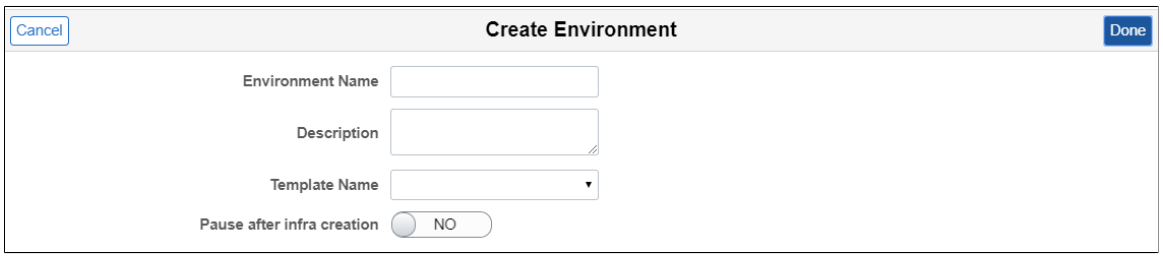
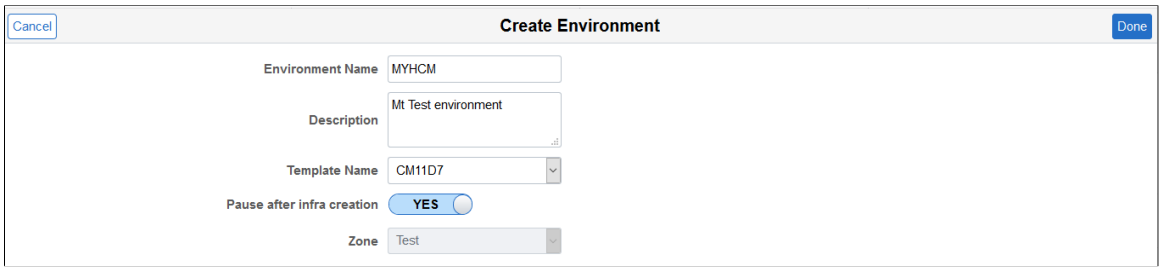


Image: Create Environment page with Pause after infra creation selected

This example illustrates the fields and controls on the Create Environment page when Pause after infra creation is selected. You can find definitions for the fields and controls later on this page



Environment Name

Name of the environment that you want to create.

Note: Length of environment name must not exceed 20 characters in OCI.

Description

Description for the environment that you want to create.

Template Name

Select a template and the zone. On selecting the template, zone options are automatically displayed.

For details on templates, see the Creating a Template section under Environment Template Page.

Pause after infra creation

Select Yes for the environment provisioning to pause after completion of the Infrastructure task. This provides the user the opportunity to do additional setup, actions, or operations on the newly created environment outside of Cloud Manager before proceeding with the PeopleSoft deployment.

Note: When you are ready to proceed to the PeopleSoft deployment, select Deploy from the related actions on the Environment tile.

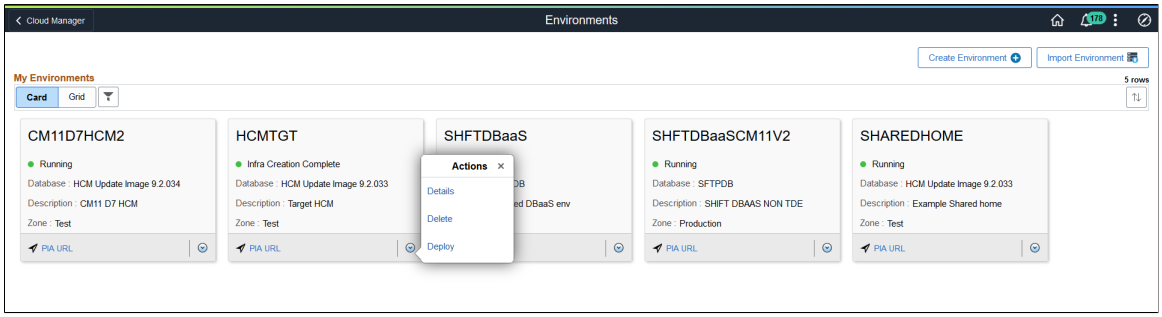
Select No (default) to continue provisioning the environment when the infrastructure layer is complete.

Zone

Select the zone for the environment. If only one zone was defined on the environment template used for this environment, it will be displayed as read-only.

Image: Deploy after Infra structure creation

This example illustrates the actions on the Environments page after Infra structure creation is complete.



Creating an Environment

Important! Before creating an environment in OCI, ensure that the template is updated with OCI-specific Infrastructure Settings such as region, primary availability domain, default compartment, default VCN, network settings, and network security group.

To create an environment:

1. Enter the required environment attributes and credentials.

   Note: Region and Availability Domains, Network Settings and Network Security sections are read only.

2. Click Done to start environment provisioning.

Alternately, you can override the default topology and environment attributes while environment provisioning.

The default database operator id for each PeopleSoft PUM instance is listed below:

- For HCM, default database operator id is PS.
- For FSCM, default database operator id is VP1.
- For CRM, default database operator id is VP1.
- For ELM, default database operator id is PS.
- For IH, default database operator id is VP1.
- For CS, default database operator id is PS.

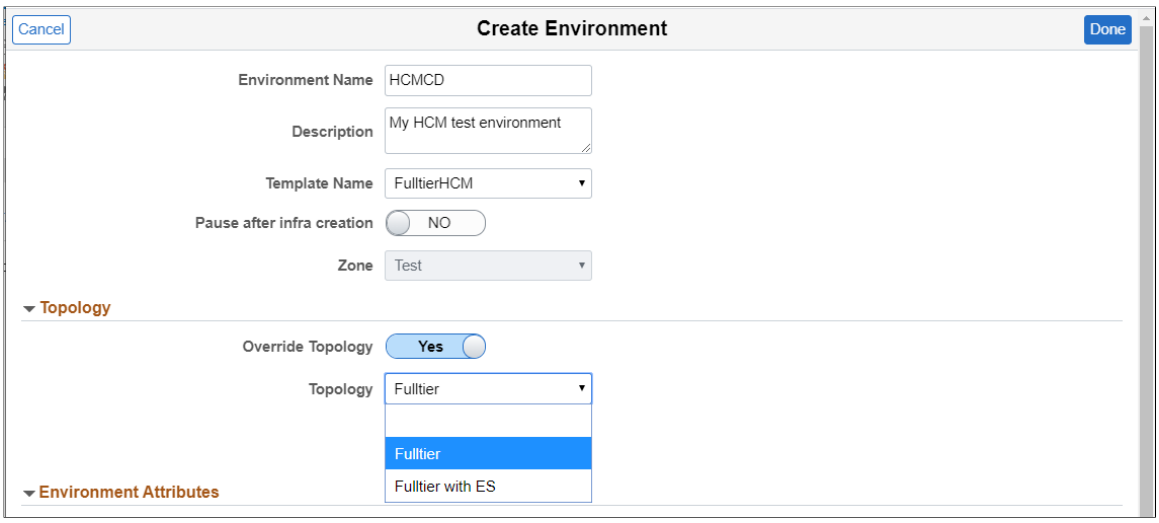
Overriding Default Topology and Attributes

If the template contains multiple topologies, you can override default topology and attributes. To override the topology:

1. Select Yes in Override Topology field.

Image: Create Environment — Override Topology field

This example illustrates the fields and controls in the Topology section of the Create Environment page.



2. Select an appropriate Topology. Corresponding description is displayed in the below text area.
3. Input the required environment attributes. The different attributes are:
    - Full Tier: Full Tier is the VM where application server domain, process scheduler domain, and the web server domain are installed.
    - Middle Tier: Middle Tier Node can be created in either Linux or Windows. The Linux the Middle Tier is the VM where application server domain, process scheduler domain, and the web server domain are installed. The Windows the Middle Tier is the VM where Windows process scheduler is installed.
    - Database Tier: Database tier is the VM where the database (non-DbaaS) is installed for the new PSFT system.
    - PeopleSoft Client: PeopleSoft Client is the VM where PeopleTools client (for example, pside) and change assistant are pre-installed.
    - Database as a Service: PeopleSoft database is deployed on DBaaS.
    - ELK Stack: ELK Stack Tier is the VM where Elasticsearch server and Kibana are installed.
4. Enter the PeopleSoft Client credentials and other required attributes.

Note: In case of OCI, the password for the PeopleSoft Client instance should meet the password complexity as per the OCI requirement.

Some custom attributes are displayed based on the selected topology nodes. If you select an Elasticsearch node, then you need to provide a couple of input parameters and passwords. Currently, if you are using the ELK DPK setup script for installing Elasticsearch, then system will not prompt for the admin and proxy user names. Therefore, it is always esadmin and people for admin and proxy

respectively. Password must be of at least 9 characters long and contain a numeric and one uppercase letter. Special characters are not accepted.

5. Click Done to start environment provisioning.

Note: Please ensure to tune the servers, database, and PeopleSoft system for optimum performance once the deployment is completed.

Accepting Licensing Agreement

If you selected to use the Linux Image from Marketplace and this is the first time you are provisioning an environment in a specific compartment, a License agreement will be displayed and must be accepted to continue. Each compartment needs to accept the license if it has not already been accepted for that compartment.

See Infrastructure Settings Page.

Using Shared File System for Linux Middle Tier using File Storage Service

Multiple middle tiers in an environment can share PS_HOME, PS_APP_HOME and PS_CUST_HOME.

Note: Shared File System is only supported for Linux middle Tier. Windows middle tier is not supported.

User must first create a new File Storage Service (FSS) in the OCI. It is recommended that this new FSS be in the same availability domain (AD) where the middle tier of the environment is provisioned.

Important! You should not use the File Storage System that you created for the Cloud Manager repository as the file system for a middle tier node in a provisioned environment.

When creating the FSS, keep the following in mind:

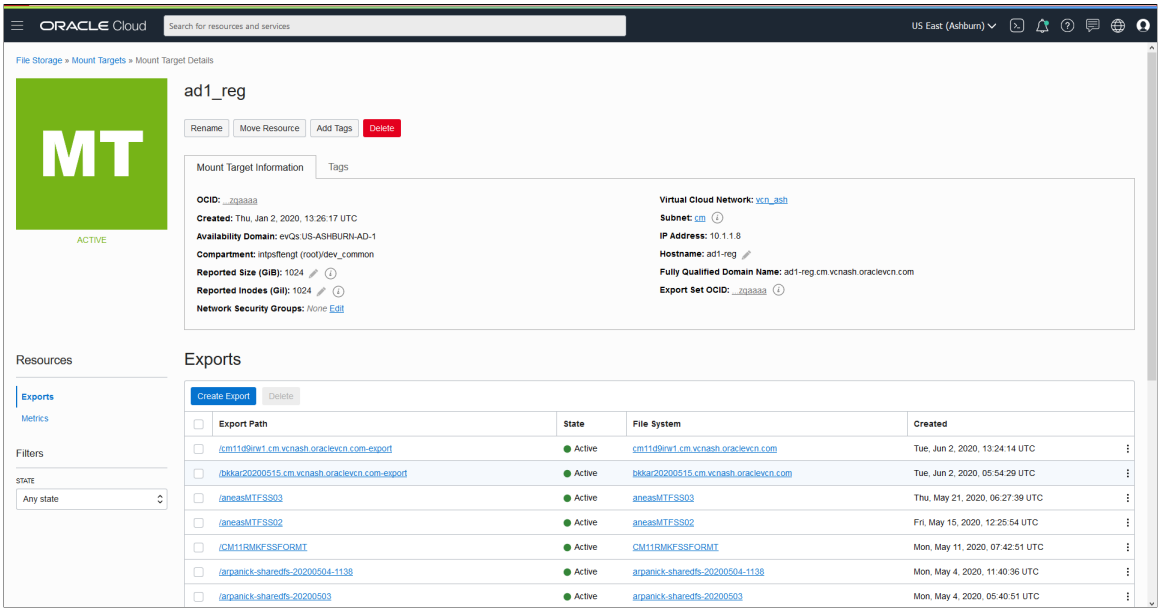
- All VMs in the subnet should have read/write access.

  See Plan the Virtual Cloud Network for PeopleSoft Cloud Manager (Optional)

- File storage mount target (TCP ports 111, 2048, 2049, 2050; UDP ports 111 and 2048) is specific to FSS ports, this has to be opened in Linux MT machines.
- FSS export path requires full read/write access.
- Network access (ports and security rules) must be configured to Mount Targets from the middle tier nodes.
- Mount Target must be a minimum of 1024 GB.

Image: Mount Target Details page

This example illustrates the fields and controls on the Mount Target Details page.



- Once the environment is running, user can update the FSS export path read/write permission to Linux Middle Tier.

  See Managing File Systems

Image: File System (Linux Midtier)

This example illustrates the fields and controls on the File System (Linux Midtier) section. You can find definitions for the fields and controls later on this page.

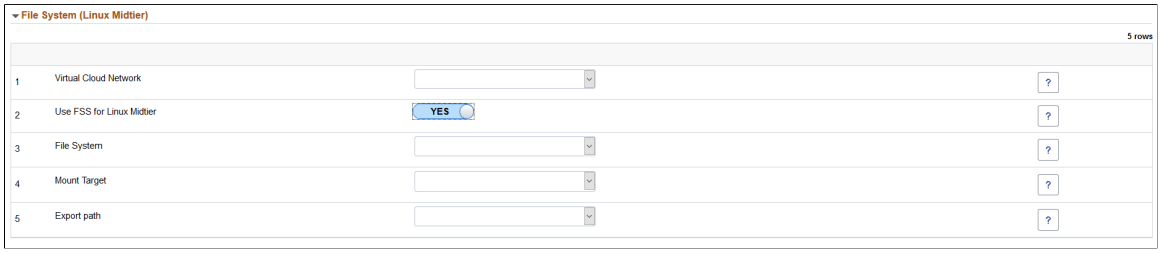
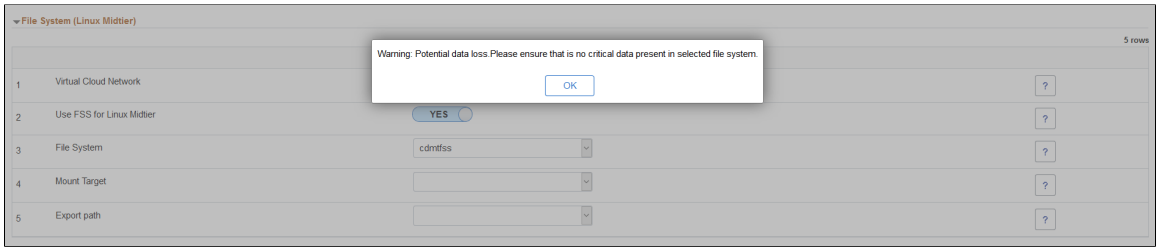


Image: File System warning message

This example illustrates the File System warning message.



Virtual Cloud Network Select the Virtual Cloud Network.

Use FSS for Linux Midtier	Select Yes to use FSS for Linux Midtier
File System	Select the File System from the available file systems in OCI. **Note:** When you tab off the field, a warning is displayed for potential loss of data. The file system should not contain any critical data.
Mount Target	Select the Mount Target from the drop down list.
Export path	Select the Export path from the drop down list.

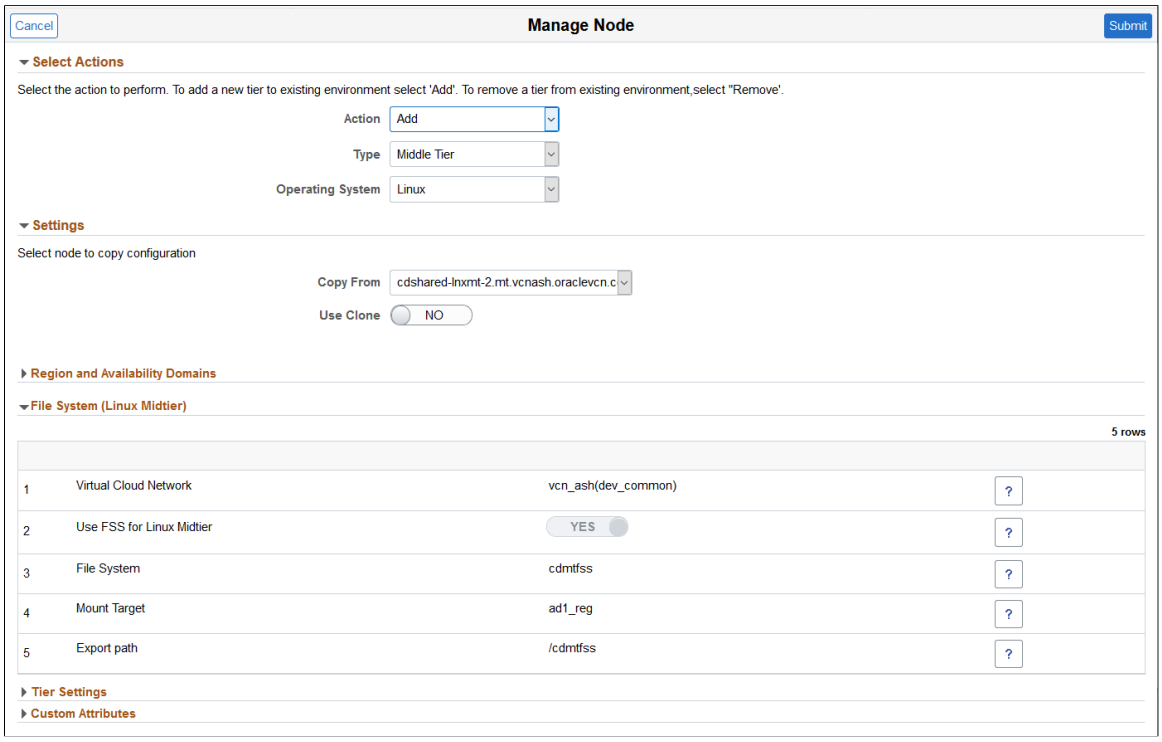
Adding a New Middle Tier

After creating an environment that shared file system, use the Manage Node action to add a new middle tier that will share the same PS_HOME, PS_APP_HOME and PS_CUST_HOME.

See Managing Nodes

Image: Manage Node page - Add Middle Tier with FSS

This example illustrates the fields and controls on the Manage Node page - Add Middle Tier with FSS.



Environment Details Page

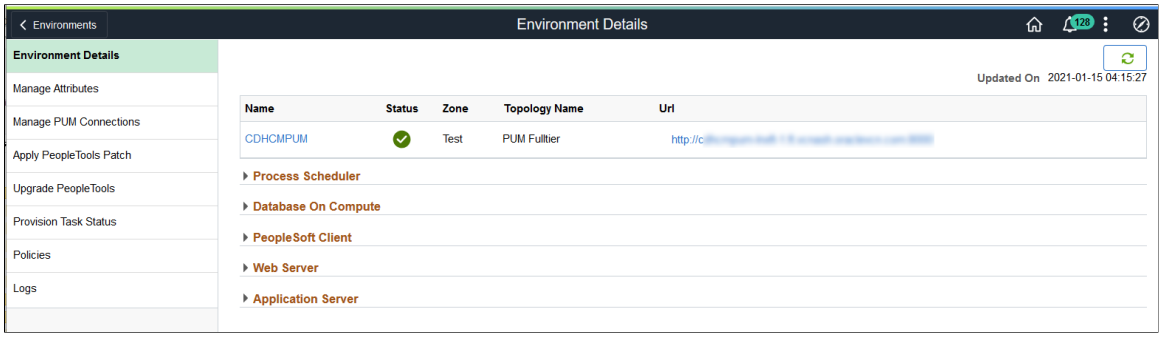
The Environment Details page (ECL_ENV_DET_FL) is a navigation collection that enables administrators to access more details of the environment from one location. It also enables the user to perform additional actions that can be performed on the environment such as performing applying a PeopleTools patch, viewing logs, and managing PUM connections.

Navigation

Click the Related Actions button corresponding to the environment. Select Details. The Environment Details page is displayed.

Image: Environment Details page

This example illustrates the fields and controls on the Environments Details Page. You can find definitions for the fields and controls later on this page.



Refresh button — Click the Refresh button, at the upper-right corner of the page, to fetch the current status of the environment.

Process Scheduler — This section provides details of the process scheduler component of the deployed PeopleSoft application environment. The Process Scheduler is responsible for processing scheduled tasks or jobs that typically do not happen during the course of a user's browser request.

Database on: Compute — This section provides details of the database server of the deployed PeopleSoft application environment. The PeopleSoft applications refers to Oracle PeopleSoft products such as PeopleSoft Customer Relationship Management (CRM), PeopleSoft Enterprise Learning Management (ELM), PeopleSoft Financials and Supply Chain Management (FSCM), PeopleSoft Human Capital Management (HCM), and PeopleSoft Interaction Hub.

Webserver — This section provides details of the web server component of the deployed PeopleSoft application environment.

Appserver — This section provides details of the application server component of the deployed PeopleSoft application environment. The application server acts as the business logic engine of the PeopleSoft system.

Database on: DBaaS — This section provides details of the database server of the deployed PeopleSoft application environment. The PeopleSoft applications refers to Oracle PeopleSoft products such as PeopleSoft Customer Relationship Management (CRM), PeopleSoft Enterprise Learning Management (ELM), PeopleSoft Financials and Supply Chain Management (FSCM), PeopleSoft Human Capital Management (HCM), and PeopleSoft Interaction Hub.

Note: The 'Database on: DBaaS' section is displayed only when a user selects 'Database as a Service' node in topology.

PeopleSoft Client

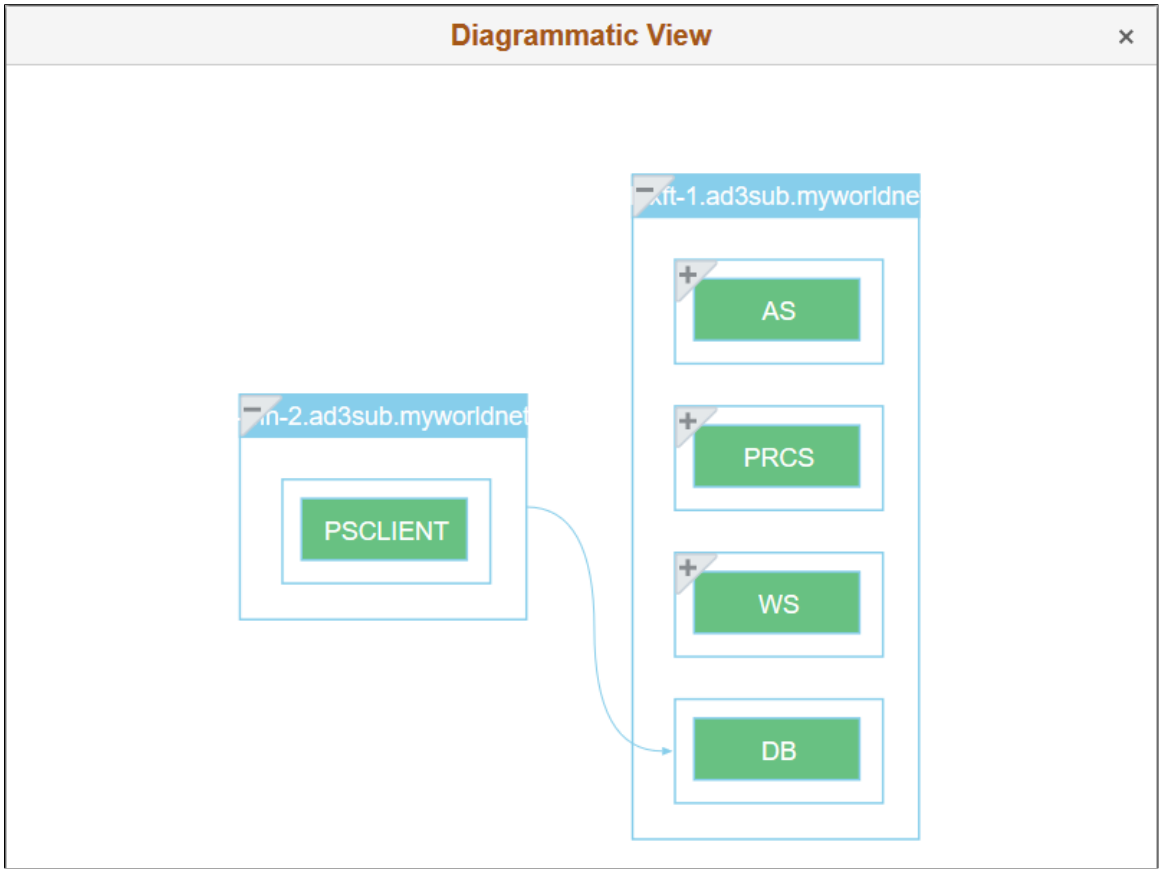
This section provides details of the Windows Client of the deployed PeopleSoft application environment. This is the Microsoft Windows virtual machine on which PeopleSoft Application Designer and PeopleSoft Change Assistant will be installed.

Note: To access PSIDE (PeopleSoft Application Designer) and Change Assistant applications for this environment, you need to RDP to Windows VM using the IP address or hostnames provided under the PeopleSoft Client section.

Click the environment name to view a diagrammatic representation of all the instances and domains running inside the VMs as shown.

Image: Diagrammatic View

This example illustrates the fields and controls on the Diagrammatic View page.

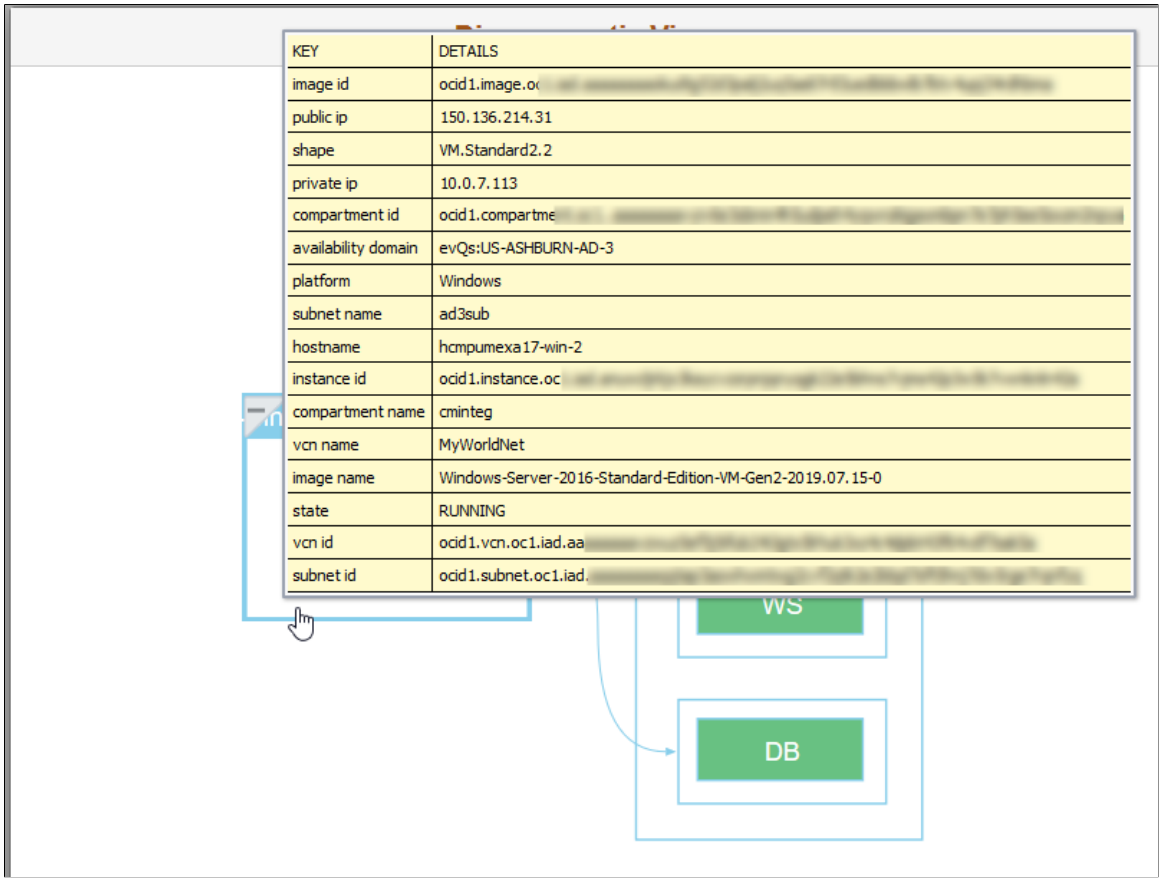


Hover the mouse over each instances for viewing the details.

You can view the status of different PeopleSoft services running within the VMs (application servers domains, process scheduler domains, web server domain, and the like) as shown:

Image: Diagrammatic View Instance Details

This example illustrates the fields and controls on the Diagrammatic View Instance Details page.



As an illustration, Process Scheduler domain details are described in the following section.

Process Scheduler Domain

This section provides details of the Process Scheduler component of the deployed PeopleSoft application environment. The Process Scheduler is responsible for processing scheduled tasks or jobs that typically do not happen during the course of a user's browser request.

Navigation

Expand Process Scheduler available on the Environment Details page.

Image: Process Scheduler Section

This example illustrates the fields and controls on the Process Scheduler section for Process Scheduler middle tier on Linux.

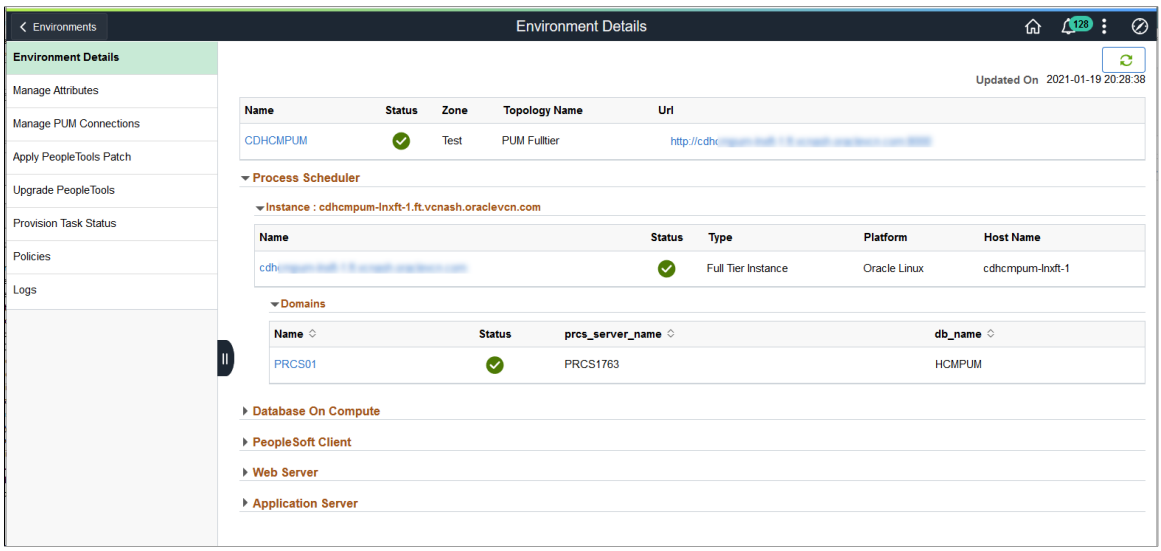
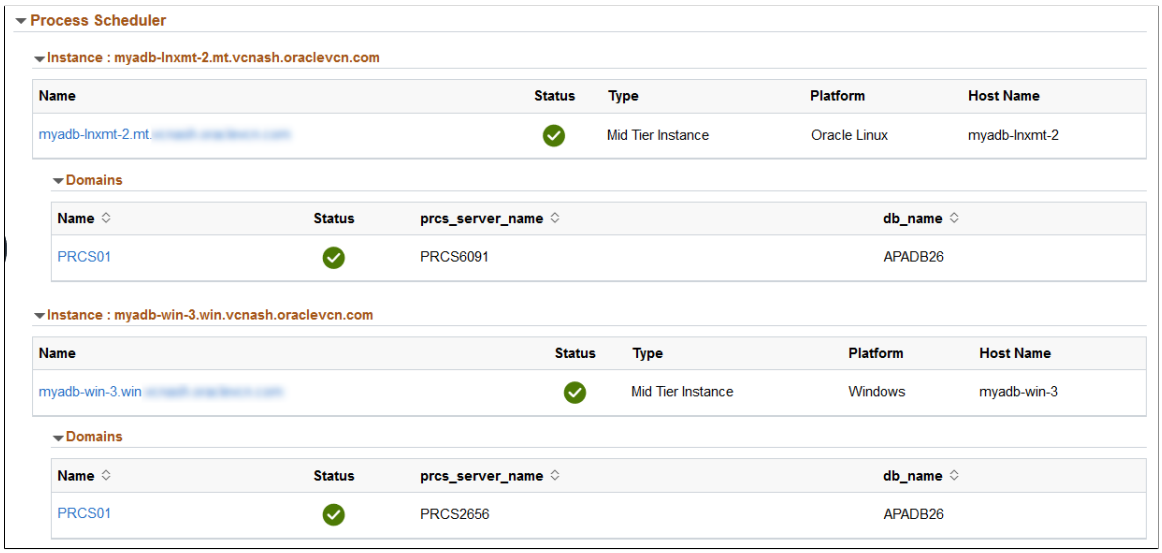


Image: Environment Details showing Process Scheduler section for a Windows instance

This is an example of where Process Scheduler was configured on a Windows instance.



Instance Details Modal Window

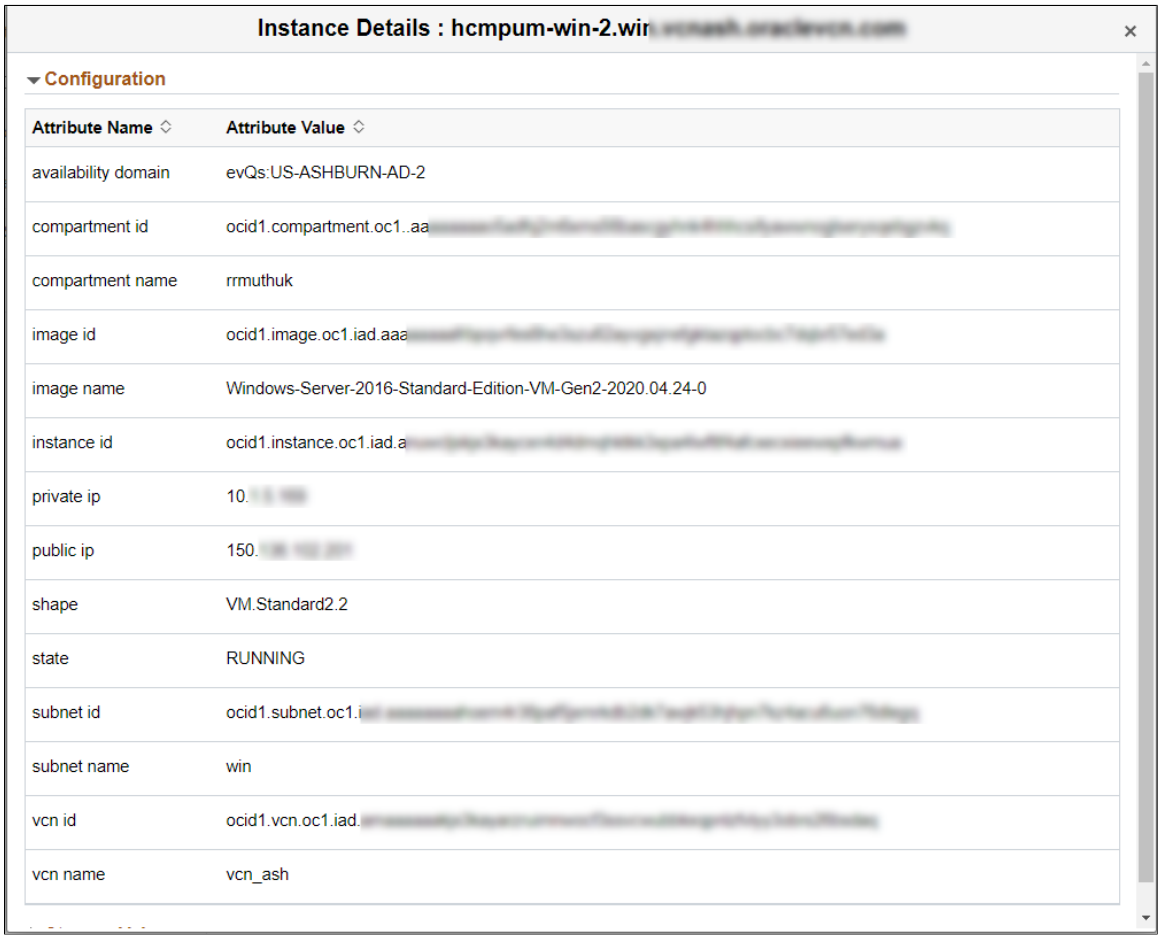
Use Instance Details modal window to view more details about the virtual machine.

Navigation

Click on the instance name.

Image: Instance Details Modal Window

This example illustrates the instance details for PeopleSoft Client.



Domain Details Modal Window

Use the Domain Details modal window to view domain details.

Navigation

Click on the domain name.

Image: Example Domain Details for Process Scheduler – Configuration

This example illustrates the configuration domain details for the Process Scheduler PRCS01.

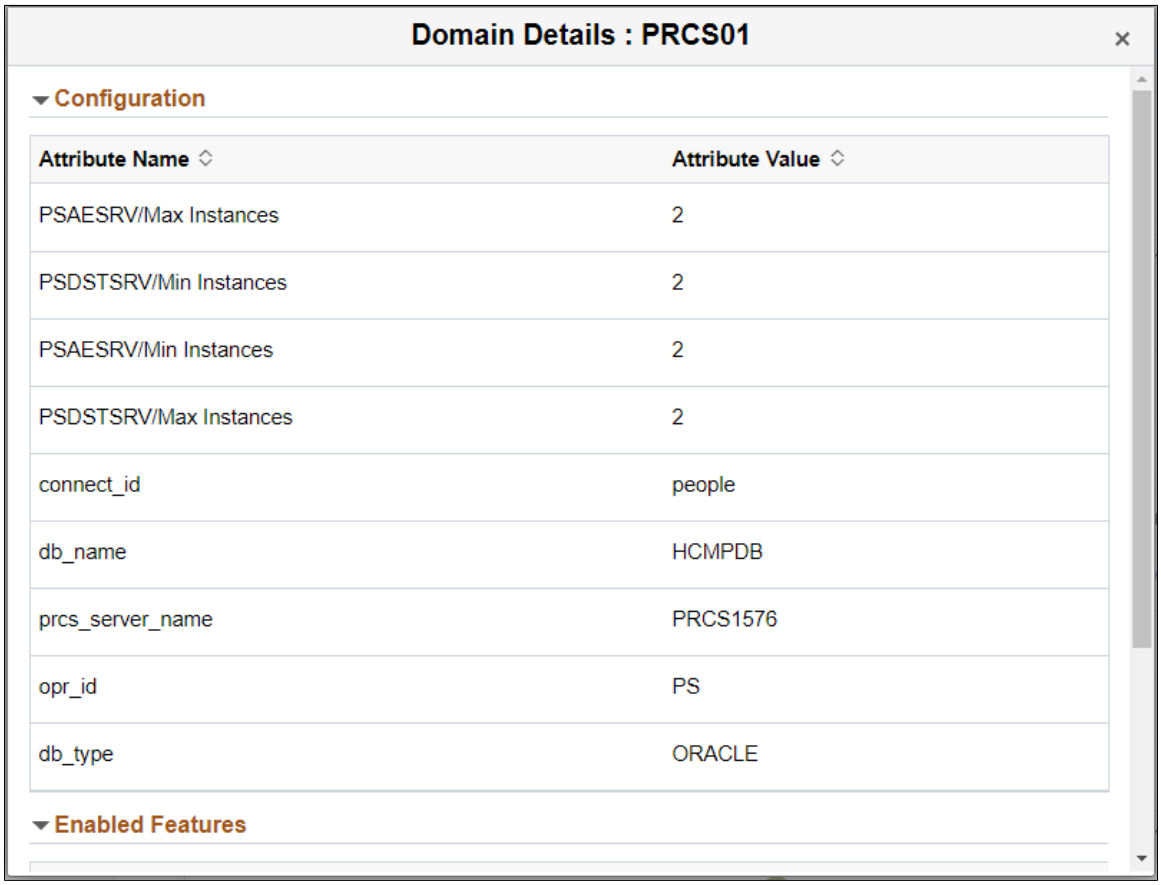
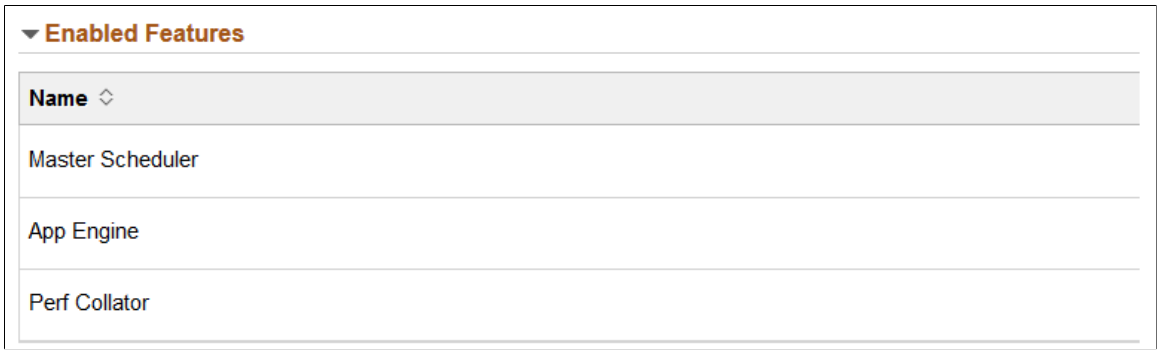


Image: Example Domain Details for Process Scheduler - Enabled Features

This example illustrates the enabled features for the Process Scheduler domain PTCS01.



Master Scheduler, Application Engine, and Performance Monitor features can be enabled for the instance.

Accessing Provisioned Environments

To access PIA of provisioned environment, click on the PIA URL link on the environment card. This will launch PIA of the newly created environment. To view more details about the environment, refer to Environment Details Page.

Note: If environments are provisioned on private subnets, then use a Bastion server or a Windows instance as a jump host. The bastion or the Windows instance must be set up on a public subnet accessible from internet.

Linux instances can be accessed using SSH. SSH private keys are required to connect to the provisioned instances. There are two private keys that can be used:

1. Cloud Manager SSH Keys for Administration - This is the SSH key pair that is created by Cloud Manager and the public key is automatically injected into the newly provisioned instances. The SSH private key file cm_adm_pvt_key is available under /home/psadm2/psft/data/cloud/ocihome/keys/.
2. User SSH key - A Cloud Manager user can create a set of SSH key pair and configure the public key in My Settings page. Using the private key, user can connect to the provisioned instances. For more details refer Configuring My Settings .

Windows instances can be accessed using RDP. Ensure to enable RDP ports in OCI security lists, as well as in the client side firewalls.

The IP addresses for Linux and Windows instances can be determined from the Environment Details Page. See Environment Details Page.

Important! It is user's responsibility to backup SSH keys for Administration and User SSH Keys to avoid losing access to provisioned instances due to loss of Cloud Manager instance or any fatal failures.

Updating SSH Keys

In Oracle Cloud Infrastructure, SSH keys are used to provide secure access to all Linux instances. It is user's responsibility to manage and secure the SSH keys that are used in OCI. Cloud Manager also uses SSH keys for managing environment nodes. Cloud Manager injects two SSH public keys into any node that it provisions. The SSH keys are:

1. SSH keys for Administration

   This key pair is generated by Cloud Manager at the time of installation (bootstrap). This key pair is used to connect and manage Linux instances provisioned as PeopleSoft environments. The key pair is available under the path - /home/psadm2/psft/data/cloud/ocihome/keys. The two files for this key pair are:

   - Private key: cm_adm_pvt_key
   - Public key: cm_adm_pvt_key.pub

2. User SSH keys

   Users can create their own personal SSH key pair and configure an additional SSH key under My Settings Page. This gets automatically configured in a newly provisioned node, enabling users to use their own keys to access PeopleSoft instances. This key is optional and will be injected into provisioned instances only if it is configured.

Note: SSH keys for Administration will be injected into all provisioned instances, irrespective of User SSH key configuration.

Updating SSH Keys for Administration

Cloud Manager uses SSH keys to connect to Linux instances deployed and managed by Cloud Manager. The public and private SSH key pair used by Cloud Manager to manage instances are located under /home/psadm2/psft/data/cloud/ocihome/keys. The public key file is cm_adm_pvt_key.pub and the private key file is cm_adm_pvt_key. From time to time, an organization will want to update or rotate SSH keys. For example:

1. A employee who was a Cloud Administrator or Cloud Manager Administrator has left the organization.
2. As a company policy, it is mandated to update keys periodically.

In such situations, an administrator must ensure to update SSH keys on both Cloud Manager instance as well as on all the managed instances that were created by Cloud Manager. The administrator must create a new pair of Administration keys and update in two locations:

- On Cloud Manager

  Backup the existing keys and replace the keys cm_adm_pvt_key.pub and cm_adm_pvt_key under /home/psadm2/psft/data/cloud/ocihome/keys. The file names should be retained as it is.

- Managed instances

  Using the old private key, SSH into each of the instances provisioned by Cloud Manager as 'opc' user. On the managed instance, update the /home/opc/.ssh/authorized_keys. Remove the previous Administration public key entry and add the new public key.

Updating User SSH Keys

To update any user SSH keys that were injected by Cloud Manager:

1. Generate a new pair of user SSH keys.
2. Log in to the managed instance using either the existing User SSH key or the Cloud Manager's SSH key for Administration.
3. Update the file /home/opc/.ssh/authorized_keys with new key and remove the existing key. Please ensure to remove the correct entry.

Generating New SSH Keys

Guidelines for generating new SSH keys:

1. New SSH key pair must be generated using the openssh ssh-keygen utility. If the key pair is generated using any other utility, then it must be converted to openssh format before using them in Cloud Manager.
2. Cloud Manager does not support encrypted ssh key. That is, ssh keys should not be protected by a passphrase.
3. When new SSH keys for Administration are generated, ensure to retain the same names for the private and public key files. The permissions of these files should be as shown below.

```
-r-x------. 1 psadm2 oinstall 1675 Jan 21 08:08 cm_adm_pvt_key

-r-x------. 1 psadm2 oinstall  382 Jan 21 08:08 cm_adm_pvt_key.pub
```


4. When new User SSH Keys are generated, the file names can be user defined but the permissions must be same as above.

Manage PUM Connections Page

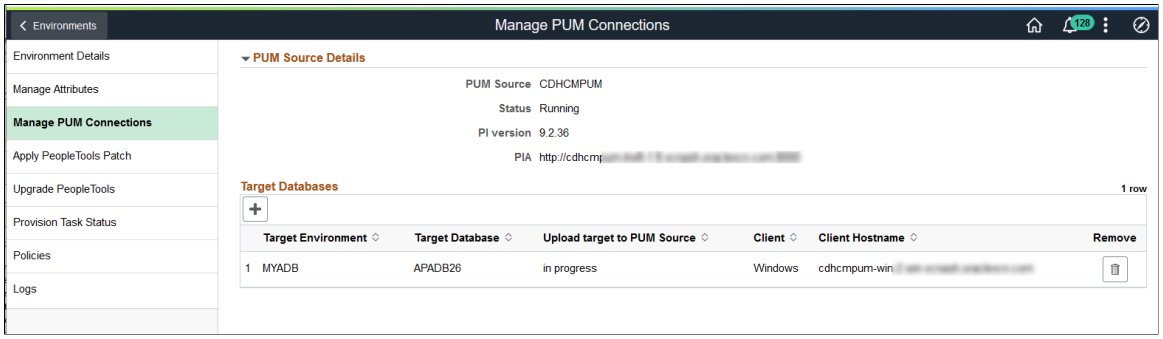
Use the Manage PUM Connections page (ECL_SA_MANAGEPM_FL) for setting up environments for selective adoption. This page appears only for environments that were deployed using a PeopleSoft Update Image and has a PeopleSoft Client (Windows Client) as part of the environment. This environment can act as a PUM Source environment. You can manage target databases for the PUM Source from this page, which will add or remove specified target databases to the PUM source environments. After adding target databases, administrators can use the PIA URL shown on this page to access PUM Dashboard to define change packages. To create and apply change packages, access Change Assistant that is installed on the PeopleSoft client. To access Change Assistant, use remote desktop (RDP) to Windows Client.

Navigation

Click the Manage PUM Connections link available on the left panel of the Environment Details page. The Manage PUM Connections page is displayed in the right panel.

Image: Manage PUM Connections page

This example illustrates the fields and controls on the Manage PUM Connections page.



The Upload target to PUM Source status is displayed as either In progress, Complete or Failed.

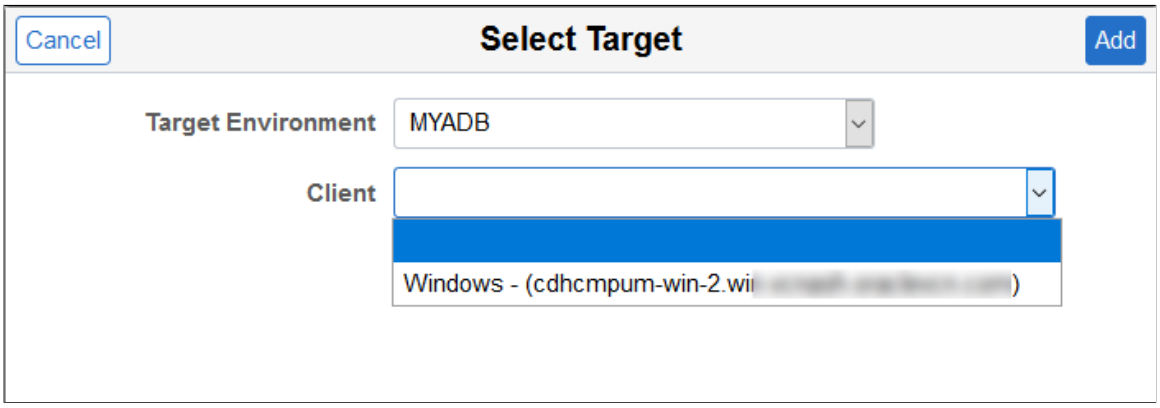
Adding Target Databases

To add a target database which you want to update, perform the following:

1. Click Add target button available in the Target Databases section.
2. Select the required target environment.

Image: Select Target modal window

This example illustrates the fields and controls on the Select Target modal window.



3. Select the client.
4. Click Add. This action starts the ‘Add Target’ and ‘Upload to PUM Source’ functionality. The status is displayed as either in progress, Complete or Failed.

Apply PeopleTools Patch Page

Use the Apply PeopleTools Patch page (ECL_ENV_PTCHUPD_FL) for applying latest PeopleTools patches.

It is recommended to take a backup of the environment prior to applying a PeopleTools patch.

Note: The Apply PeopleTools Patch link is available only if a Windows client node (PeopleSoft Client or Windows middle tier) is associated with the selected environment.

For environments on PeopleTools 8.57 or higher, customizations made to Application Server (psappsrv.cfg) and Process Scheduler Server (psprcs.cfg) are preserved during a PeopleTools Patch. The following Web Server files are also preserved.

- $PS_CFG_HOME/webserv/WEBSERVER01/config/config.xml and any custom folders
- $PS_CFG_HOME/webserv/WEBSERVER01/applications/peoplesoft/PORTAL.war/WEB-INF/psftdocs

---

Note: User has to manually update other customization files in the webserver.

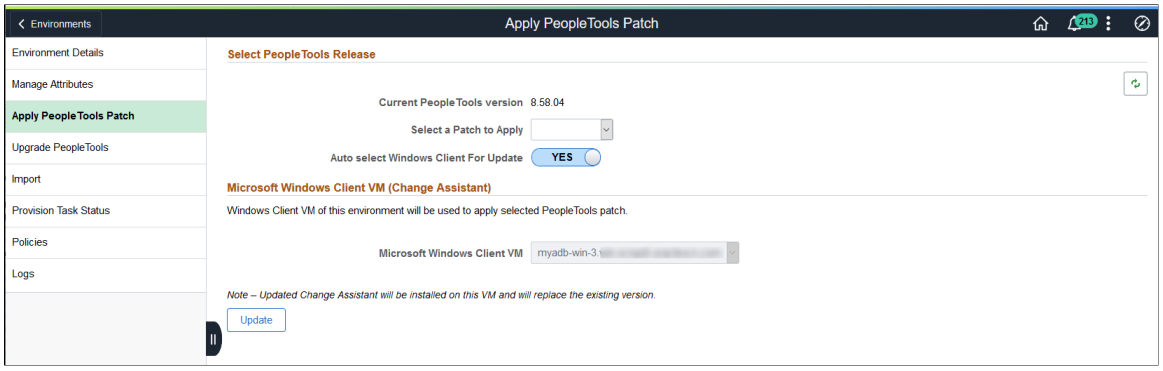
The PeopleTools patch process saves the configuration files during the unprovisioning task. The files are then imported using PSADMIN.

Navigation

Click the Apply PeopleTools Patch link available on the left panel of the Environment Details page. The Apply PeopleTools Patch page is displayed in the right panel.

Image: Apply PeopleTools Patch page

This example illustrates the fields and controls on the Apply PeopleTools Patch page. You can find definitions for the fields and controls later on this page.



Select a Patch to Apply — Select an appropriate PeopleTools patch to be applied on the target environment.

Update — Click this button to apply the changes.

Note: User can select the patch update entry from the grid to see a window which shows the tasks executed for the patch update process and their real-time status. There is provision to mark failed tasks as complete so as to complete the patch update use-case in failure scenarios.

Note: Ensure that the latest PeopleTools patch is already downloaded and available in the Repository.

Upgrade PeopleTools Page

Use Upgrade PeopleTools page (ECL_ENV_UPGD_FL) to upgrade PeopleTools version (major version changes).

It is recommended to take a backup of the environment prior to performing a PeopleTools upgrade.

For environments on PeopleTools 8.57 or higher, customizations made to Application Server (psappsrv.cfg) and Process Scheduler Server (psprcs.cfg) are preserved during a PeopleTools Upgrade. Webserver configurations are not preserved in a PeopleTools upgrade. The webserver will be redeployed.

The PeopleTools patch process saves the configuration files during the unprovisioning task. The files are then imported using PSADMIN.

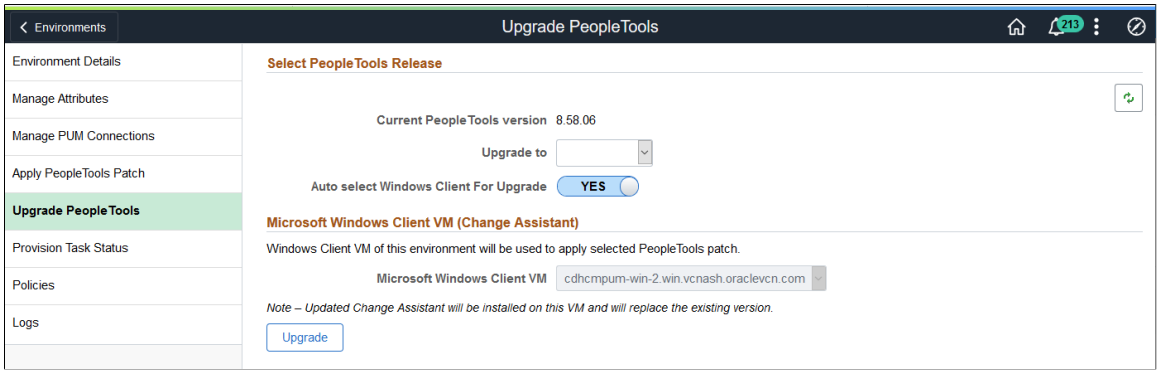
Note: The Upgrade PeopleTools link is available only if a Windows client node (PeopleSoft Client or Windows middle tier) is associated with the selected environment.

Navigation

Click the Upgrade PeopleTools link available on the left panel of the Environment Details page. The Upgrade PeopleTools page is displayed in the right panel.

Image: Upgrade PeopleTools page

This example illustrates fields and controls on the Upgrade PeopleTools page.



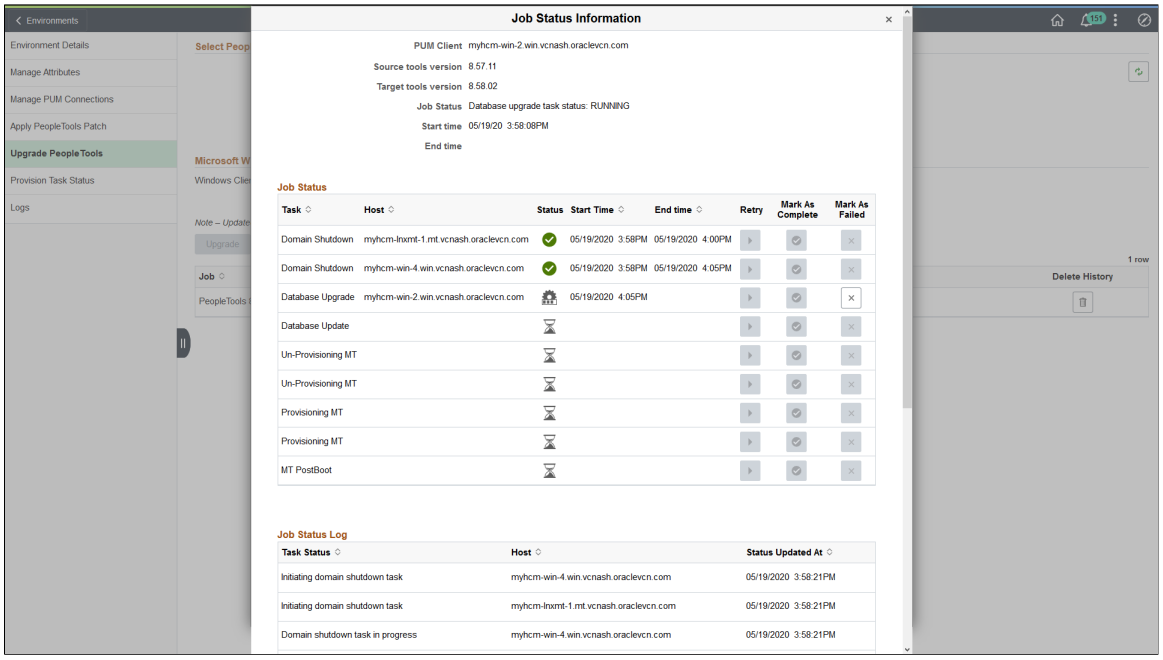
Upgrade to	Select the major PeopleTools version.
Auto select Windows Client For Upgrade	Select Yes to auto select. Select No to select the Windows Client to use for the upgrade from the Microsoft Windows Client VM drop-down list box.
Upgrade	Click this button to apply the changes. Before doing Upgrade, user must ensure to take a backup of the environment.

After clicking the Upgrade button, the job status will be displayed on the page.

Click on the link in the Status column to view the Job Status Information modal window where you can view detailed information regrading the job.

Image: Job Status Information Modal Window

This example illustrates the fields and controls on the Job Status Information Modal Window where the Job Status is Complete.



You can view upgrade process details such as jobs executed successfully, jobs which are in pending status, and failed jobs.

Policies Page

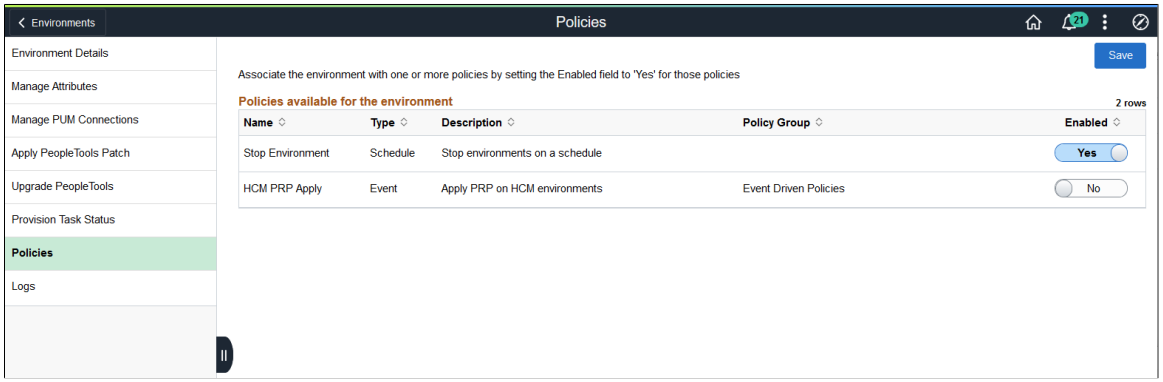
Use the Policies page (ECL_POLICY_ENVS) to associate policies with the environment name.

Navigation

Click the Policies link available on the left panel of the Environment Details page.

Image: Environment Policies page

This example illustrates the fields and controls on the Environment Policies page. You can find definitions for the fields and controls later on this page.



All the active policies defined by a Cloud Manager administrator or the user that created the environment are displayed. Use the Enabled column to associate the policy with the environment.

When a policy is enabled for an environment, the environment name will be appended to the Environment Names condition property or action parameter for the Policy. Likewise, if the policy is disabled, it will be removed from the Environment Names condition property or action parameter for the Policy.

See Setting Policy Conditions and Action.

Manage Attributes Page

Use the Manage Attributes page (ECL_ENV_RESET_FL) to update managed environment attributes, if user modified any parameter outside Cloud Manager and for adding the PeopleSoft (Windows) Client.

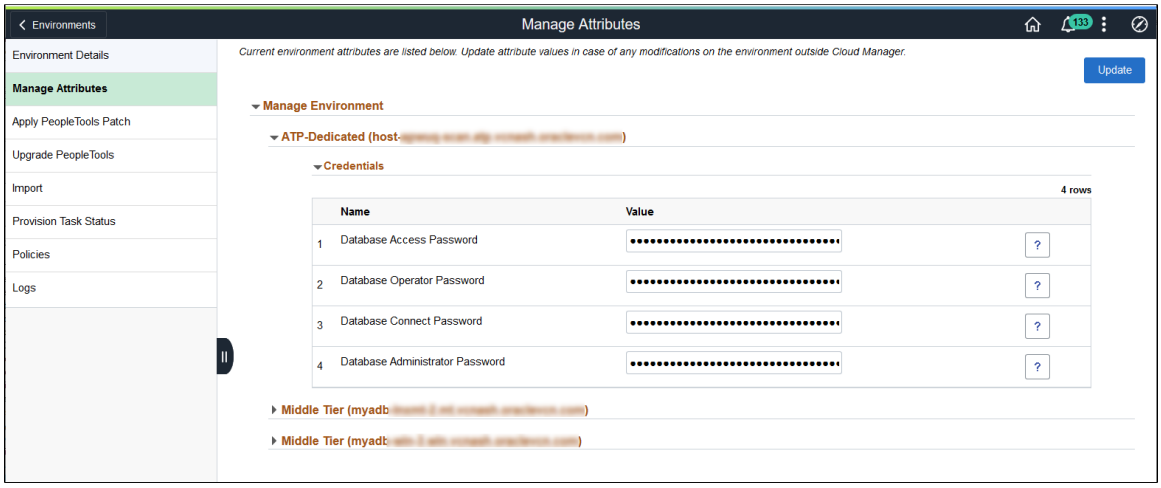
Note: The Manage Attributes page must be updated only when a user modifies the environment attributes directly on the instance. For example, if a user modifies the OPRID Password on the instance directly, then user must update and save the password for Cloud Manager to store in its database. Otherwise, the password stored in Cloud Manager will be stale and any operation that is dependent on this OPRID Password will fail. Click the Refresh button on the environment details page to fetch the current status of the environment node.

Navigation

Click the Manage Attributes link available on the left panel of the Environment Details page. The Manage Attributes page is displayed in the right panel.

Image: Manage Attributes page

This example illustrates the fields and controls on the Manage Attributes page.



You can edit the required parameters by expanding each domain and click save. For details on environment attributes, see Environment Attribute Details section in Managing Template.

Logs Page

Use the Logs page (ECL_ESEARCH_FL) to view the logs for all actions that are performed on the environment.

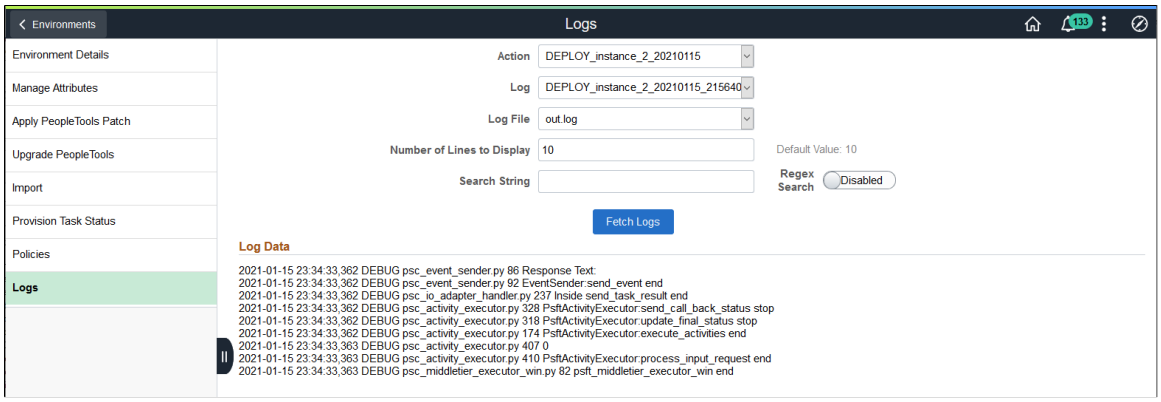
Note: The contents of the log files are displayed in reverse (latest first) order.

Navigation

Click the Logs link available on the left panel of the Environment Details page. The Logs page is displayed in the right panel.

Image: Logs page

This example illustrates the fields and controls on the Logs page.



Action

Select the Action from the drop down.

Actions include:

- ADD_NODE
- CREATE_DB_BACKUP
- ES_UNPROVISION
- LIFT
- OCI_CLONE
- POSTBOOT_CONFIG
- PTU_PEOPLETOOLS_PATCH_UPDATE
- PTU_PEOPLETOOLS_UPGRADE
- PTU_REPROV_MT
- PTU_STOP
- PTU_UNPROV_MT
- REMOVE_NODE
- SHIFT_DEPLOY_TDE
- SHIFT_DEPLOY
- ADD_TARGET
- START

	• STOP
Log	Select the log associated with the action.
Log File	• console.log • out.log • tf.err Terraforma error log • tf.out Terraforma log
Number of Lines to Display	Enter number of lines to display.
Search String	Enter a search string.
Fetch Logs	Click to fetch the logs.

Cloning Environment

Use the Clone Environment action to duplicate an exact copy of an existing PeopleSoft environment running in Cloud Manager. The new environment is built by reconfiguring the disks from deep clone, saving installation and deployment time.

The following restrictions apply:

- Parallel cloning for same source environment is not supported.
- Clone feature will not be able to trigger a clone if a previous clone for the same source environment is in a failed state.

  Delete the failed cloned environment using Cloud Manager. Cloud Manager will clean up all the resources relating to the failed OCI clone environment.
- Clone feature does not support BM instance cloning.

Use cases for cloning environments include:

- Creating a duplicate environment with Database, Middle Tier, Elastic Node including Kibana, Web Server and Windows client running in distributed nodes with the exact configuration and data as the source environment.
- Creating a scaled down copy of the production environment with just the database.
- Creating a scaled down copy with Database, Middle Tier and WebServer for a test environment.

Note: The cloned environment is an exact copy of the existing environment. Once the cloned environment is running, you can perform scaling and Lifecycle Management actions.
See Managing Nodes.

Scenarios for cloning an environment include:

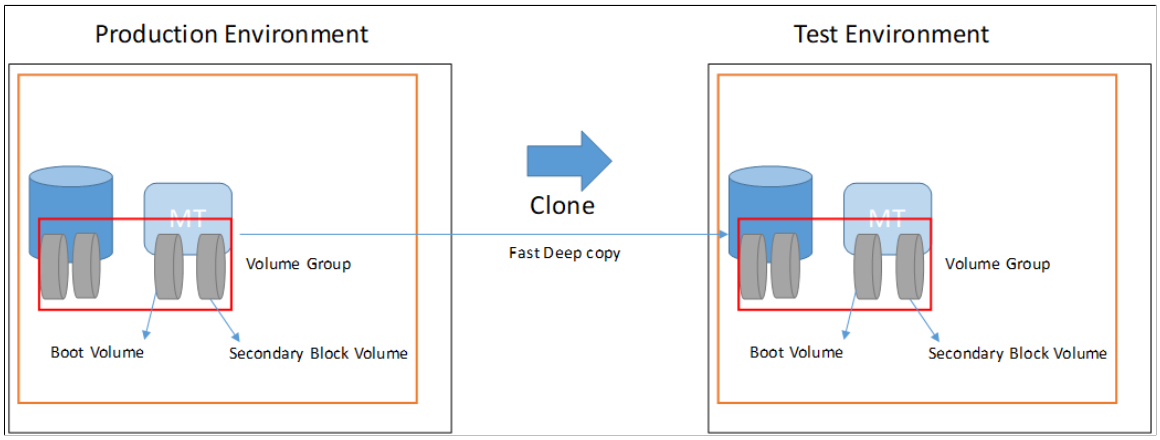
- All environment components are running on compute instances.
- Database is running on DBS (Database as Service Platform as Service) and other components are running on compute instances (Infrastructure as a Service).
- Database is running on ATP-Dedicated (Autonomous Transaction Processing Database) and other components are running on compute instances (Infrastructure as a Service).

Cloning Compute Instances

When all of the components for the PeopleSoft environment are running on Compute, the clone process uses OCI Cloud APIs to clone the boot volume and secondary block volume into a volume group. The volume group is then used to create a new instance of the environment.

Image: Fast Cloning for Compute

This diagram illustrates that the cloning operation will copy both the boot volume and the secondary block volume into a volume group, then perform a fast deep copy to create a new environment that is the exact copy of the source.

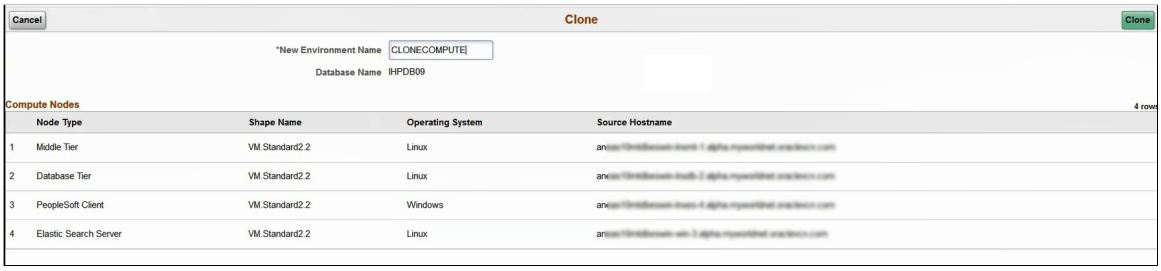


To clone an environment with all components running on compute instances :

1. From the Cloud Manager Homepage, select the Environments tile.
2. Click on the Related Actions button corresponding to the environment to be cloned and select Clone Environment.
3. The Clone Window displays all the components for the environment.

   Image: Clone Environment — Compute Instance

   This is an example of the Clone page where all components are running on compute.



4. Enter a New Environment Name.
5. Click the Clone button.
6. Select Yes to confirm. Cloning will initiate.

   The cloning process will take 10 to 15 minutes.
7. Use the Refresh button to view the status. Status will change from Initiating to Provisioning and then to Running.

Cloning an Environment With Database is Running on DBS and Other Nodes on Compute

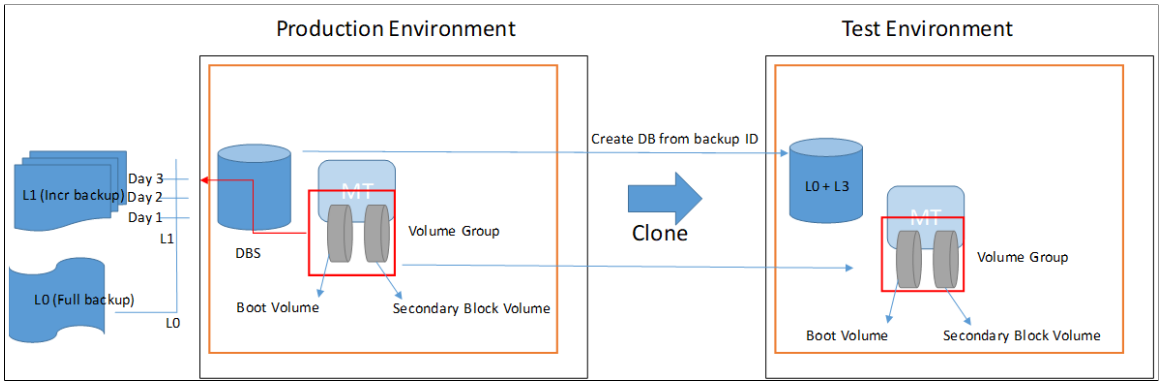
For environments with database on DBS, the Clone operation requires a database backup to create the corresponding database node in the cloned environment. There are two options for the database backup:

- Create a new database backup as part of the clone operation.

  Note: This is the default operation to create a new a point-in-time fullback up to use for cloning the database instances.
- Use an existing database backup from the OCI backup services, in this case both database backup and middle tier versions should be in synch.

Image: Fast Cloning for DBS Environment

This diagram illustrates backing up the database from a full backup and the latest incremental backup to create the cloned database environment.

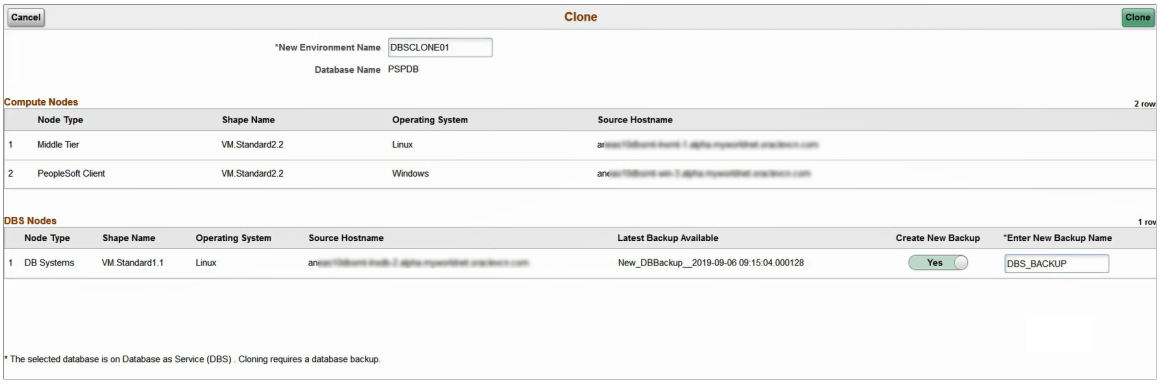


To clone an environment where the database is running in DBS and other nodes are on compute:

1. From the Cloud Manager Homepage, select the Environments tile.
2. Click on the Related Actions button corresponding to the DBS environment to be cloned and select Clone Environment.
3. The Clone Window displays two sections, one for the Compute Nodes and one for the database system.

Image: Clone Environment on DBS

This example illustrates the fields and controls on the Clone page for an environment where the database is running as a service. You can find definitions for the fields and controls later on this page.



New Environment Name — Enter the name for the new environment.

Create New Backup — Select *Yes* to create a new point in time backup of the database.

Select *No* if you want to use an existing backup.

Enter New Backup Name — If you selected *Yes* to create a new backup, a backup name is generated. You can edit the backup name.

If you selected *No* to create a new backup, the available backups are populated in the drop down list.

4. After entering the environment name and selecting the backup preference, click the Clone button.
5. Select Yes to confirm. Cloning will initiate.
6. Use the Refresh button to view the status. Status will change from Initiating to Provisioning and then to Running.

Cloning Imported Autonomous Database Environment

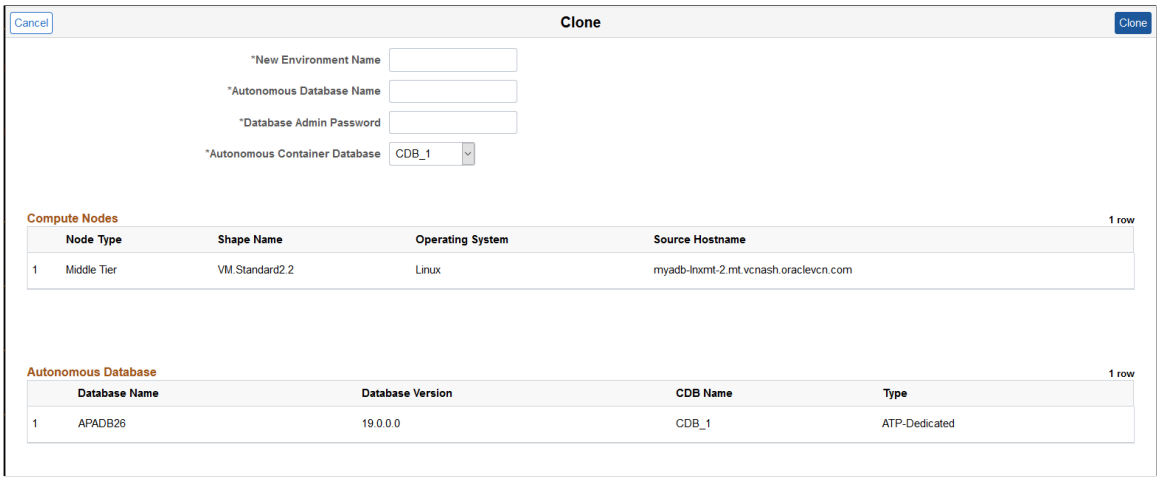
To clone an imported Autonomous Database (ADB) environment:

1. From the Cloud Manager Homepage, select the Environments tile.
2. Click on the Related Actions button corresponding to the ATP-D environment to be cloned and select Clone Environment.
3. Enter the values on the Clone page.

Note: ATP-D supports direct cloning from the source ATP-D.

Image: Clone page for ATP-Dedicated environment

This example illustrates the fields and controls on the Clone page for ATP-Dedicated environment. You can find definitions for the fields and controls later on this page.



New Environment Name Enter the name for the new environment.

Autonomous Database Name The autonomous database name must be unique throughout the tenancy.

Database Admin Password Enter the database administrator password.

Autonomous Container Database Select the container from the drop down list. You can clone to a the same or a different container. The container must be under the same Encryption Key management.

4. Click Clone.

Importing Environment

Cloud Manager supports importing PeopleSoft environments that are running on Oracle Cloud into Cloud Manager as a managed instance.

- Database is running on DB System (Database as a Service).

  ExaCS, DB-VM, and DB-BM are supported

- ATP-Dedicated database running in OCI.
- Other components are running on compute instances (Infrastructure as a Service).

Note: Databases created manually on Compute (VM or Bare Metal) are not supported.

Prerequisites

You must perform the following prerequisites:

1. OCI Credentials

Get the following OCI Credentials for the components you want to import from the OCI Console:

- Database Credentials for DB System
- Database System OCID
- Database OCID
- Database Private IP

  The node for the database contains the private ip.
- Autonomous Database OCID
- Midtier OCID
- PeopleSoft Client OCID
- Elastic Search OCID
- Windows middle tier OCID

2. User Profile Credentials
   - Default OPC user
   - DPK user profiles like psadm2, psadm3 should be present in the environment.
3. Copy Cloud Manager SSH public key to all the nodes that will be imported.
   a. Login to the Cloud Manager putty as psadm2

      sudo su – psadm2

      Open and copy the pub key from /home/psadm2/psft/data/cloud/ocihome/keys/cm_adm_pvt_key.pub

   b. Next log into the Database system as opc, access .ssh/authorized_keys and paste the key from step a into it. This is required to authenticate Cloud Manager to access the Database environment to import the database system.

   c. Log onto each additional node to be imported (Middle Tier, PeopleSoft Client, Elastic Search, Windows middle tier), access .ssh/authorized_keys and paste the key from step a into it.
4. Make sure that the tns entry is present in tnsnames.ora on the database system you are importing.
5. D drive is mandatory for a Windows client.
6. Oratab entry for db home is required in this format <Oracle_SID>:<DB_HOME_PATH>.

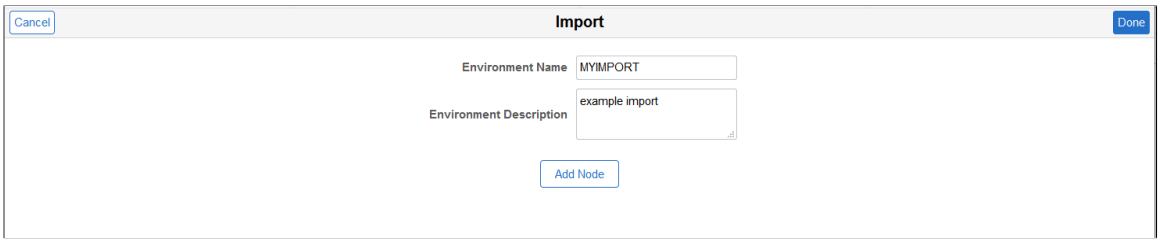
Importing Environment

To import an environment:

1. From Cloud Manager homepage, select Environment Tile.
2. Select Import Environment button.

   Image: Import Environment page

   This example illustrates the fields and controls on the Import Environment page. You can find definitions for the fields and controls later on this page.



Environment Name	Enter a name for the new environment.
Environment Description	Enter a description for the new environment.
Add Node	Select to add a node to the environment.

3. Click the Add Node button.
4. Select the instance type from the drop down list. Six types of tiers can be imported:

   - ATP-Dedicated
   - Database System
   - ELK Stack
   - Middle Tier
   - PeopleSoft Client
   - Windows Middle Tier

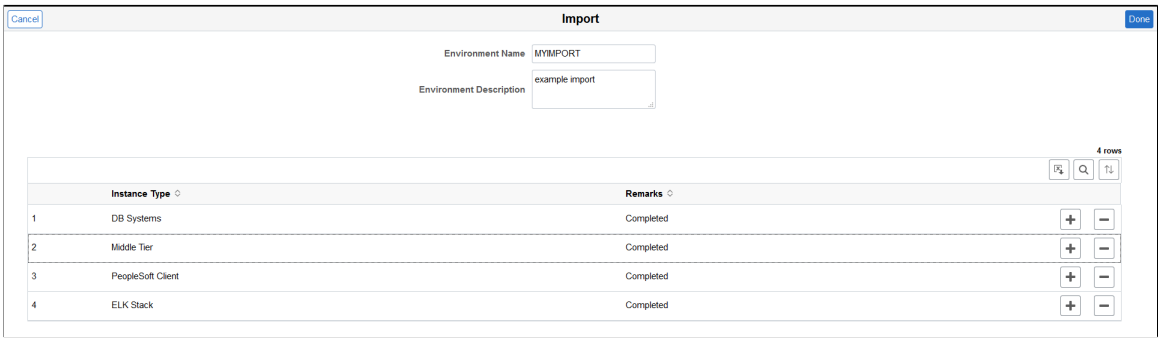
5. The Add Node page for the instance type is displayed.
6. Enter the values for the instance type and click OK.
7. To add another instance type, click the + icon and select the instance type.

   Note: Each instance type is added separately.

8. Once you have included all the nodes for the environment, click Done.

Image: Example Import with Multiple Nodes

This example illustrates the fields and controls on the Example Import with Multiple Nodes.



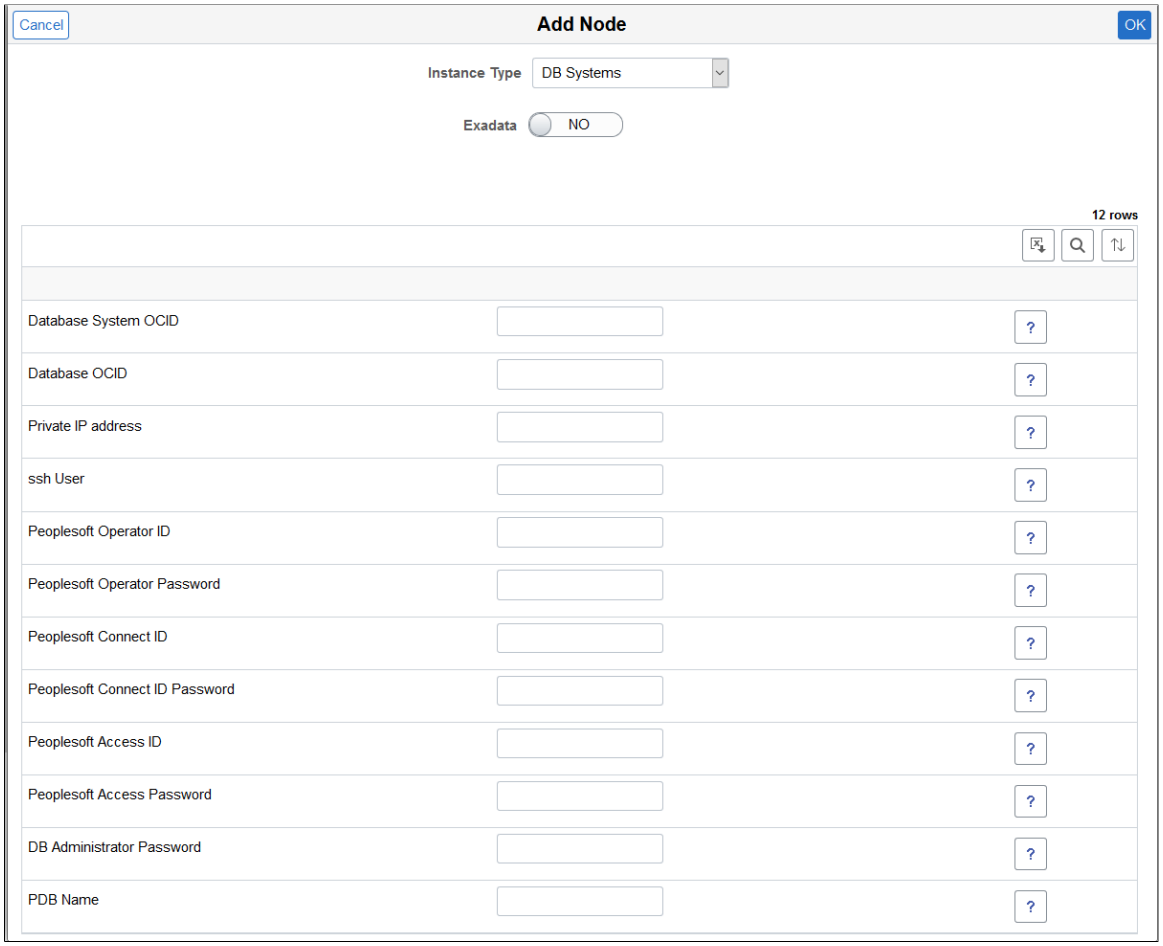
9. The respective tile is added to the Environments page with the status of *ImportingMultipleTier*.
10. To view the status of the import, select Details action for the respective tile on the Environments page.

Database System Instance Type

For the database system node, all the values are mandatory.

Image: Import DB Systems node

This example illustrates the fields and controls on the Add Node page for DB Systems. You can find definitions for the fields and controls later on this page.



Exadata Select Yes if the DB System is Exadata. An additional field for Container Database Name will be added.

Database System OCID Database System OCID for the target database.

Database OCID Database OCID for the target database.

Private IP Address Private IP address for the target the Database environment.

ssh User ssh user on the database system being imported

PeopleSoft Operator ID PeopleSoft Operator ID

PeopleSoft Operator Password PeopleSoft Operator Password

PeopleSoft Connect ID PeopleSoft Connect ID

PeopleSoft Connect Password PeopleSoft Connect Password

PeopleSoft Access ID PeopleSoft Access ID

PeopleSoft Access Password PeopleSoft Access Password

DB Administrator Password DB Administrator Password

PDB Name Pluggable Database Name

This is the database name in the tnsnames.ora file.

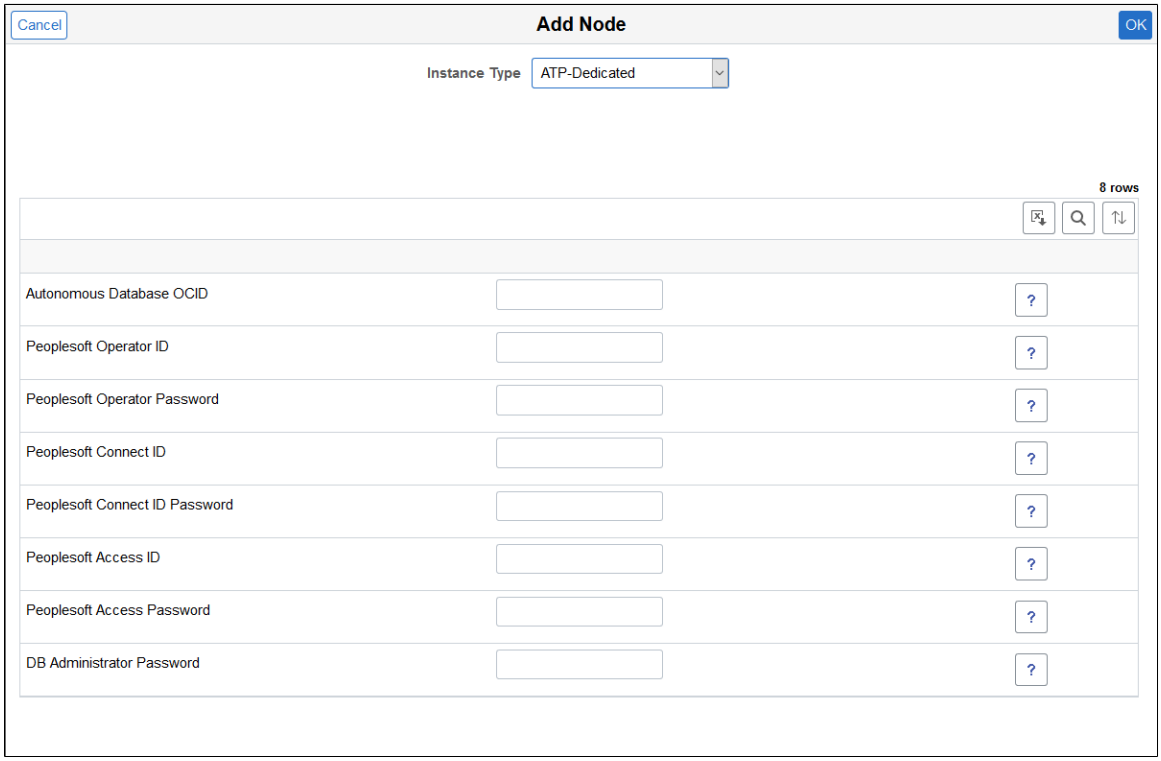
Container Database Name For Exadata DB systems enter the container database name.

ATP-Dedicated Instance Type

For the ATP Dedicated node, all the values are mandatory.

Image: Add ATP-Dedicated Node

This example illustrates the fields and controls on the Add Node page for ATP-Dedicated Node. You can find definitions for the fields and controls later on this page.



Autonomous Database OCID Autonomous Database OCID for the target database.

PeopleSoft Operator ID PeopleSoft Operator ID.

PeopleSoft Operator Password PeopleSoft Operator Password.

PeopleSoft Connect ID PeopleSoft Connect ID.

PeopleSoft Connect Password PeopleSoft Connect Password.

PeopleSoft Access ID PeopleSoft Access ID.

PeopleSoft Access Password PeopleSoft Access Password.

DB Administrator Password DB Administrator Password

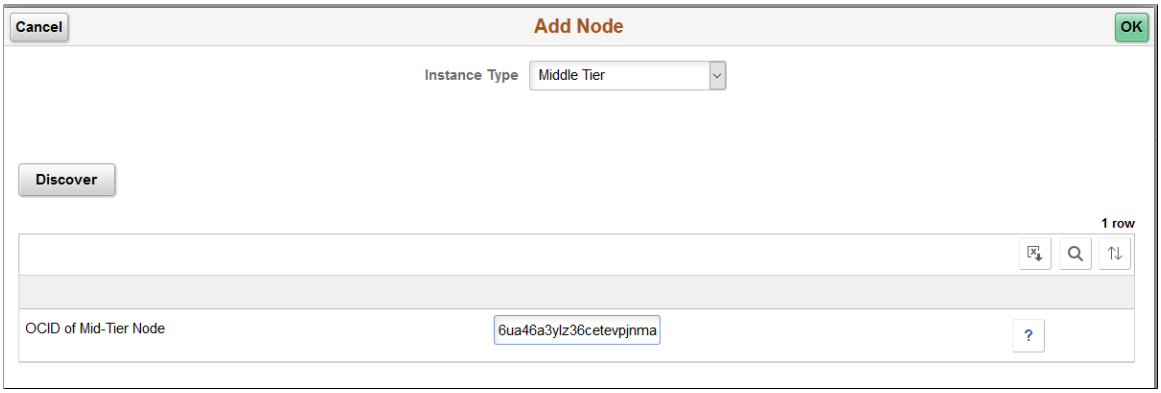
Middle Tier Instance Type

To import a Middle Tier node:

1. Click the + icon on the Import page.
2. Select Middle Tier Instance Type.
3. Enter the Middle Tier OCID.
4. Click Discover.

   Image: Add Middle Tier Node

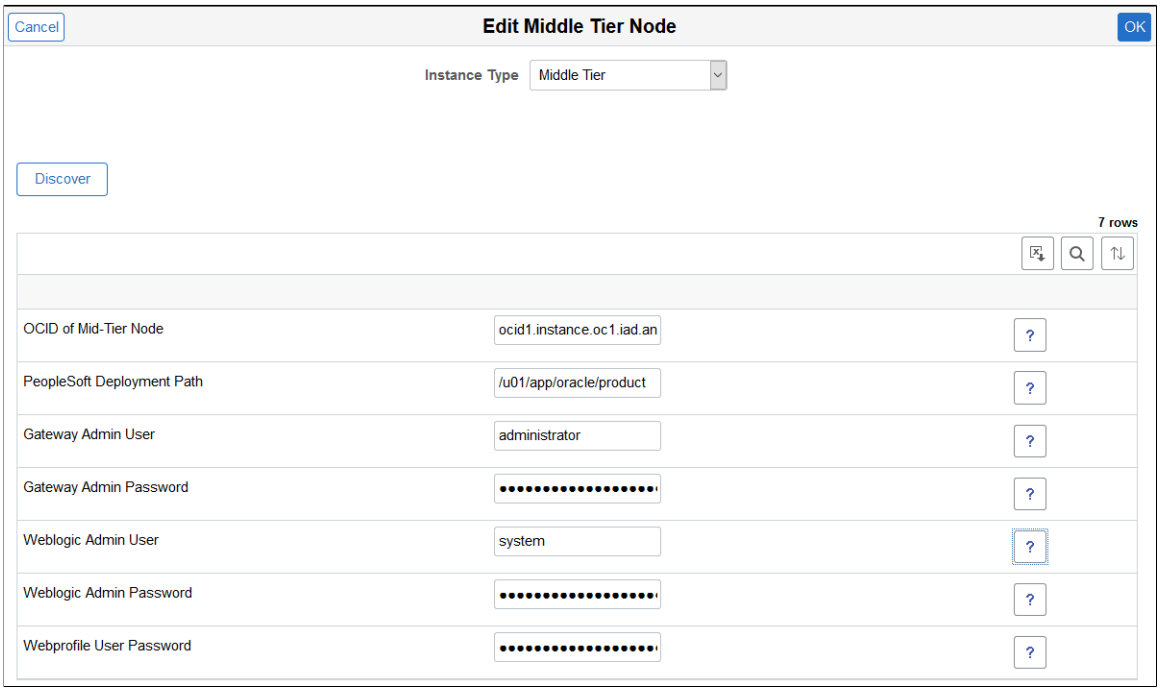
   This is an example of discovering the Middle Tier Node.



5. Discover will ssh into the machine and find the servers(app/web/scheduler) that are present, the PeopleSoft deployment path and whether COBOL is enabled or not.
6. Based on the servers that are present, a popup message will appear listing the servers that were discovered. Click OK.
7. Enter the credentials for the Middle Tier, then click OK.

Image: Add Middle Tier Node Credentials

This is an example of the credentials required for App Server, Web Server and Process Scheduler.



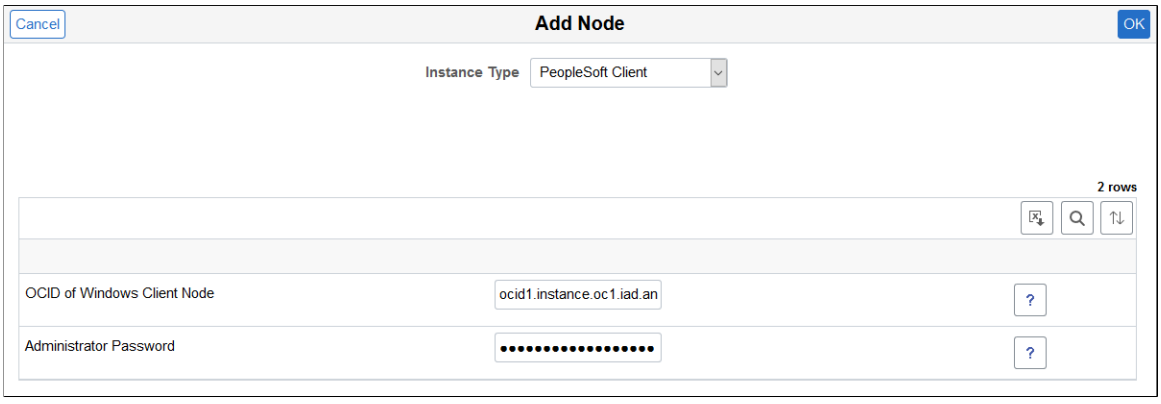
PeopleSoft Client Node

To import a PeopleSoft Client node:

1. Click the + icon on the Import page.
2. Select PeopleSoft Client Instance Type.
3. Enter the PeopleSoft Client OCID and password.

   Image: Add PeopleSoft Client Node

   This example illustrates the fields and controls on the Add PeopleSoft Client Node page.



4. Click OK.

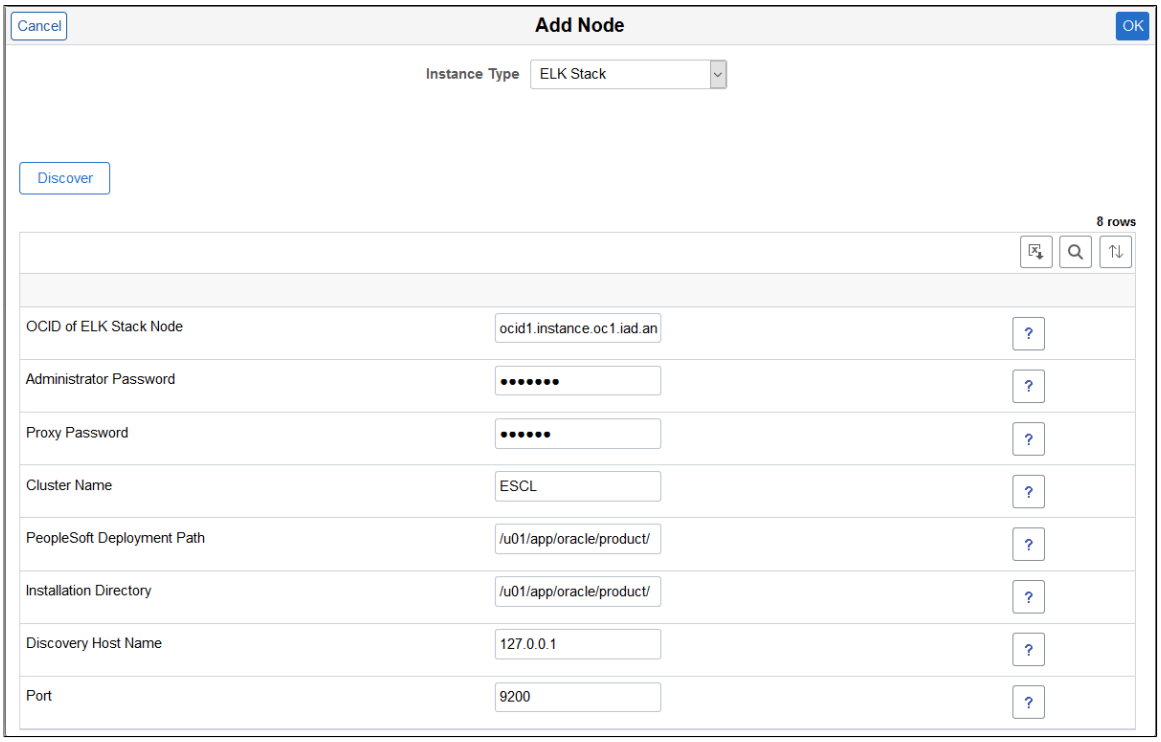
ELK Stack Node

To import an ELK Stack node:

1. Click the + icon on the Import page.
2. Select ELK Stack Instance Type.
3. Enter the ELK Stack node OCID.
4. Click Discover.
5. Click OK on the message that the Elasticsearch Server details were discovered.
6. Enter the credentials and click OK.

Image: Add ELK Stack Node

This example illustrates the fields and controls on the Add ELK Stack Node.



Environment Details — Import Status

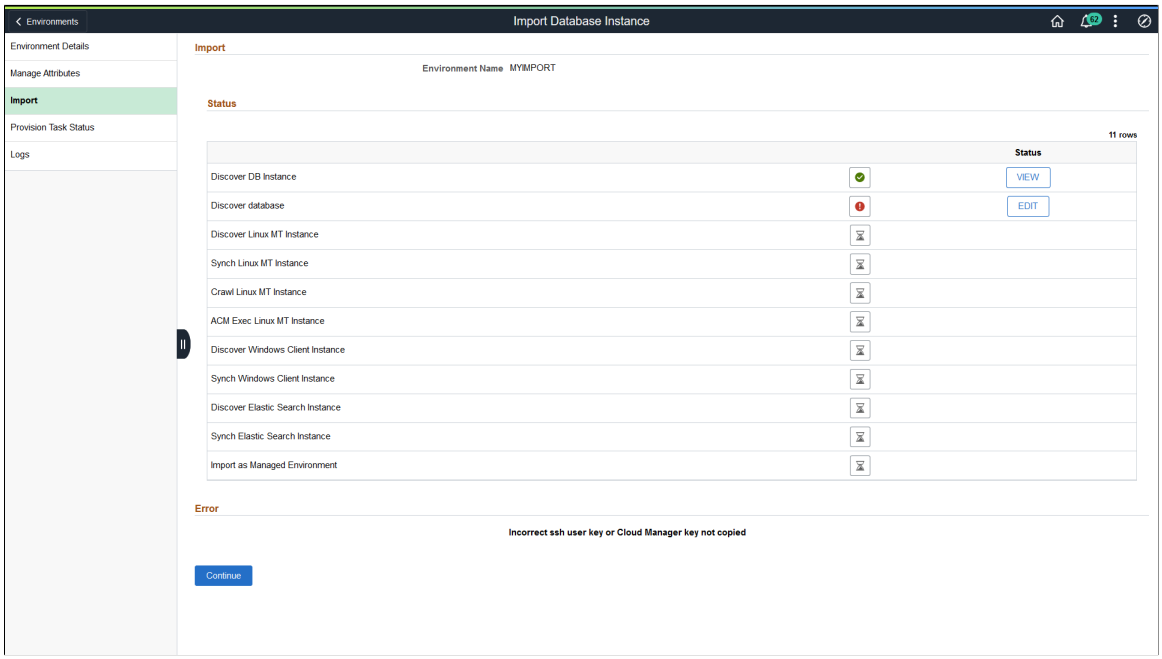
To view the status of the import:

1. The respective tile is added to the Environments page with the status of ImportingMultipleTier.
2. To view the status of the import, select Details action on the tile.
3. Select Import from the left-side menu.

The Detailed status page shows the import steps and status of Import activity.

Image: Status of Environment being imported

This example illustrates the import status.



The Status column will display one of the following buttons:

- View

  Displays the output of that particular step.

- Edit

  Displays the inputs for a step that fails. You can edit the inputs and retry the step.

- None

  Some steps do not contain any output.

After the completion of each step, View button will be displayed to view the respective input parameters.

Status Icons

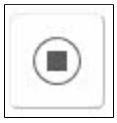
Pending

Success

In Progress

Failed

Continue



Abort

Step details

Pause

If there are any errors in a step, then Errors will be shown and Edit button will be displayed to view and edit the respective input parameters.

Location of Database Import log files:

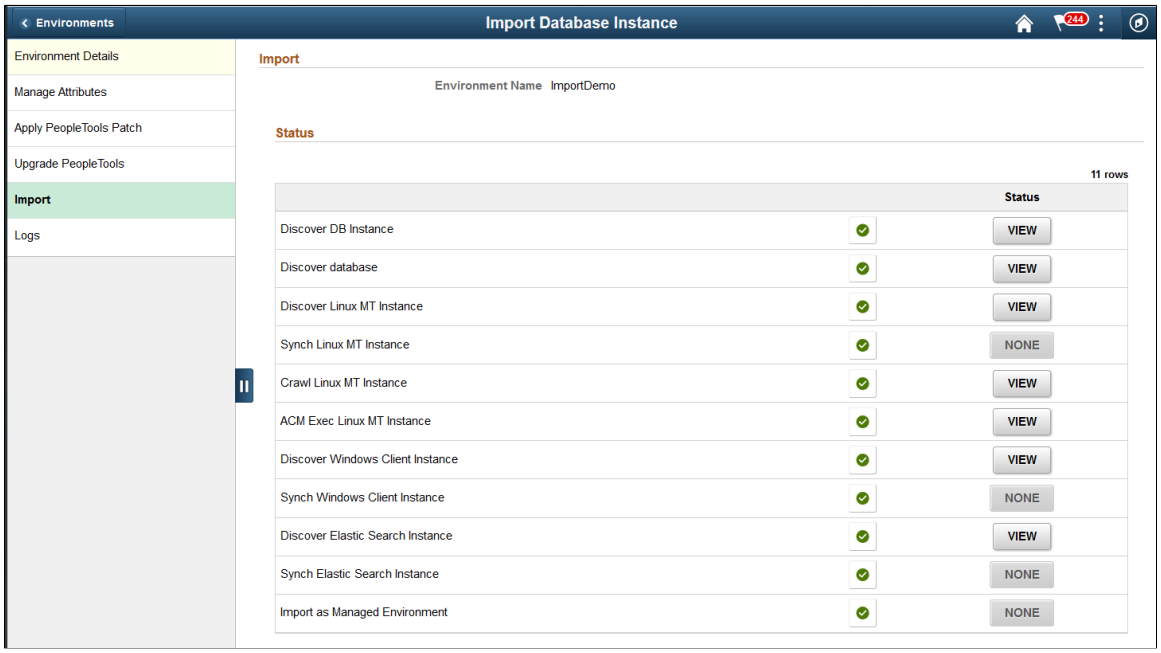
- Import Database instance — terraforma logs are located */home/psadm2/psft/data/cloud/cmlogs/envs/<Import envName>* . Log on as psadm2 user.
- Import Database — psp.log is located */home/psadm2/psft/pt/<pt release number>/appserv/prcs/PRCSDOM/LOGS*. Log on as psadm2 user.
- Discover UI logs — psp.log is located */home/psadm2/psft/pt/<pt release number>/appserv/APPDOM/LOGS*. Log on as psadm2 user.

Once edited, select Continue button to re-try the failed and subsequent steps.

If the steps succeed target Database becomes a managed instance under Cloud Manager.

Image: Import Environment Status

This example illustrates the fields and controls on the Import Environment Status.



If a step has no specific output, a disabled None button is displayed instead of the View button.

Post Import Actions

Imported environment supports the following functions:

- Review environment details and manage attributes.

  See Manage Attributes Page

- On Demand Scale Up and Scale down.

  See Managing Nodes

- Start
- Stop
- Delete

  The database node regardless of whether it is running on Database systems or compute is not deleted.

- Upgrade
- Update

Lifecycle activities like “Apply PeopleTools Patch” and “Upgrade PeopleTools” can be done on the imported environment just like any other Cloud Manager provisioned environment.

Deleting Environment for Imported Nodes

If you select to delete an imported node in Cloud Manager, the following occurs:

- Deletes the scaled up environment.
- Cleans up Metadata stored in Cloud Manager.

Note: Database Systems node is not deleted.

Managing Nodes

Cloud Manager supports on-demand scaling in OCI, which is the ability to scale up or down (horizontal scaling) by adding or removing nodes to an active running PeopleSoft environment as necessary. Using Manage Nodes, you can:

- Add additional middle tiers to a running database or middle tier. (Scale up)
  - Middle tier nodes are added one at a time.
  - Multiple middle tiers (Application Server, Web Server, Process Scheduler Server and Windows) are supported.

  Note: Add or remove node is not supported for full tier environment.
- Remove middle tier node from an environment. (Scale down)
- Add PeopleSoft Client.

  Note: Multiple PeopleSoft Clients are supported.
- Add an ELK Stack node.

  Adding ELK Stack node to an environment requires an IB domain that was configured in the environment by Cloud Manager. If not, the ELK Stack option will not be available when adding a node through Manage Node option. In such scenario, add a new Middle Tier node with IB enabled and then add the ELK Stack node.

  ELK Stack supports two nodes:

  - If Elasticsearch is already running in a node, Kibana cannot be installed in that node.
  - To install Kibana, ELK Stack is required. So the user has to provision ELK Stack and Kibana in a new node.

Adding Nodes

To add a node to a running environment:

1. Click the Related Actions button corresponding to the environment.
2. Select Manage Node.
3. Select Add action.
4. Select Type.

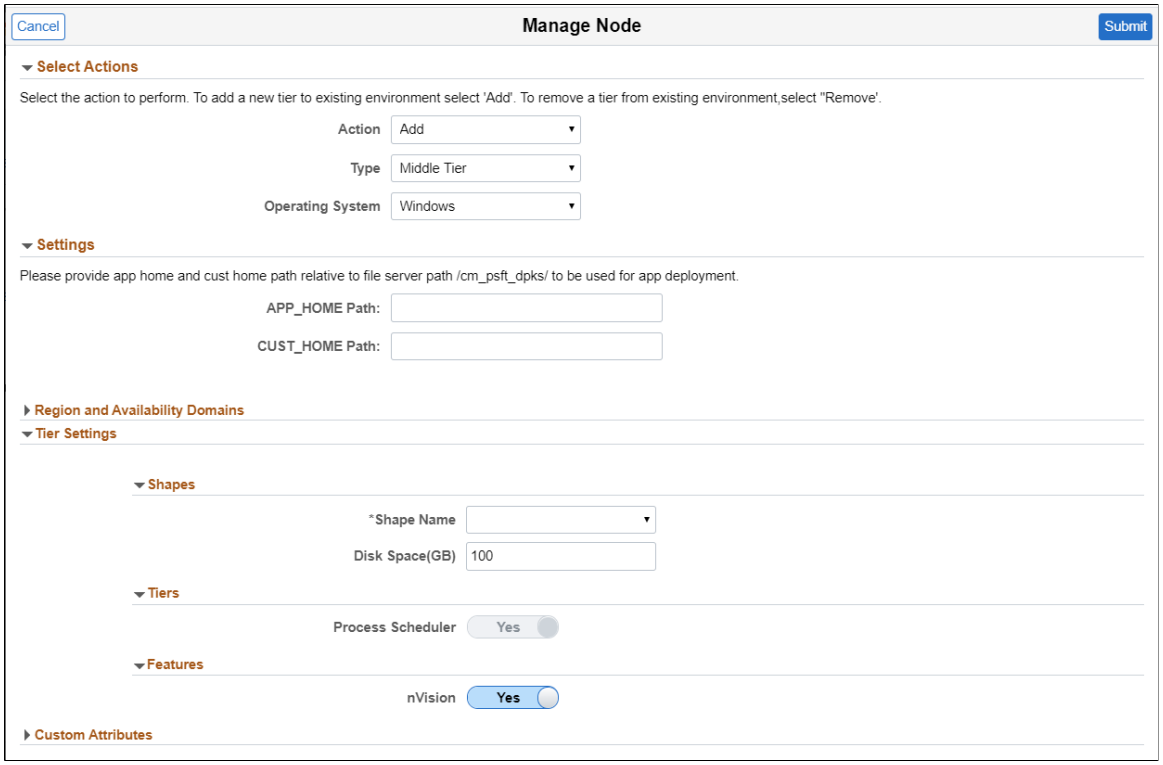
5. Select the Operating System.
6. If the type is Middle Tier then the there is an option to select an existing MT node from which configuration/custom configuration can be copied for the node being added.
7. Enter the required credentials and settings.
8. Click Submit and confirm.
9. Scale Up process status are:
    - InitiatingScaleup
    - ScaleUpInProgress
    - Running
    - ScaleupFailed

Navigation

Click the Related Actions button corresponding to the environment. Select Manage Node. The Manage Node page is displayed.

Image: Manage Node page – Add Middle Tier Windows Node

This example illustrates the fields and controls on the Manage Node page for adding a Windows middle tier node.



Note: Windows Middle Tier node is only supported for PeopleTools 8.57 and above. It is not supported on PeopleTools 8.55 or 8.56 environments.

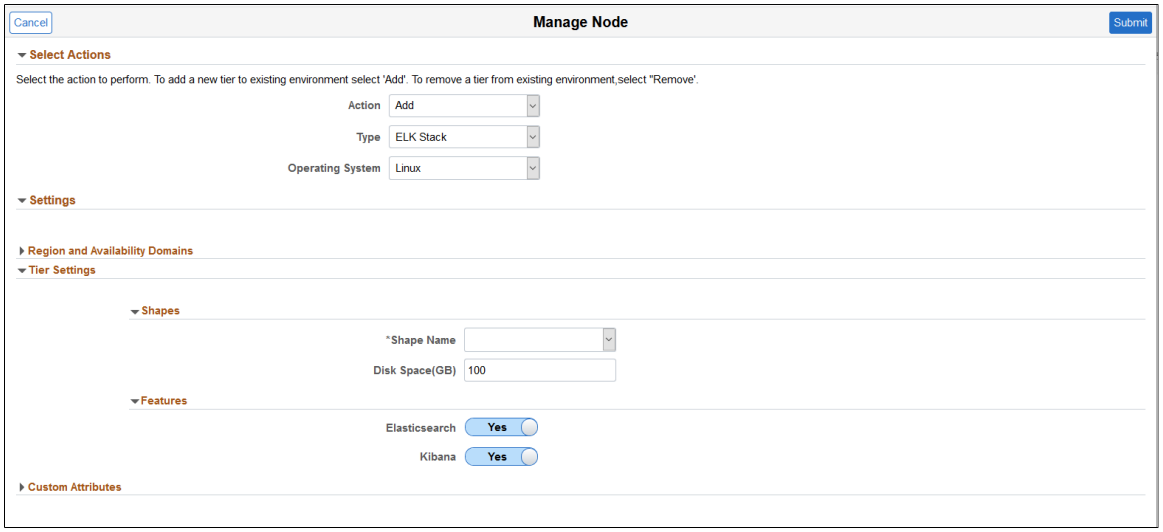
The APP_HOME Path and CUST_HOME paths are not mandatory when adding a windows middle tier. However if you want to copy app home and/or cust home contents to the Windows middle tier perform the following:

1. Create a directory inside file server mount in the Cloud Manager. For example:
    a. Create a directory ps_app_home_win inside /cm_psft_dpks.
    b. Place the app_home contents as a zip file inside this directory.
    c. Create a directory ps_cust_home_win inside /cm_psft_dpks.
    d. Place the cust_home contents as a zip file inside this directory
2. Provide the path to PS_APP_HOME and/or PS_CUST_HOME. For example: ps_app_home_win and ps_cust_home_win.
3. When the Windows mid-tier node is provisioned, the contents in the zip file will be extracted to the machine.

See Creating Windows Middle Tier Nodes.

Image: Manage Node page – Add ELK Stack Node

This example illustrates the fields and controls on the Manage Node page for adding a ELK Stack node.



You must select at least one feature. Elasticsearch and Kibana can be added in the same node.

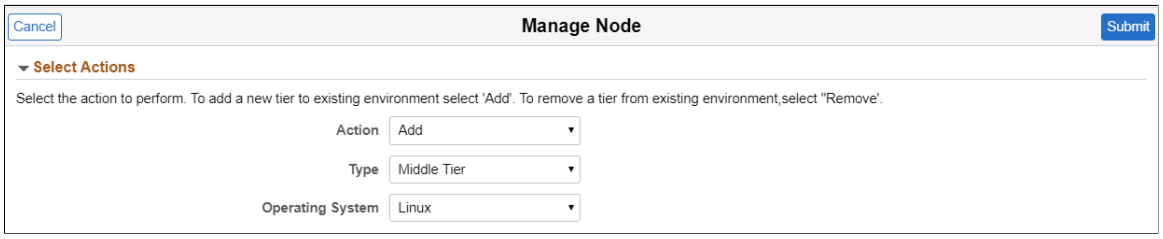
See Creating ELK Stack Node.

Adding Middle Tier Node

This is an example of adding a middle tier node to an environment.

Image: Add Middle Tier Node example

This example illustrates the fields and controls on the Manage Node page to add a Linux middle tier node.



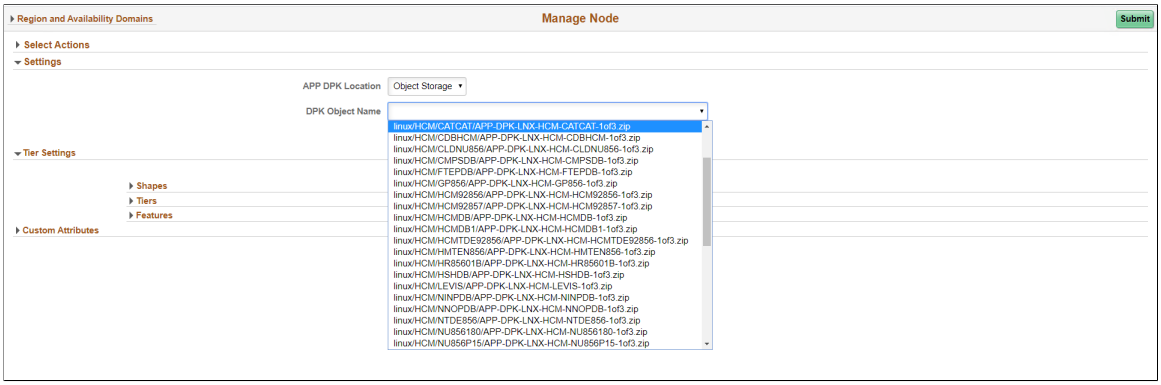
In the Settings section, select the location of the Application DPK.

- Object Store

  When you select Object Store, the DPK Object Name drop down list will display all the application DPK files in Object Store.

  ### Image: Application DPK in Object Store

  This example illustrates the fields and controls on the Manage Node page where the Application DPK location is Object Store.

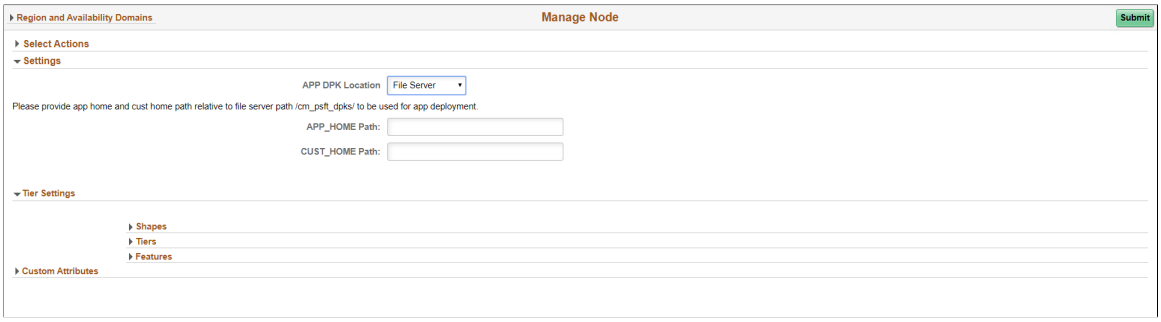


- File Server

  If you manually copied app home and cust home to the file server provide the relative path to the file server.

Image: Application DPK in File Server

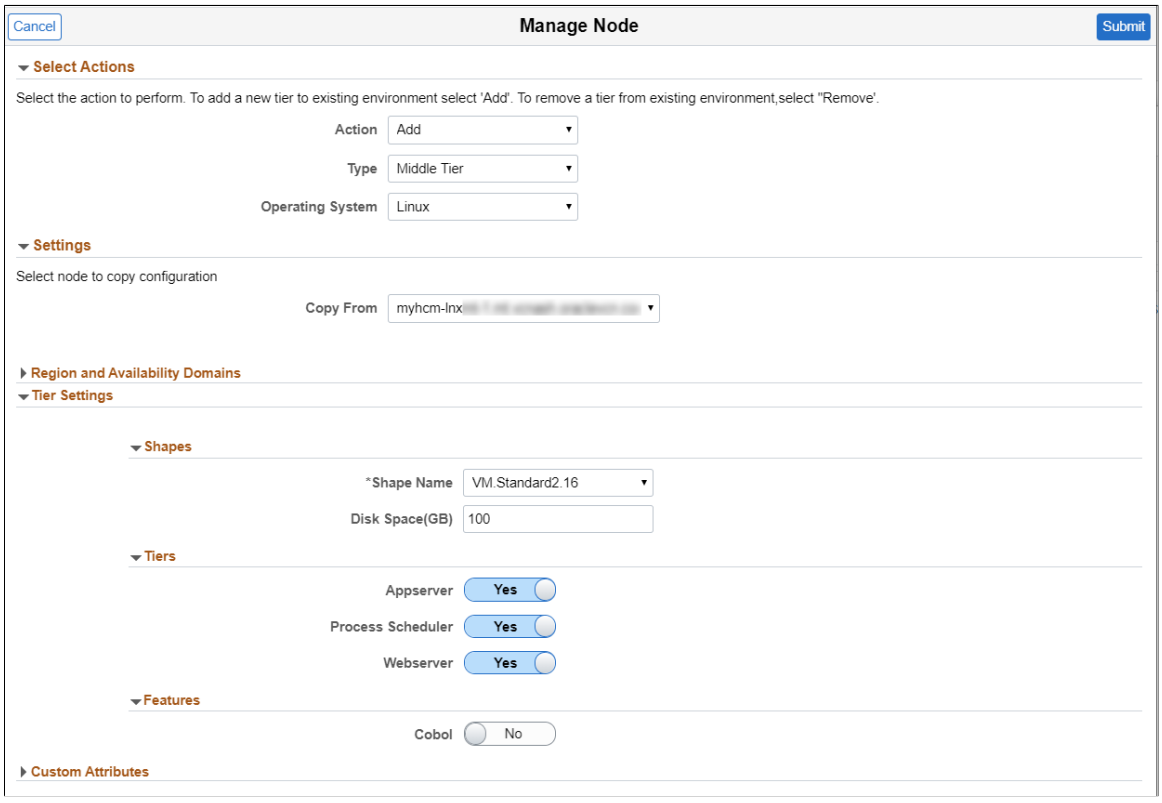
This example illustrates the fields and controls on the Manage Node page where the Application DPK location is File Server.



Adding Additional Middle Tier Nodes

Image: Manage Node page – Add Middle Tier Node

This example illustrates the fields and controls on the Manage Node page for adding a Linux middle tier node.



Expand the sections.

Action Available actions are:

- Add
- Remove

Type	Available Types are: • Middle Tier • PeopleSoft Client • ELK Stack **Note:** The options are enabled based on which node is already available in the environment.
Operating System	Select either Linux or Windows.
Copy From	If a middle tier exists for the environment, select the middle tier node from the drop down list. The configuration/custom configuration will be retrieved.
Regions and Availability Domains	Defaults to the Regions and Availability settings of the environment to which new node is being added. These fields are read only.
Tier Settings	Enter the required Shapes and Tiers. See Environment Template – Select Topology Page
Custom Attributes	Enter Credentials, General Settings, Network Settings, Network Security Group Settings, Fault Domain Settings and Domain Settings. Network Settings for compartment and virtual cloud network are read only. Select the subnet for the primary instance. See Configuring Custom Attributes

Removing Nodes

To remove a node:

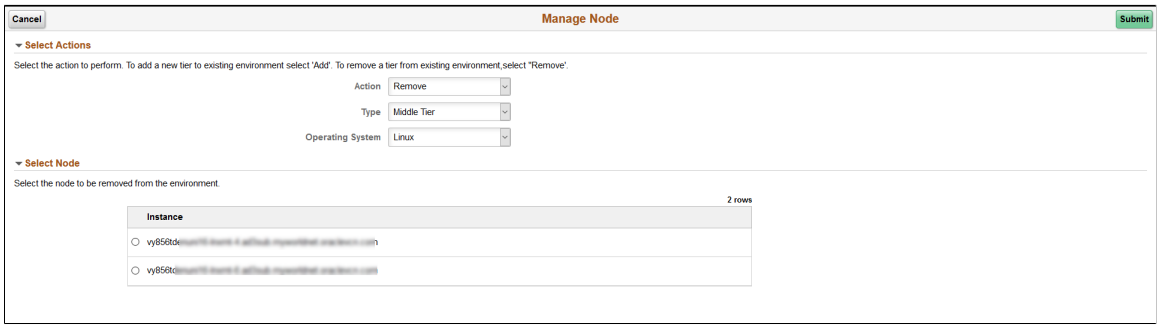
1. Click the Related Actions button corresponding to the environment.
2. Select Manage Node.
3. Select Remove action.
4. Select Type.
5. Available Nodes will be displayed.

   Note: Database node can not be deleted.

6. Select the node to remove.
7. Click Submit and confirm.

Image: Manage Node page – Remove Middle Tier Node

This example illustrates the fields and controls on the Manage Node page for removing a node.



Retrying and Resuming Provisioning

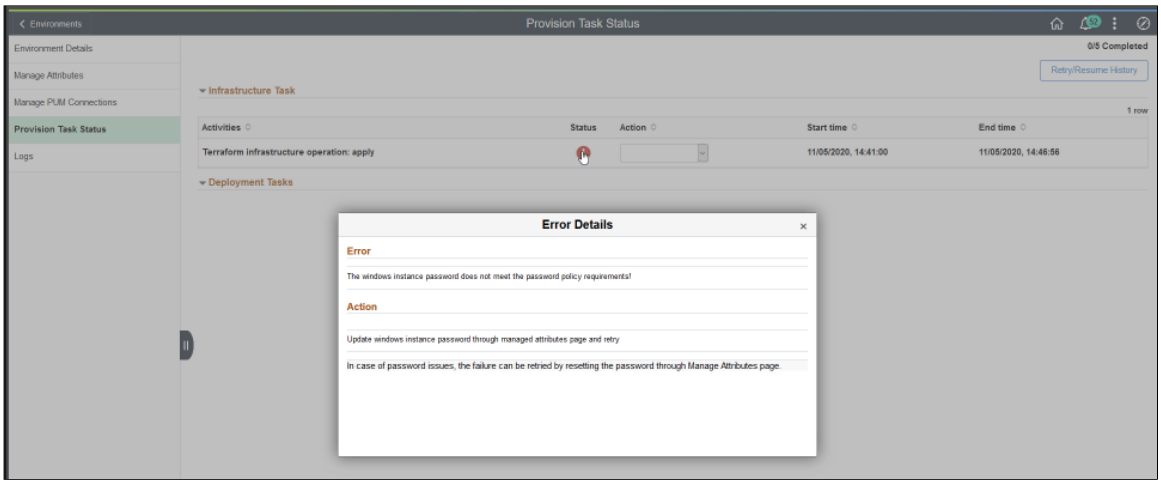
Cloud Manager provides the ability to resume provisioning when a recoverable failure occurs. This applies to provisioning a new environment, shifting an environment or adding nodes using Manage Node action.

To view the failed task:

1. Select the Environments tile.
2. Select Details for the environment.
3. Select Provision Task Status.
4. Click on the Failed icon to view the error.

   Image: Provision Task Status showing failed task

   This example illustrates the fields and controls on the Provision Task Status showing failed task.



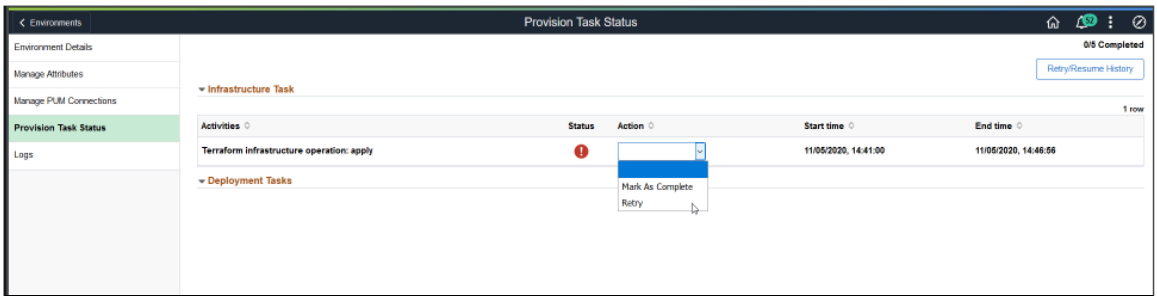
5. The Error Details will indicate the action to be performed to correct the error. The logs will also provide error details.
6. After correcting the error, return to the Provision Task Status.

7. Select the action from the drop down list..

Note: Only activities can be retried.

Image: Provision Task Status Retry/Resume

This example illustrates the fields and controls on the Provision Task Status Retry/Resume.



Mark as Complete — If you manually corrected the error, select this action to mark the failed task as complete and continue with the next task.

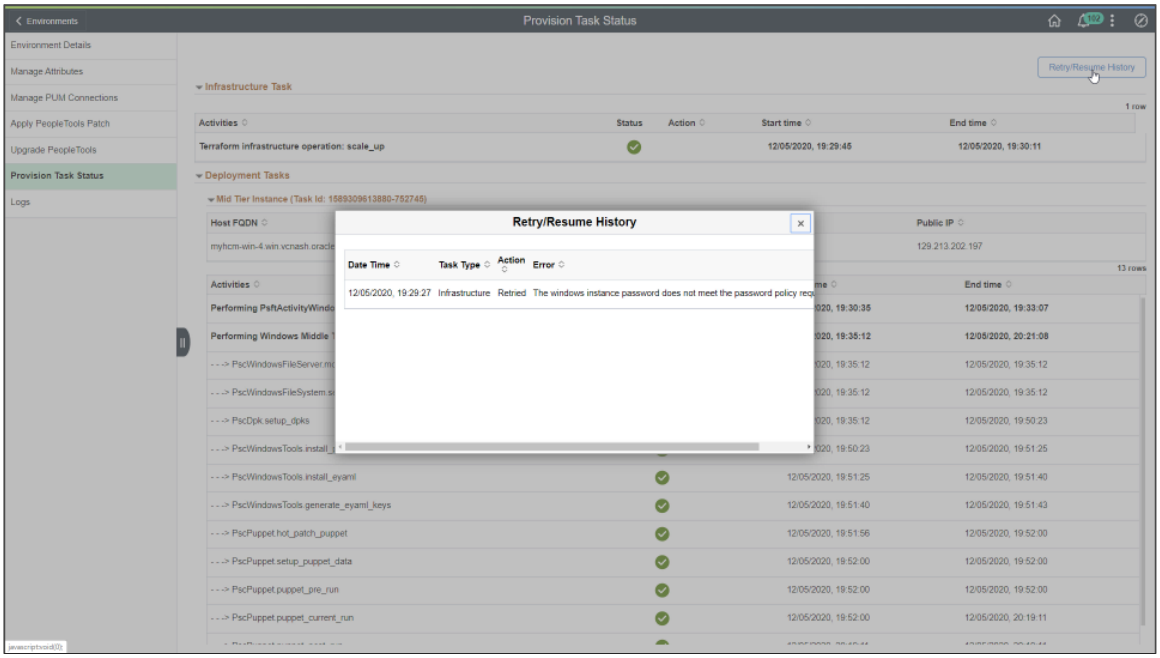
Warning! Manually corrected errors are not validated by Cloud Manager.

Retry — Select this action to retry the task with the updated attributes.

8. The Failed task is retried and provisioning continues.
9. Use the Retry/Resume History button to review any failed tasks.

Image: Retry/Resume History page

This example illustrates the fields and controls on the Retry/Resume History page where provisioning is complete.



Backing Up and Restoring Environment

Use the Backup and Restore action to take a backup or restore an environment from the backup. Backup action will backup all nodes in the environment.

The time to backup and restore depends on the size of the database. The system will be online and reads are not affected. Import, Clone, Update and Instance restarts might affect the backup process.

Backing Up the Environment

It is recommended to take a backup:

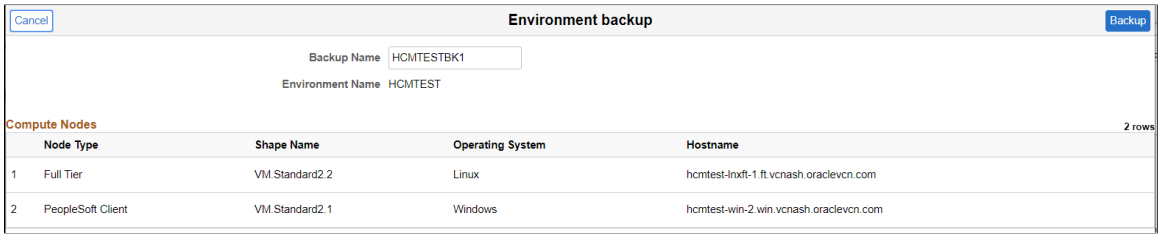
- Before applying a PeopleTools Patch.
- Before applying a PeopleTools upgrade.
- Before adding or removing a node.

To create a backup:

1. On the Environments page, select related actions for the environment and select Backup/Restore.
2. Any existing backup for the environment will be displayed.
3. Click the Create Backup button.
4. Enter the backup name and click Backup. The backup name has to be unique.

Image: Environment Backup page

This example illustrates the fields and controls on the Environment Backup page. You can find definitions for the fields and controls later on this page.

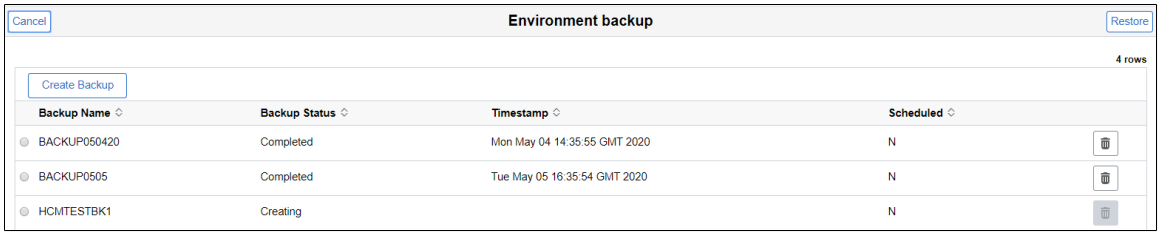


The nodes for the environment are displayed on the Environment Backup page.

The backups for an environment are displayed with the status.

Image: Backup Status

This example illustrates the fields and controls on the Environment Backup page showing the current status. You can find definitions for the fields and controls later on this page.



Backup Name Name of the backup

Backup Status Displays the current status, Creating, In-Progress, Completed or Error.

Timestamp Time the backup was created.

Scheduled Currently backups can not be scheduled, so this column will have N.

Delete icon Click the delete icon to delete an existing backup.

Only backups in the Completed status can be deleted. The delete will clear all the block volumes and other dependency resources in OCI.

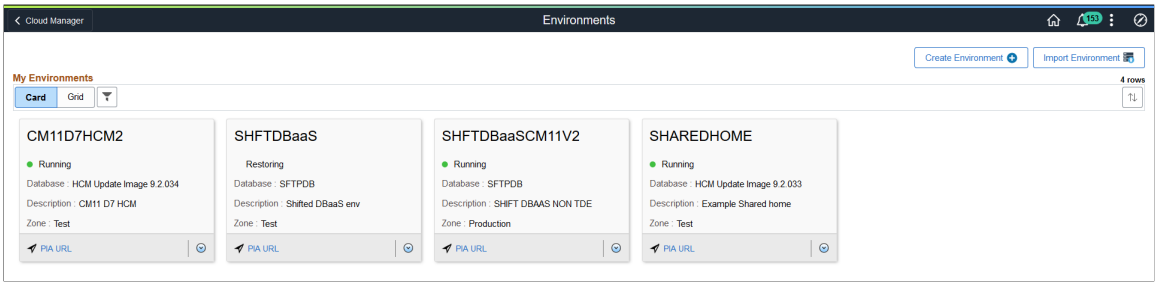
Restoring an Environment

When you select to restore an environment from a backup:

- The Restore overwrites all the data on the target instance.
- The Target instance will be unavailable during the restore process.

Image: Restoring Environment

This example illustrates the fields and controls on the Environments page when an environment is restoring.



- Only one instance at a time can be restored on a target instance.

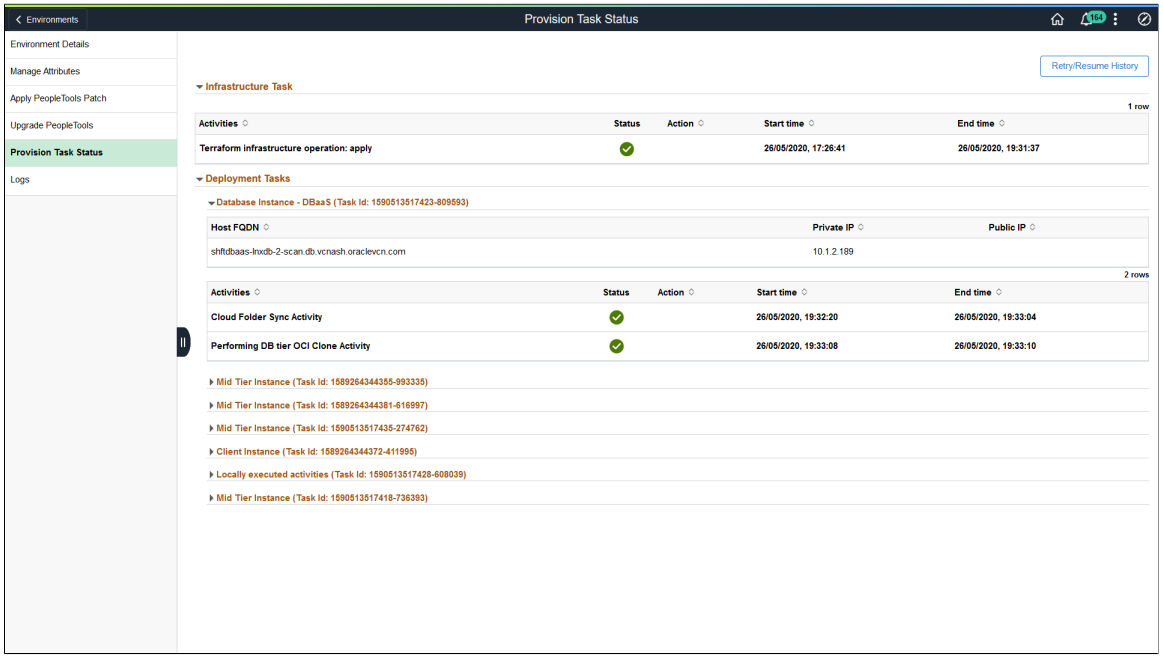
To restore an environment:

1. On the Environments page, select related actions for the environment and select Backup/Restore.
2. Any existing backup for the environment will be displayed.
3. Select the radio button corresponding to the backup you want to restore.
4. Click the Restore button.
5. All the nodes for the selected environment will be restored to the same instance.

Use Provision Task Status on the environment details page to check the progress of the restore operation.

Image: Provision Task Status for restore operation

This example illustrates the fields and controls on the Provision Task Status for restore operation. You can review the deployment tasks.



Refreshing DB Systems Environment

You can refresh DB Systems environments managed by Cloud Manager from a backup in Object Store or from another DB system managed by Cloud Manager.

- The RMAN database backup for an on premise environment lifted to Cloud Manager resides in the Object Store.

  See Running Lift Using Hot Backup (RMAN)

- Backups for other DB Systems environments in Cloud Manager are stored in OCI block storage.

  See Backing Up and Restoring Environment

Refresh supports:

- Refresh database only.
- Refresh environment which includes database, PS App Home and PS Cust Home.

Important! The source and target database must be on the same version. Source environment backup must contain spfile.

To refresh an environment:

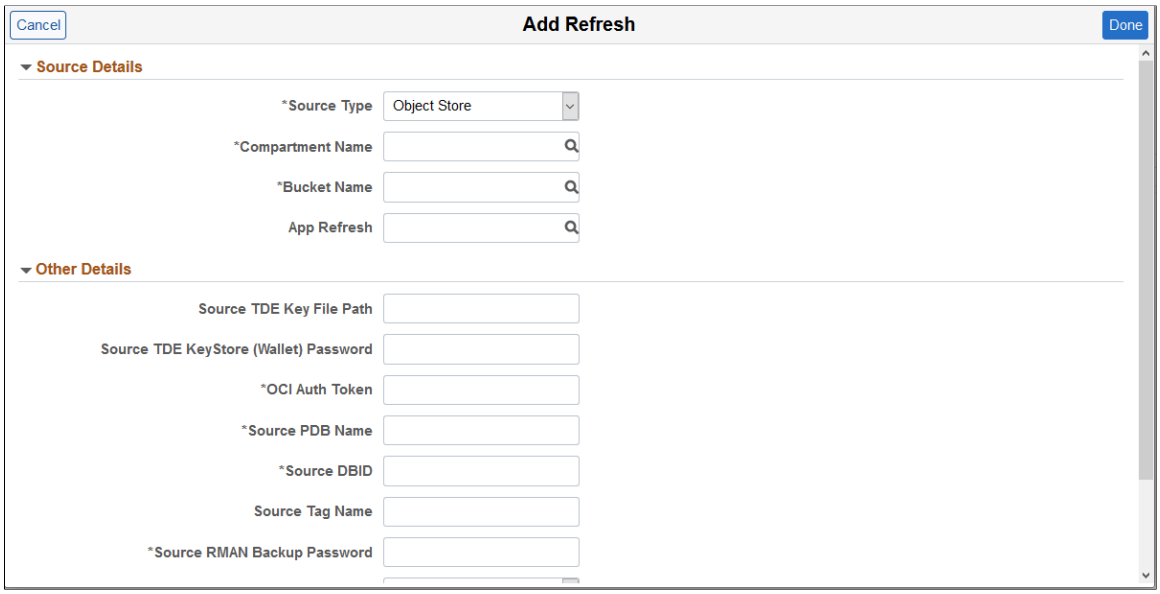
1. Navigate to the Environment tile.
2. Select Refresh from the actions for the DB Systems environment you want to refresh.
3. On the Refresh page, select the Source Type.
4. Enter the values for the backup.
5. Click Refresh.

Note: Perform a backup of the environment prior to the refresh. Before starting the Refresh, ensure that the backup has completed.

Refreshing from Object Store

Image: Add Refresh page where Source Type is Object Store

This example illustrates the fields and controls on the Add Refresh page where Source Type is Object Store. You can find definitions for the fields and controls later on this page.



Source Type Select the Object Store from the drop down list.

Compartment Name Select the compartment used when the backup was taken using DBCLI (database command line interface) or Oracle Database Cloud Backup Module (ODCBM).

Bucket Name Select the bucket name used when the backup was taken using DBCLI (database command line interface) or Oracle Database Cloud Backup Module (ODCBM).

App Refresh Select the name of the application backup to refresh PS App Home and PS Cust home.

Leave this field blank if you want to refresh the database only.

Source TDE Key File Path If TDE is enabled on the source database enter the TDE key file path.

Source TDE KeyStore (Wallet) Password If TDE is enabled on the source database enter the TDE KeyStore (Wallet) Password.

OCI Auth Token Enter the OCI Auth Token for the source database.

Source PDB Name Select the name used when the backup was taken using DBCLI (database command line interface) or Oracle Database Cloud Backup Module (ODCBM).

Source DBID The source DBID is available during the RMAN backup stage, user must have the source DBID available.

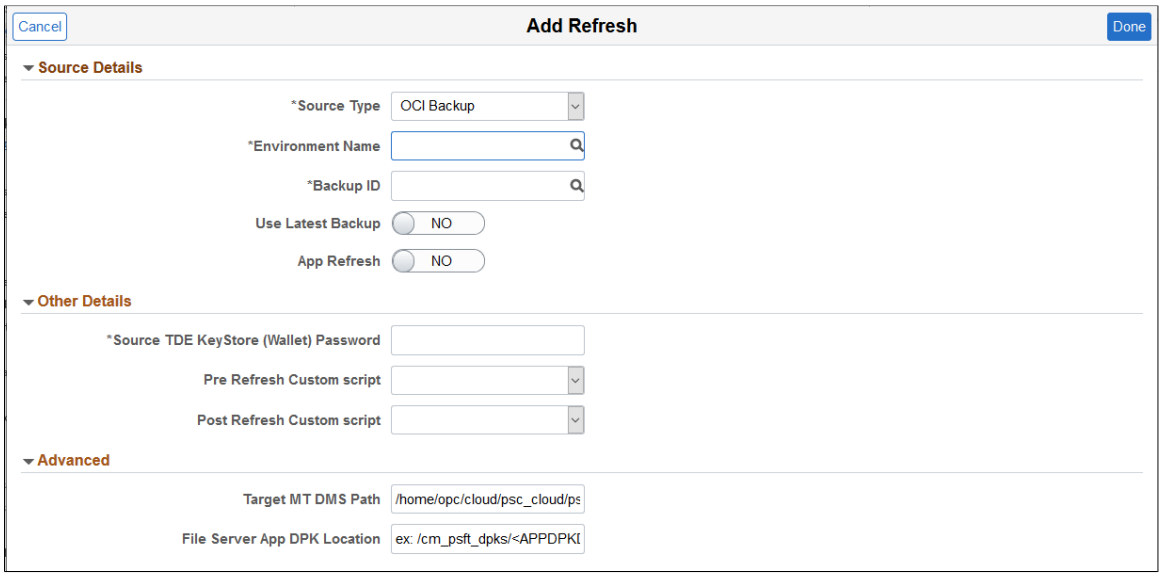
Source Tag Name	The tag name that was specified during the RMAN backup.
Source RMAN Backup Password	Enter the RMAN backup password. This field only applies to non-TDE databases.
Pre Refresh Custom script	Select an uploaded script to execute prior to refreshing the environment. This script is run from a middle tier belonging to the target environment.
Post Refresh Custom script	Select an uploaded script to execute post refreshing the environment. This script is run from a middle tier belonging to the target environment.
Target MT DMS Path	Path to Data Mover scripts on the target middle tier node.

Note: Application DPK contains the absolute path in Cloud Manager for PS_APP_HOME and PS_CUST_HOME. If application DPK only includes PS_APP_HOME, only PS_APP_HOME of target will be refreshed, otherwise both PS_APP_HOME and PS_CUST_HOME will be refreshed.

Refreshing from OCI Backup

Image: Add Refresh page where Source Type is OCI Backup

This example illustrates the fields and controls on the Add Refresh page where Source Type is OCI Backup. You can find definitions for the fields and controls later on this page.



Source Type	Select OCI Backup from the drop down list.
Environment Name	Select the environment to refresh from the drop down list.
Backup ID	Select the Backup ID from the drop down list.
Use Latest Backup	Select Yes to use the latest backup.
App Refresh	Select Yes to refresh PS App Home and PS Cust Home as well as the database.

	Select No for a database refresh only.
Source TDE KeyStore (Wallet) Password	The Source Wallet password is the same as the Database Administrator password.
Pre Refresh Custom script	Select an uploaded script to execute prior to refreshing the environment. This script is run from a middle tier belonging to the target environment.
Post Refresh Custom script	Select an uploaded script to execute post refreshing the environment. This script is run from a middle tier belonging to the target environment.
Target MT DMS Path	Path to Data Mover scripts on the target middle tier node.

Retrieving Failed Refresh

Important! Before doing refresh make sure that an environment backup is done.

To retrieve failed refresh:

1. Select Details > Environment Details and click Refresh.

   Environment may come to Running state.

2. If status updates to Not Started, check the following:

   - PDB, CDB name after refresh may differ from the actual. Correct the names.
   - DB Admin, access usernames and passwords may differ from actual. Correct DB credentials.

3. If status still results in failed status, check Details > Provision Task Status.

   - If failure is in INFRA task, retry from Provision Task Status page.
   - If that does not work, use the backup and restore feature to restore the environment.
   - Make sure spfile is present.

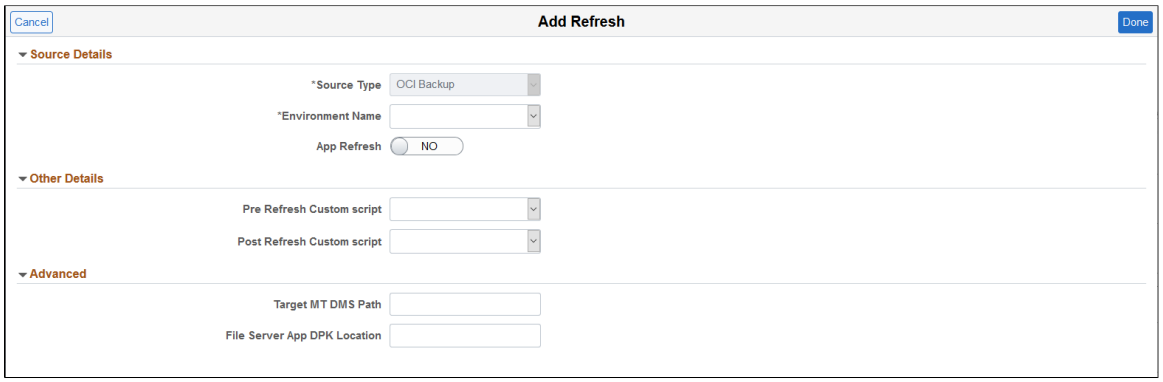
Refreshing ATP-D Environment

To refresh a ATP-D environments, select the Refresh from the actions for the ATP-D environment you want to refresh.

The Source Type option is read only because the target is created from source directly without taking a backup of the source.

Image: Add Refresh page for ATP-D environment

This example illustrates the fields and controls on the Add Refresh page for ATP-D environment. You can find definitions for the fields and controls later on this page.



Environment Name Select the environment to refresh from the drop down list.

App Refresh Select Yes to refresh PS App Home and PS Cust Home as well as the database.

Select No for a database refresh only.

Pre Refresh Custom script Select an uploaded script to execute prior to refreshing the environment. This script is run from a middle tier belonging to the target environment.

Post Refresh Custom script Select an uploaded script to execute post refreshing the environment. This script is run from a middle tier belonging to the target environment.

Target MT DMS Path Path to Data Mover scripts on the target middle tier node.

File Server App DPK Location Location of Application DPK.

Chapter 4

Using Governance Framework

Understanding Governance Framework

Cloud Manger provides the ability to define and manage policies. Using the governance framework, administrators can manage life cycle activities of environments. Policies can be scheduled or executed realtime by connecting through events.

A policy is made up of two parts - conditions and actions. For example, the policy for backing up of all environments every Friday at 10 PM would have the following condition and action:

- Condition: Execute the policy at 10PM every Friday
- Action: Backup of all environments

After defining policies, the policies can be associated with environments using one of the following:

- Specify the environments for the policy when creating the policy using the Policy Editor.

  See Setting Policy Conditions and Action

- Specify policies for an environment from the Environment Policies page.

  See Policies Page

- Specify the policies in the Environment Template used to create the environment.

  See Environment Template – Security and Policies Page

Using Policy Editor

To access the Policy Editor (ECL_POLICY_EDITOR), select the Governance tile.

The Policy Editor is used to add policies, as well as manage existing policies. Policies will be displayed by Policy Group. Policy groups are optional and can be used to group policies together for display. Any policies that are not associated with a specific policy group will be shown under Default Policies.

See Creating Policy Groups

Adding a Policy

When you add a policy, the owner is the user who defined the policy. The owner can be an administrator user or a self service user.

Policies defined by an administrator can be applied on any policy object artifact. For example, if an administrator adds a policy for stopping environments, then all the environments available in the Cloud Manager instance (irrespective of which user created the environment) can be associated with the policies.

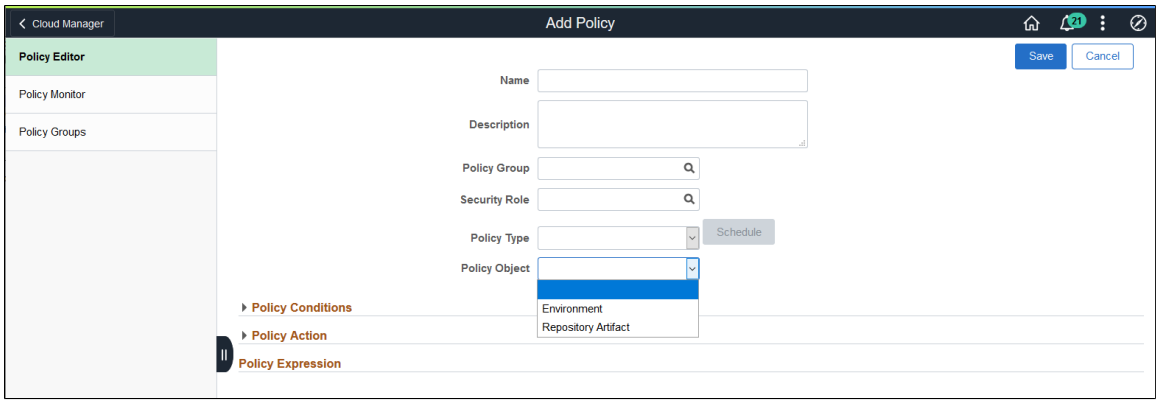
Policies created by a self service user can be applied to the environments created by that user.

To add a policy:

1. Select the Governance tile.
2. Click the Add Policy button.

Image: Add Policy page

This example illustrates the fields and controls on the Add Policy page. You can find definitions for the fields and controls later on this page.



Name Enter a name for the policy.

Description Enter a description for the policy.

Policy Group Policy groups are used to group policies together. The policy does not need to belong to a group.

Security Role Select the security role that can edit the policy.

Policy Type Select the policy type.

- Schedule

  Policy can be scheduled for a start date and time or recurrence.

- Event

  Based on an event, for example PRPs are downloaded.

Schedule This button is available when the policy type is Schedule. Select to set the policy schedule.

See Setting Policy Schedule

Policy Object

A Policy object exposes properties and actions, which are used by the Policy editor to set policy conditions and action for the policy.

Built-in policy objects are:

- Environment

  Used for creating policies for lifecyle activities on environments, for example start and stop.

- Repository Artifact

  Used for creating policies based on artifacts in the repository.

Setting Policy Schedule

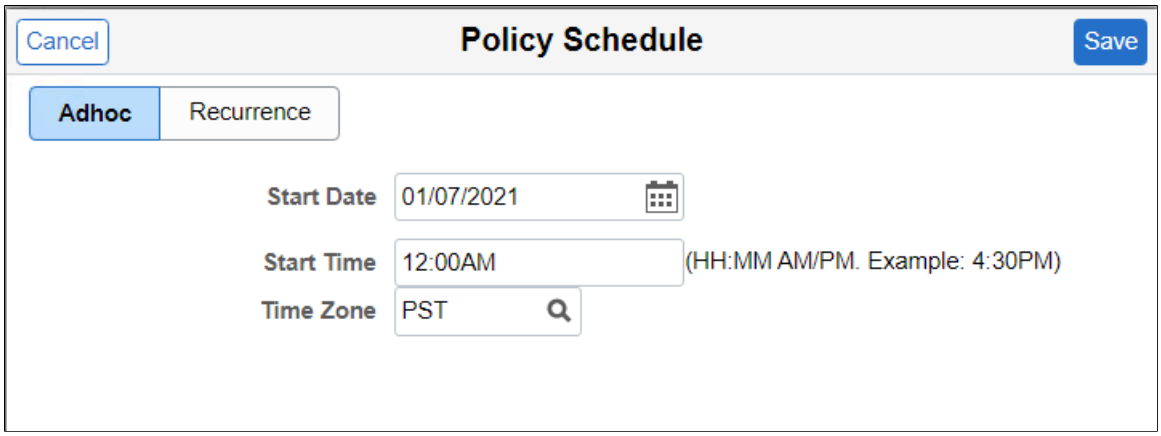
When you select the Schedule button from the Add Policy page, you can select to create an adhoc schedule or a recurrence.

Adhoc

Select Adhoc if you want to schedule the policy for a specific data and time.

Image: Adhoc Policy Schedule

This example illustrates the fields and controls on the Adhoc Policy Schedule page. You can find definitions for the fields and controls later on this page.



Start Date Select the start date.

Start Time Enter the start time.

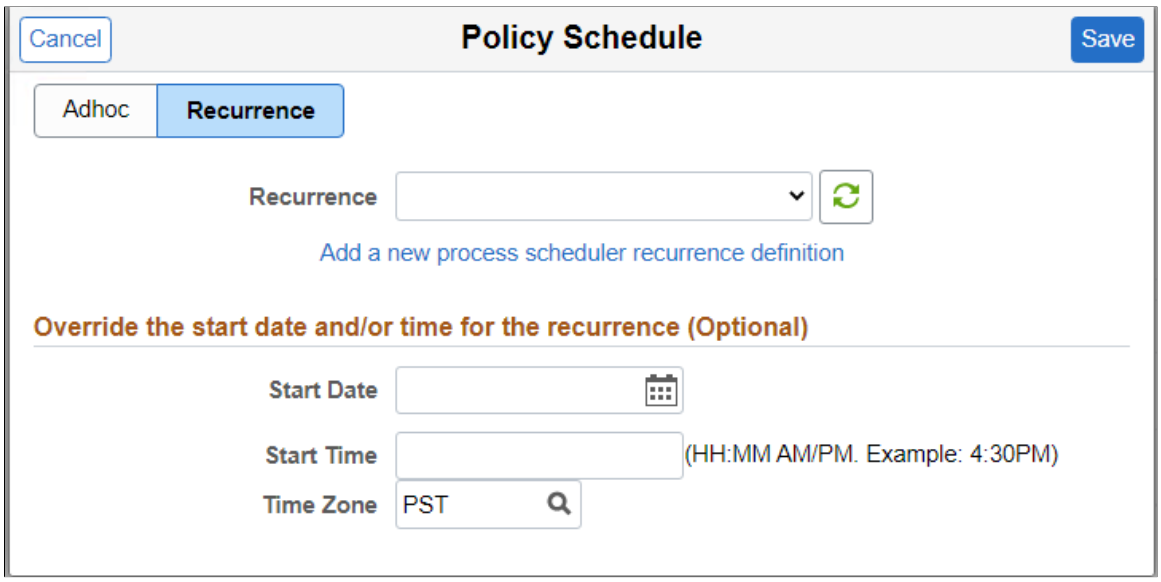
Time Zone Select the time zone.

Recurrence

Select Recurrence if you want the policy to be executed on a recurrence schedule.

Image: Recurrence Policy Schedule

This example illustrates the fields and controls on the Recurrence Policy Schedule page. You can find definitions for the fields and controls later on this page.



Recurrence	Select an existing process scheduler recurrence schedule.
Add a new process scheduler recurrence definition	Select this link if you want to add a new recurrence definition. This link will open the Process Scheduler Recurrence Definition page.
Start Date	Optionally, you can enter a start date for this recurrence.
Start Time	Optionally, you can enter a start time for this recurrence.
Time Zone	Optionally, you can enter a time zone for this recurrence.

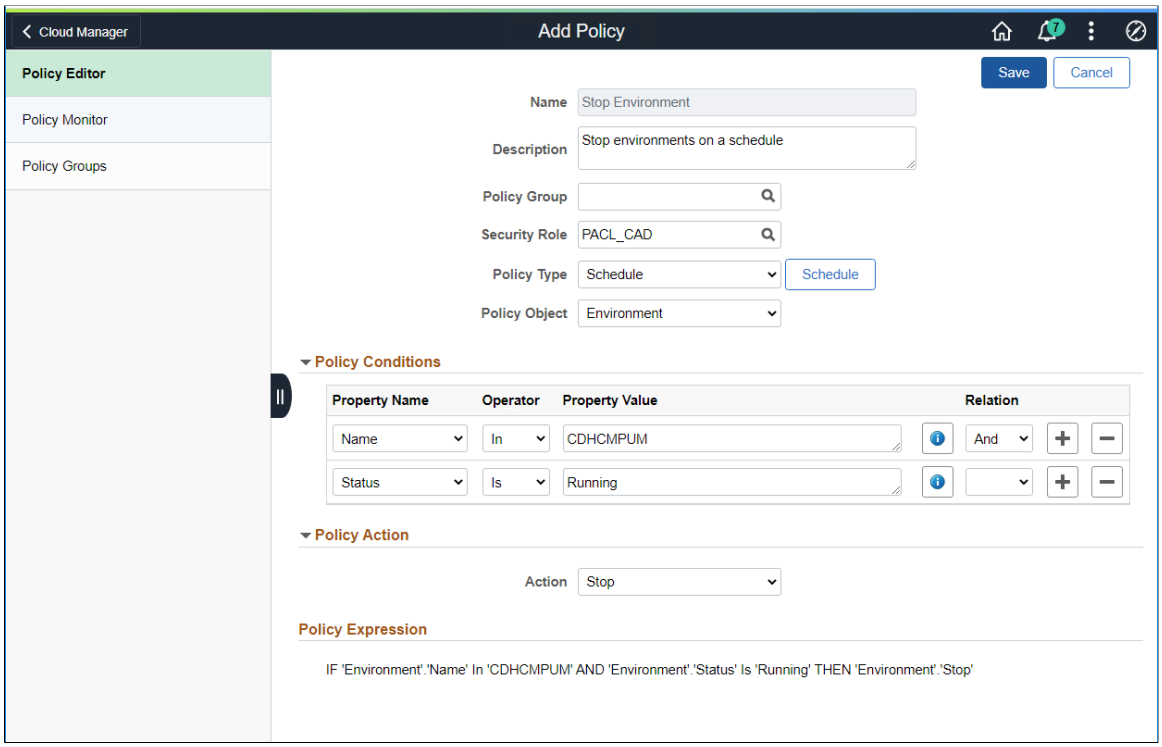
Setting Policy Conditions and Action

Based on the policy object selected, the policy conditions and action will change.

Environment Example

Image: Example Adding Environment Policy

This example illustrates the fields and controls on the Add Policy page where the Object Type is Environment. You can find definitions for the fields and controls later on this page.



Property Name

Select the property name:

- Event Type

  Only applies to event based policies.

- Name
- Status

Operator

Select either In or Is.

Property Value

Enter the property value.

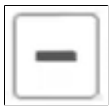
Enter a single value or a comma separated list of values.

Mouse over this icon for an explanation of the property and example values.

Relation

Select the relation.

Select to add another condition.



Select to delete a condition.

Action

If the policy object is Environment, the available actions are:

- Backup
- Refresh
- ScaleDown
- ScaleUp
- Start
- Stop

Action Parameters

Depending on the policy action selected, the action parameters are displayed. Mandatory actions parameters are prefixed with an asterisk (*) and must be entered. Mouse over the Info icon for the action parameter for information on how to enter the parameter value.

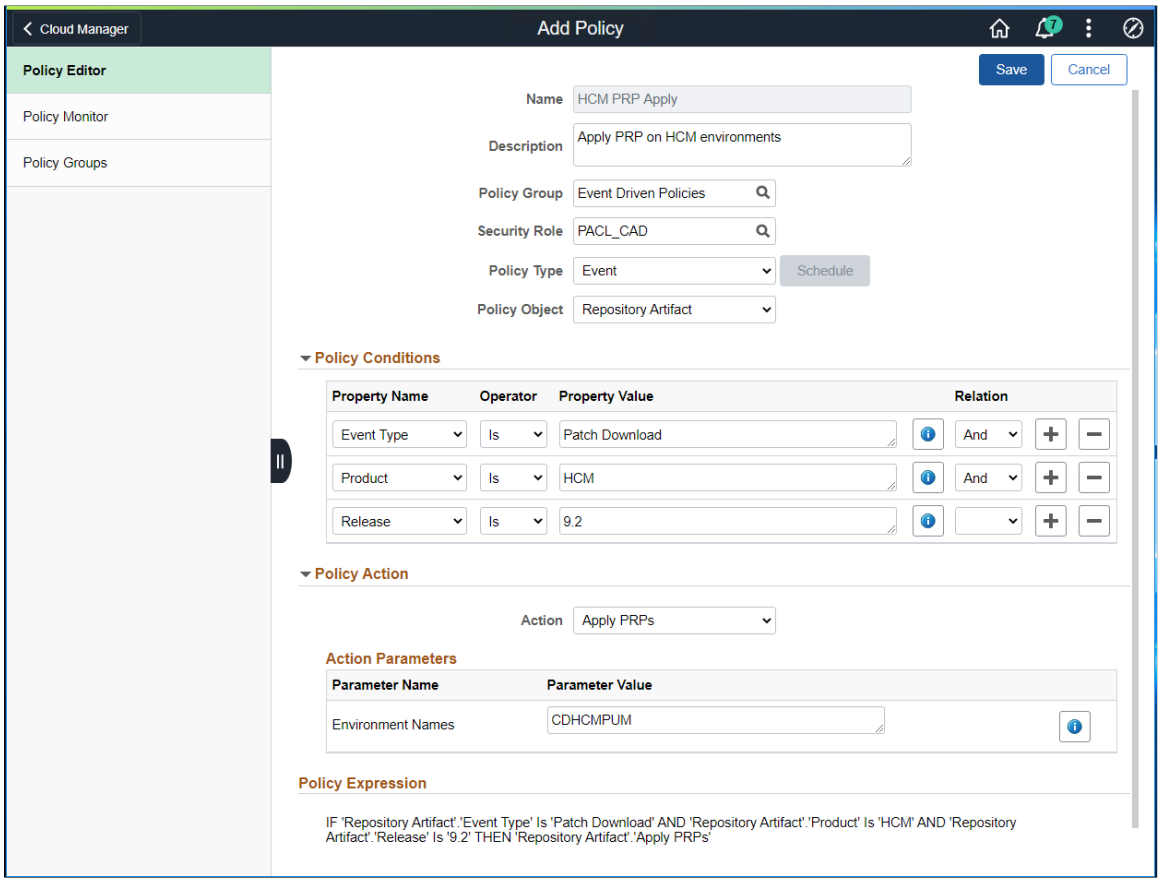
Policy Action	***Action Parameters***
Backup	Backup Prefix
Refresh	Environment Name Backup ID Use Latest Backup App Refresh Source TDE KeyStore (Wallet) Password Pre Refresh Custom script Post Refresh Custom script Target MT DMS Path File Server App DPK Location See Refreshing DB Systems Environment

Policy Action	*Action Parameters*
ScaleDown	Node Count Auto Scale Application Server Domain Process Scheduler Domain PIA Domain
ScaleUp	Node Count Auto Scale Application Server Domain Process Scheduler Domain PIA Domain

Repository Artifact Example

Image: Example Adding Repository Artifact Policy

This example illustrates the fields and controls on the Add Policy page where the Object Type is Repository Artifact. You can find definitions for the fields and controls later on this page.



Property Name Select the property name:

- Event Type
- Product
- Release

Operator Select either In or Is.

Property Value Mouse over the Info icon to view available values. For Event Type property, the only supported value is *Patch Download*.

Use the Info icon to view available values.

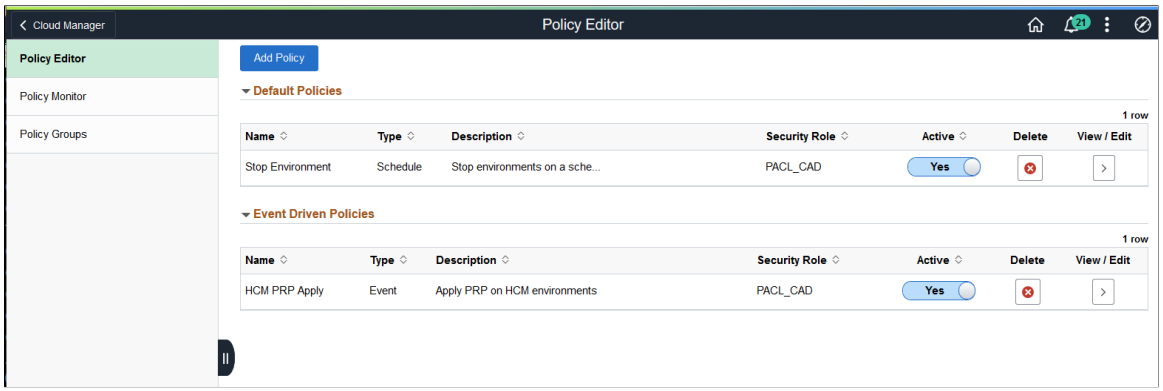
Action Initially the only valid option from the drop down list is Apply PRPs.

Managing Policies

All defined policies are available and grouped by policy group.

Image: Policy Editor page

This example illustrates the fields and controls on the Policy Editor page. You can find definitions for the fields and controls later on this page.



Active — Select Yes or No to activate or inactivate a policy.

Once a policy is inactivated, it will be suspended and will not be executed.

Delete — Use the Delete icon to remove a policy.

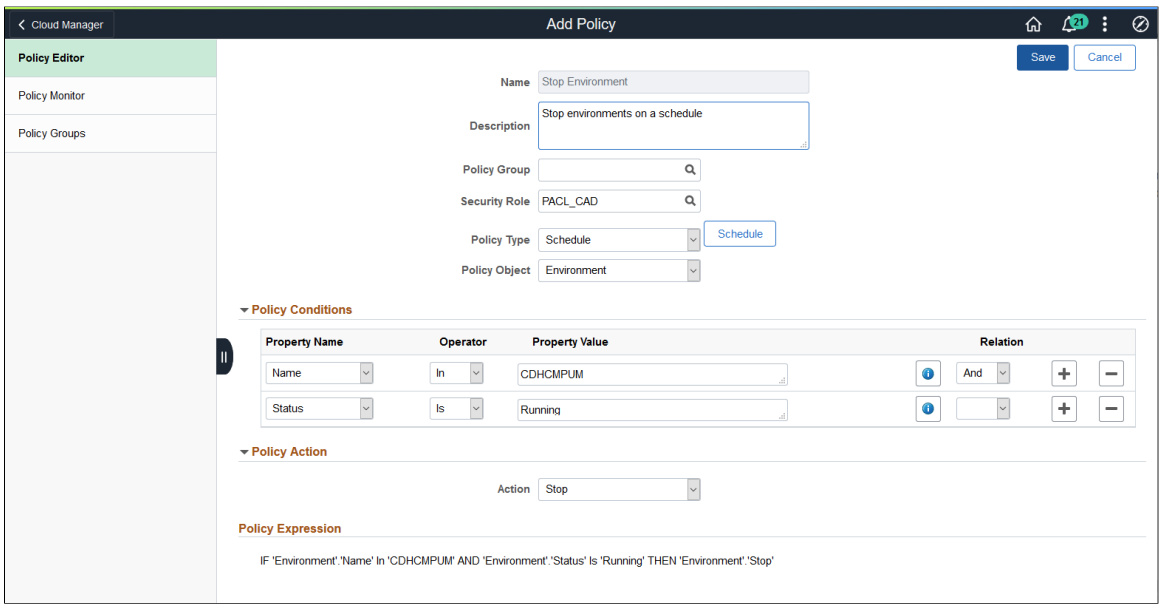
View/Edit — Click the edit icon to view or edit a policy. The user must belong to the security role assigned to the policy in order to edit the policy. If the user does not belong to the security role, the user can view the policy, but can not edit it.

Editing the Policy

When you select to edit or view the policy, the policy is displayed.

Image: Example Edit Policy

This example illustrates the fields and controls on the Add Policy page when you select to edit or view a policy.



Note: Environments can be added to or removed from a policy directly from the Environment Details page. See Policies Page

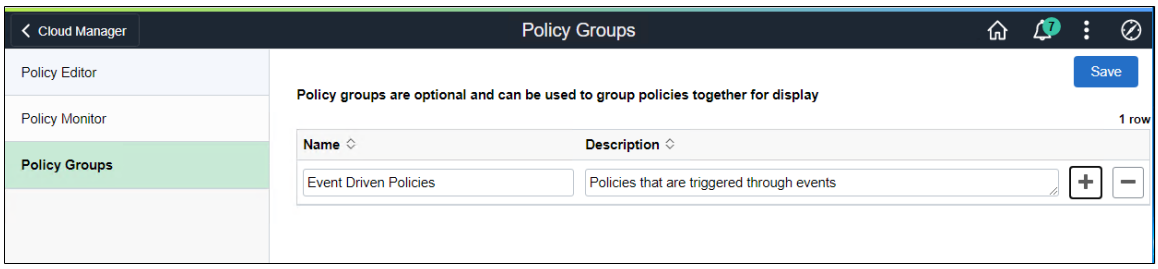
Creating Policy Groups

Policy groups are optional and are used to group policies together for display.

To view or add a policy group, select the Governance tile, then select Policy Group.

Image: Policy Groups page

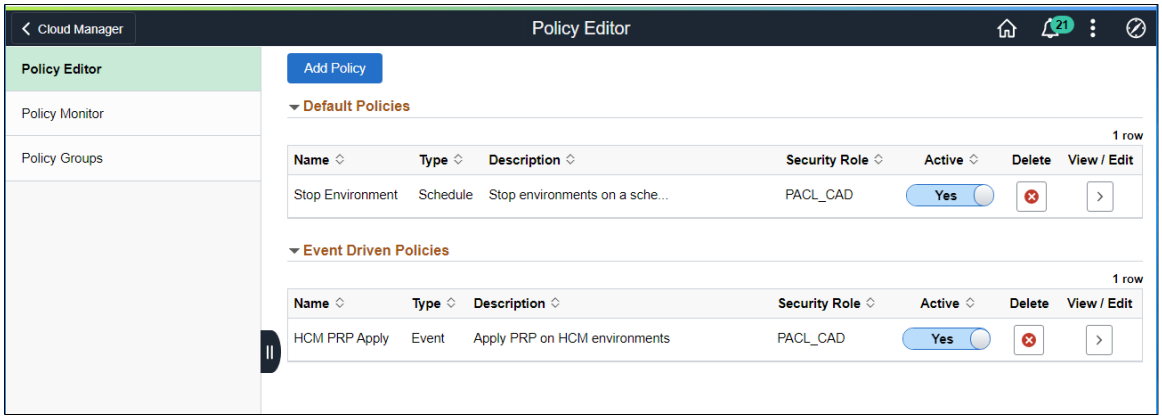
This example illustrates the fields and controls on the Policy Groups page. You can find definitions for the fields and controls later on this page.



When policy groups are created, they will display as such on the Policy Editor page.

Image: Policy Editor with Policy Groups

This example illustrates the fields and controls on the Policy Editor page that contains Policy Groups.

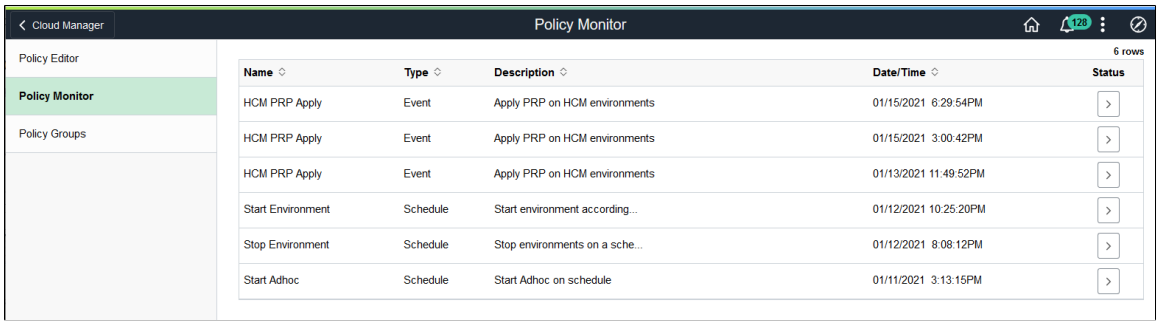


Using Policy Monitor

Use the Policy Monitor page to track the execution status of the policies.

Image: Policy Monitor page

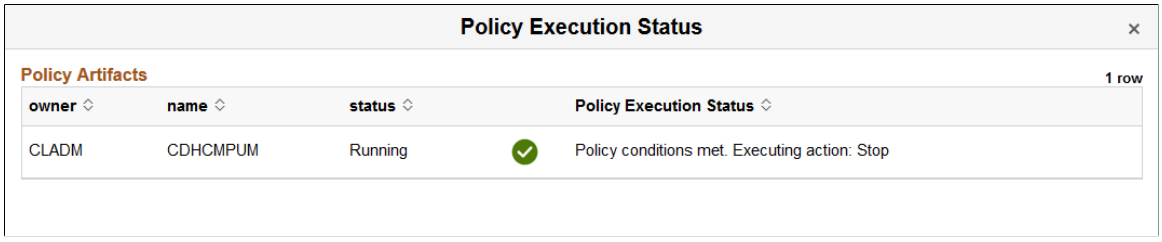
This example illustrates the fields and controls on the Policy Monitor page. You can find definitions for the fields and controls later on this page.



Select the > icon to view the policy execution status.

Image: Policy Execution Status page

This example illustrates the fields and controls on the Policy Execution Status page.



Chapter 5

Managing Alerts and Notifications

Viewing Alerts and Notifications

Alerts and Notifications are used to notify users that new patches have been downloaded and are available for Cloud Manager, as well as the patch details and priority.

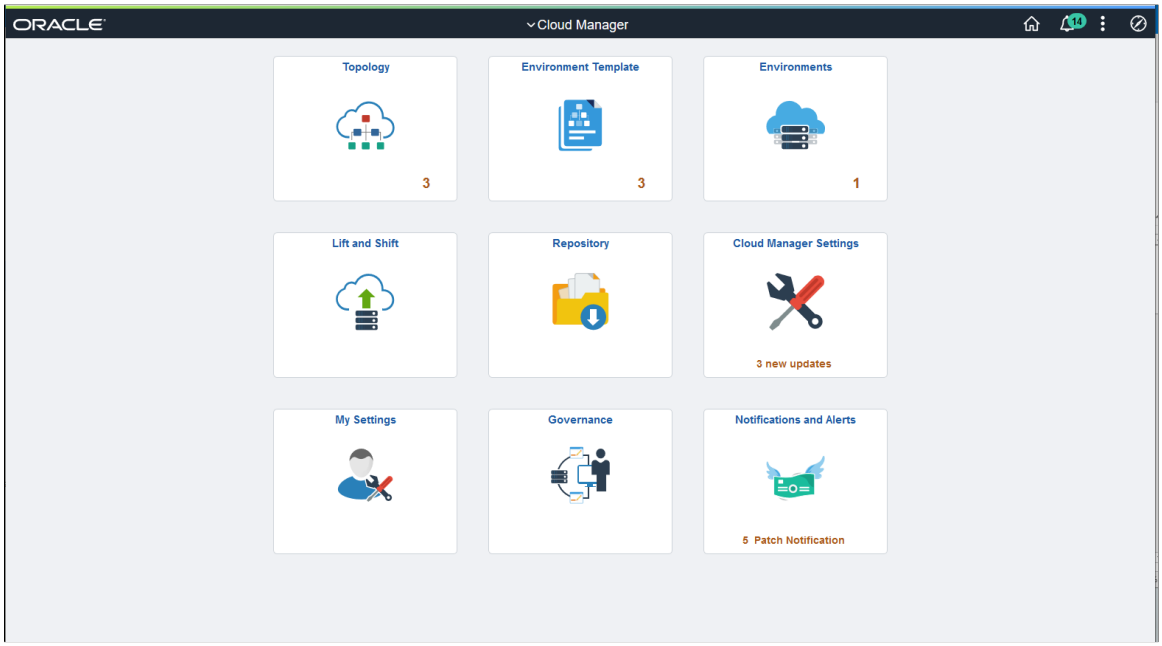
Note: You must subscribe to the IH_91_Linux download channel.

Use the Manage Updates page in Cloud Manager Settings to apply the PRPs. See Updating Cloud Manager Overview

The Alerts and Notifications tile is displayed on the Cloud Manager Homepage. If new patches are available the tile will indicate the number of notifications.

Image: Alerts and Notifications tile

This example illustrates the fields and controls on the Alerts and Notifications tile. You can find definitions for the fields and controls later on this page.



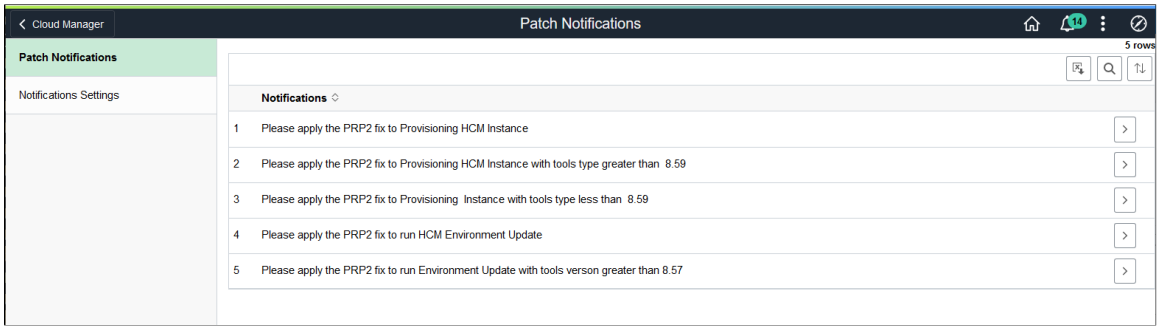
Using the Patch Notifications Page

Select the Alerts and Notifications tile to view the Patch Notifications page.

Note: Only unapplied patch notifications are displayed.

Image: Patch Notifications page

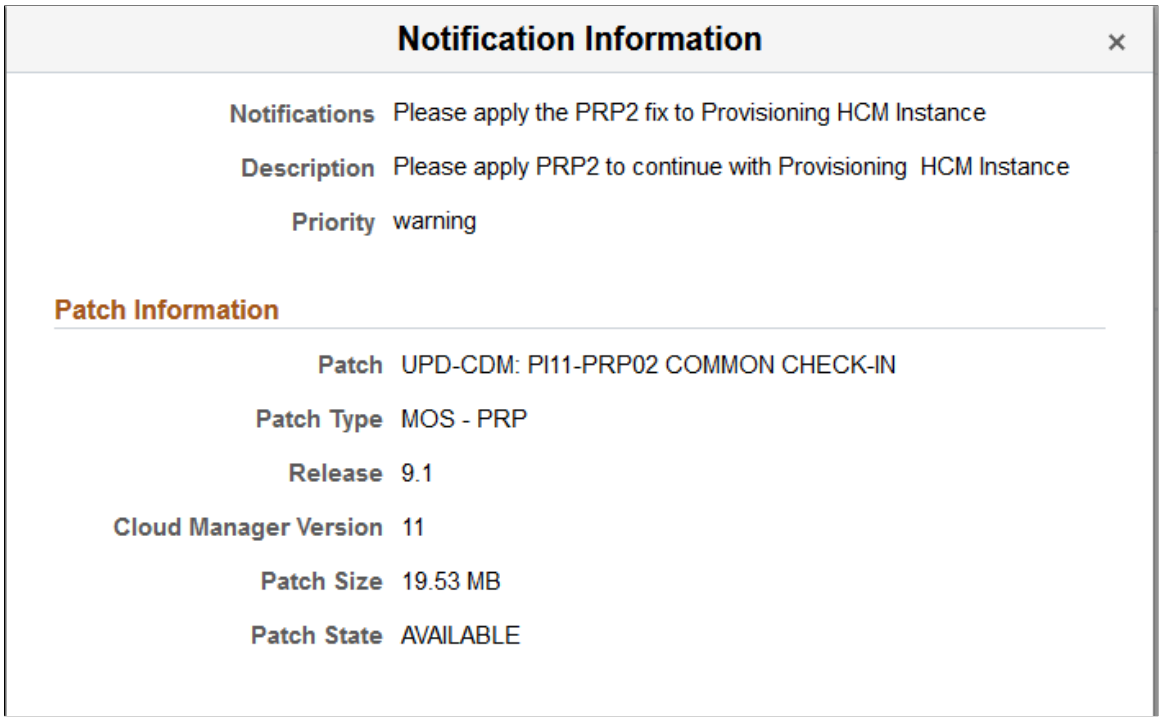
This example illustrates the fields and controls on the Patch Notifications page. You can find definitions for the fields and controls later on this page.



Patch notifications are displayed. Use the > button to view the notification information.

Image: Notification Information

This example illustrates the fields and controls on the Notification Information. You can find definitions for the fields and controls later on this page.



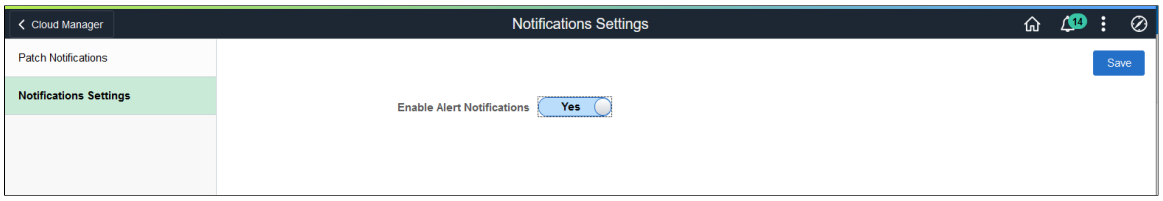
The notification information includes a description and priority, as well as the patch information.

Enabling Notifications

When you enable notifications, you will be alerted if you perform an activity in Cloud Manager that is affected by the patch. For example, you want to create a new environment or apply a PeopleTools patch. To enable notifications, select the Alerts and Notification tile, then select Notification Settings.

Image: Notification Settings page

This example illustrates the fields and controls on the Notification Settings page. You can find definitions for the fields and controls later on this page.



Enable Alert Notifications Select Yes to enable notifications.

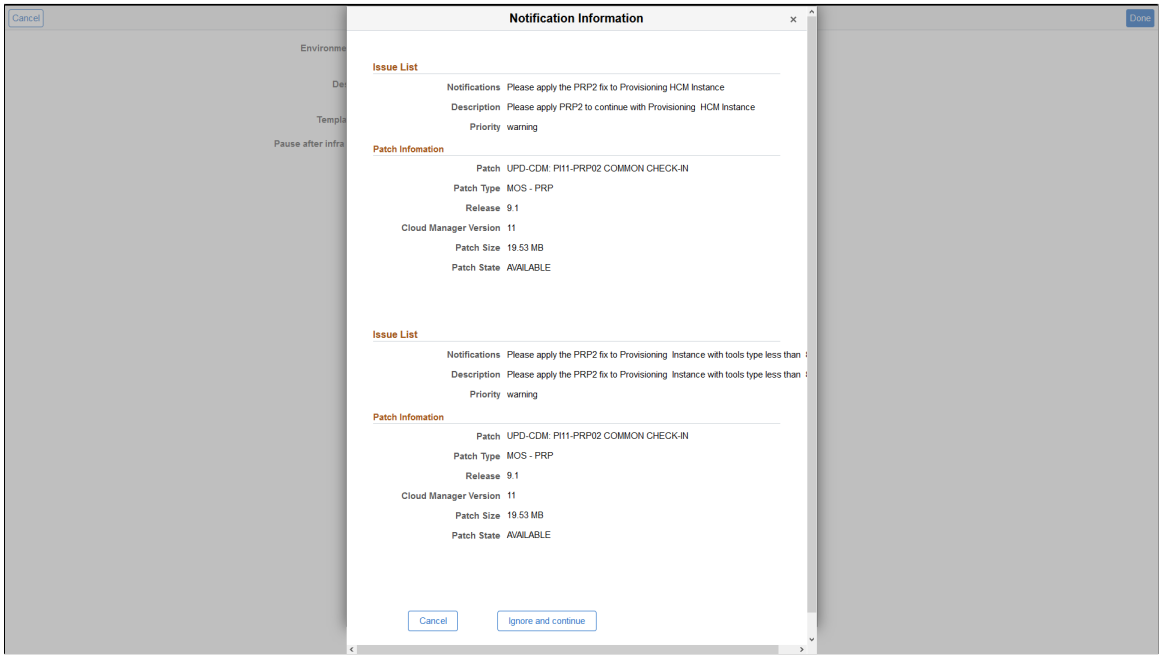
If you select No, you will not receive a notification when performing an activity affected by the patch.

Example Creating Environment

If notifications are enabled and a patch affects creating an environment, a message will be displayed.

Image: Notification when creating an environment

This example illustrates a notification on the Create Environment page, when a patch is available and notifications are enabled.



Cancel Select to cancel.

Apply the patch using the Manage Updates page.

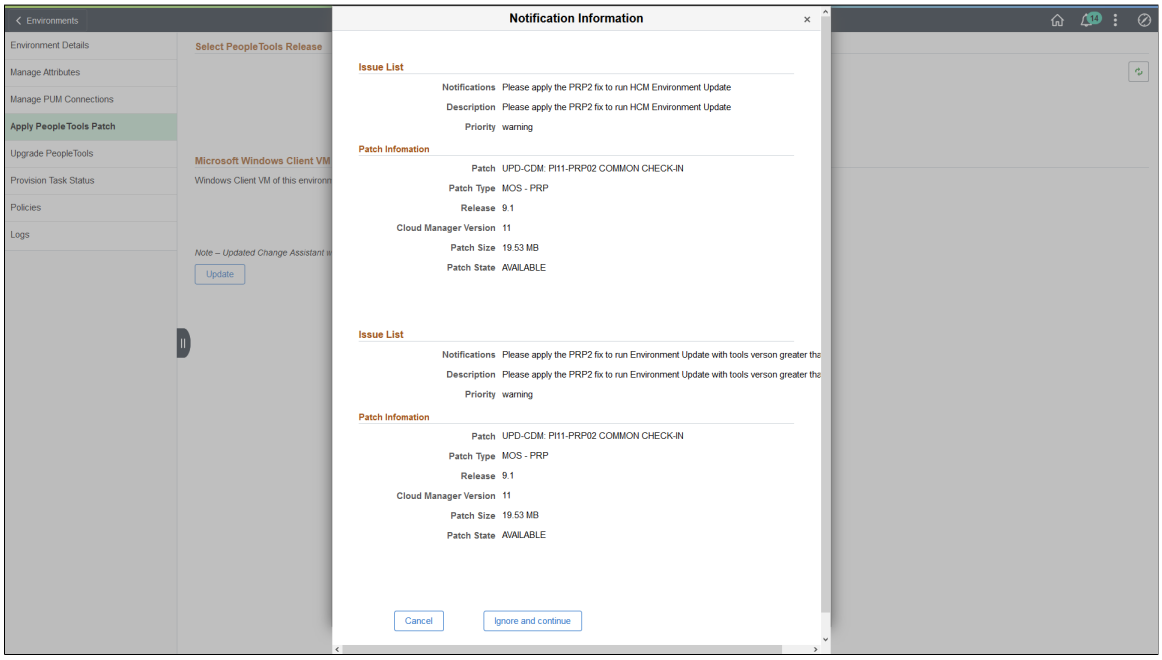
Ignore and continue Select to ignore the notification and continue.

Example Apply PeopleTools Patch

If notifications are enabled and a patch affects applying a PeopleTools patch, a message will be displayed.

Image: Notification when applying a PeopleTools patch

This example illustrates a notification on the Apply PeopleTools Patch page, when a patch is available and notifications are enabled.



Cancel	Select to cancel. Apply the patch using the Manage Updates page.
Ignore and continue	Select to ignore the notification and continue.

Chapter 6

Using the Lift and Shift Process to Migrate On-Premise Environments to Oracle Cloud

Understanding the Lift and Shift Process

The Lift and Shift process in Cloud Manager enables the automated migration of on-premise PeopleSoft environments to Oracle Cloud. Migration to Cloud is achieved in two steps:

- Lift: Using the lift utility provided in Cloud Manager, PeopleSoft Application environment data (for example, PS_APP_HOME, PS_CUST_HOME) is packaged into DPK format and PeopleSoft Oracle database is backed up using RMAN and uploaded to Oracle Object Storage.

  The Lift utility provided in Cloud Manager lifts the application tier (middle tier) and packages it into a DPK. The database tier is independently packaged into a separate DPK.

  Cloud Manager supports database lift using hot backup. Hot backup is performed with RMAN (Recovery Manager) using Oracle Database Cloud Backup Module (ODCBM) that is bundled with the lift utility.

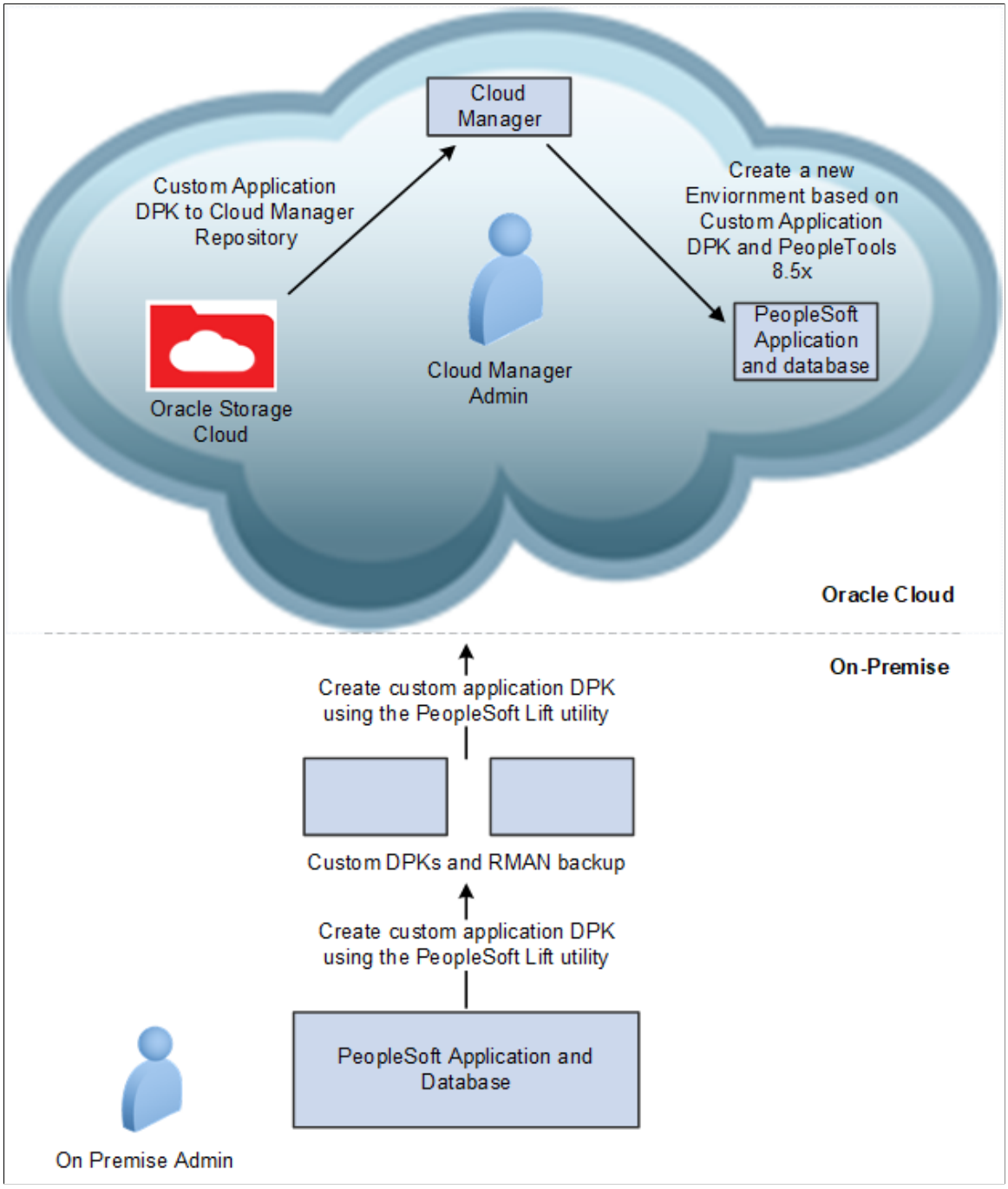
  Note: The DPKs that were lifted using older versions of CM, may not be successfully shifted in later CM versions.

- Shift: Cloud Manager downloads the lifted DPKs and RMAN backup. It then creates a new environment on Oracle Cloud. Once shifted, customers can use Cloud Manager to further manage, scale up or scale down or clone these environments.

  Note: Before doing a Shift action, Lift and Shift topology must be updated with the right VM shapes for each node.

Image: Lift and Shift Process

Overview of the Lift and Shift process



Customers will download the Lift utility from the Cloud Manager and run it on an on-premise environment to create and upload customer application DPKs to the Oracle Cloud Service. Then using Cloud Manager, they use the customer application DPK to create a running application environment intact with all the customizations that have been done on-premise. It is a two-step process that simplifies days of laborious tasks. The Lift and Shift process is helpful to migrate many of your different environments such as demo, development, test and training environments to the Oracle Cloud. Once an environment has been lifted, you can provision as many separate instances as you need.

To migrate a PeopleSoft environment from on-premise to Oracle Cloud using Cloud Manager, it must be on Linux (OEL/RHEL) 6 or above, running application version 9.2 or above. The database must be on Oracle 12c or above and PeopleTools version 8.55 or above.

Using the Lift Process to Migrate an Environment to the Oracle Cloud Infrastructure (OCI)

Pages Used to Migrate the Environment to Oracle Cloud

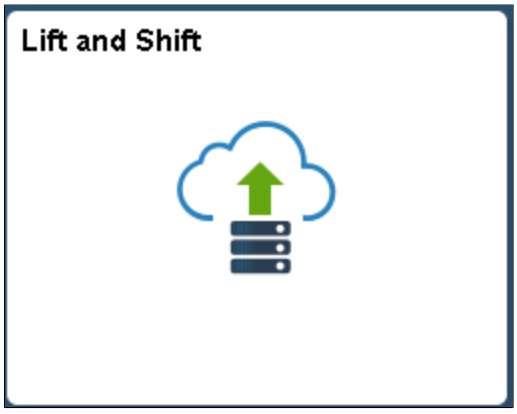
Page Name	*Definition Name*	*Usage*
Lift and Shift Tile	ECL_LAS_HOME_FL_GBL (CREF for the tile)	To access Lift and Shift landing page.
Lift and Shift Page	ECL_LAS_HOME_FL	The landing page containing the lift utility and the lifted containers.

Lift and Shift Tile

Use the Lift and Shift tile (ECL_LAS_HOME_FL_GBL) to access Lift and Shift landing page. The Lift and Shift tile is delivered as part of the Cloud Manager home page.

Image: Lift and Shift Tile

This example illustrates the Lift and Shift tile.



Lift and Shift Page

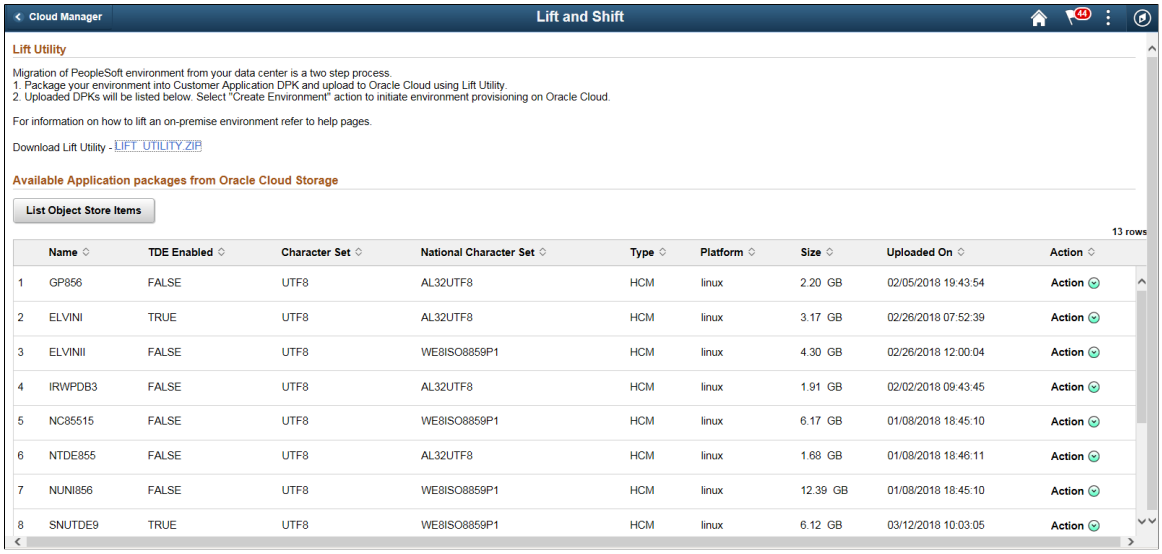
Use the Lift and Shift landing page (ECL_LAS_HOME_FL_GBL) to view and access the lifted environments (uploaded customer DPKs in Oracle Cloud for Cloud Manager).

Navigation

Click the Lift and Shift tile on the delivered Cloud Manager Fluid Home page. The Lift and Shift page is displayed.

Image: Lift and Shift page

This example illustrates the fields and controls on the Lift and Shift page.



Note: Currently, in PeopleSoft Cloud Manager, an updated version of the Lift utility is available that captures more details from on premise environment. DPKs that were lifted earlier using Lift Utility from Cloud Manager Image 8 or older can no longer be deployed in Cloud Manager Image 10. Hence, you must delete those old DPKs and do a lift operation again on the on-premise environments.

Name — Name of the lifted environment.

TDE Enabled — Whether the database has encrypted tablespaces or not.

Character Set — The database character set used for lift operation.

National Character Set — Whether the database is unicode or non unicode. AL32UTF8 indicates unicode database and the value WE8ISO8859P1 indicates non unicode database.

Type — Shows the PeopleSoft application product pillar.

Platform — Indicates the Operating System platform.

Size — Total size of the lifted DPKs.

Note: Assume that if the lifted DPK size is K, then the disk size should be 2.5 times K.

Uploaded On — The date and time on which the DPKs were uploaded in Oracle Cloud.

Action — Use this button to perform a variety of related actions, such as viewing the details of each of the lifted DPKs, provisioning a new environment, and to delete a lifted DPK.

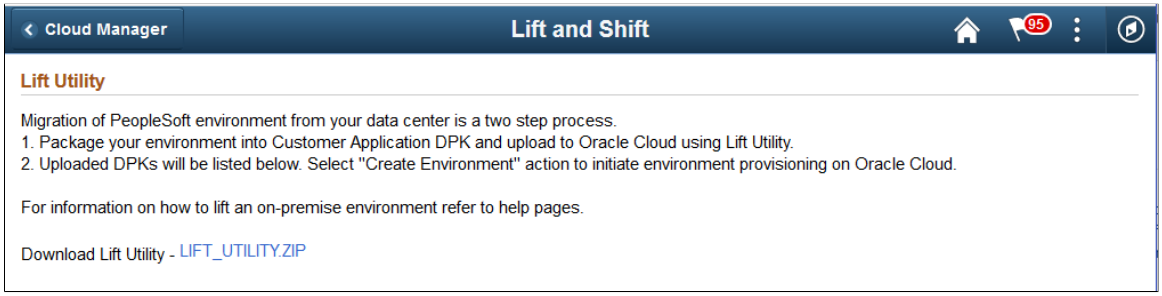
List Object Store Items	Click this button to refresh the lifted application list and make it current.

Downloading the Lift Utility

Navigate to the Lift and Shift page and click on the LIFT_UTILITY.ZIP. Please make sure you have applied any PRPs or fixes to Cloud Manager before downloading the utility. Copy the utility to the on-premise PeopleSoft system that needs to be migrated.

Image: Lift and Shift page

This example illustrates the link to the Lift utility.



Installing Lift Prerequisites

Required Lift Prerequisites Applications

Lift prerequisite applications include:

- Python 3.6
- YUM Modules (gcc, libffi-devel, openssl-devel, zlib, wget)
- PIP Modules (oci-cli, pyyaml, xmltodict, requests, ensurepip)
- Java 1.8 (For database tier instance for RMAN)

Using the Automatic Lift Prerequisite Utility

The Lift prerequisite install feature will verify and install the applications required to perform Application Lift and Database (RMAN) Lift based on the user input.

This Lift prerequisite validation will be triggered in silent mode when the user triggers the Lift utility (psft-osl.sh) to validate the user environment before invoking the Lift to OCI.

Warning! Automatically installing the pre-requisites may update or overwrite any existing version on the system. Please review the packages that will be installed automatically.

Requirements for using this utility:

- Ensure the necessary proxy and ports are set in order to access Internet, download and install the required prerequisite applications.
- Script must be triggered by the root user to install the applications.
- If the customer doesn't permit installation or in an event of failure during installation, the script will exit and the customer would need to install the prerequisites manually.

  See Manually Installing Lift Prerequisites

To automatically install the Lift prerequisite applications:

1. Download and copy the Lift Utility to the On Premise instance.
2. Login as root to the On Premise instance.
3. Extract the Lift utility zip to a temporary folder and set full permissions to the folder.

   ```
   $ mkdir /tmp/CM9_LIFT
   $ unzip LIFT_UTILITY.zip -d <LIFT_UTILITY_PATH>
   $ chmod -R 777 <LIFT_UTILITY_PATH>
   ```

4. Navigate to the below path:

   ```
   $ cd <LIFT_UTILITY_PATH>/setup
   ```

5. Trigger the Lift Prerequisite install script.

   ```
   $ sh psft-lift-setup.sh
   ```

6. Generate the Oracle Cloud Infrastructure Auth Token. See Generating Oracle Cloud Infrastructure Auth Token.

Script Examples for Automatic Lift Prerequisite Utility

When you run the utility, it will ask if this is a database environment or an application environment.

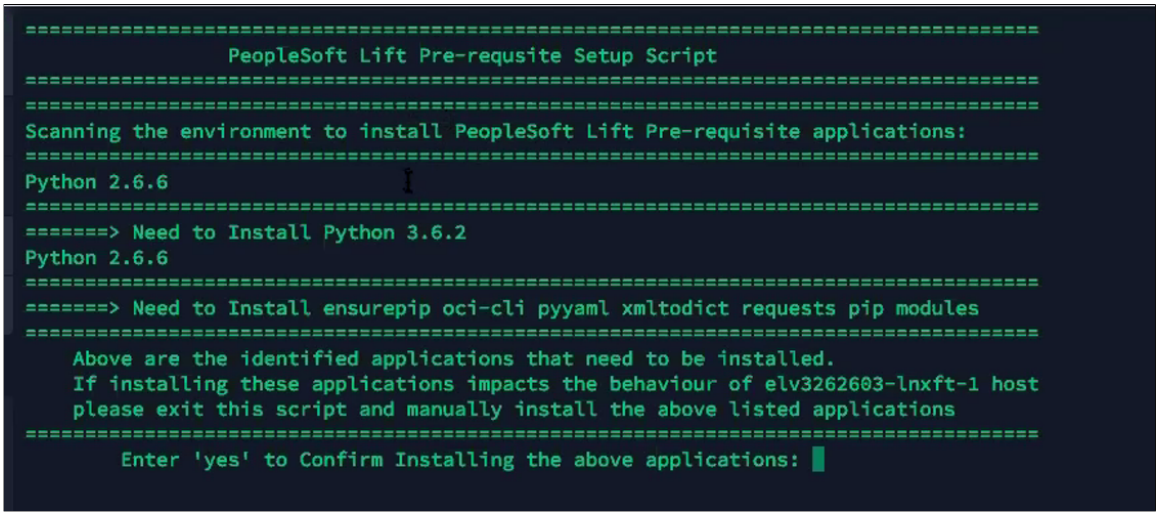
```
Is <environment> a Database Environment: (yes/no):
```

- Application environment (answer no at above prompt)

  The system will scan the environment and indicate the applications that need to be installed.

Image: Example PeopleSoft Lift Prerequisite Setup Script for Application Environment

This example illustrates applications that are required for an application lift.

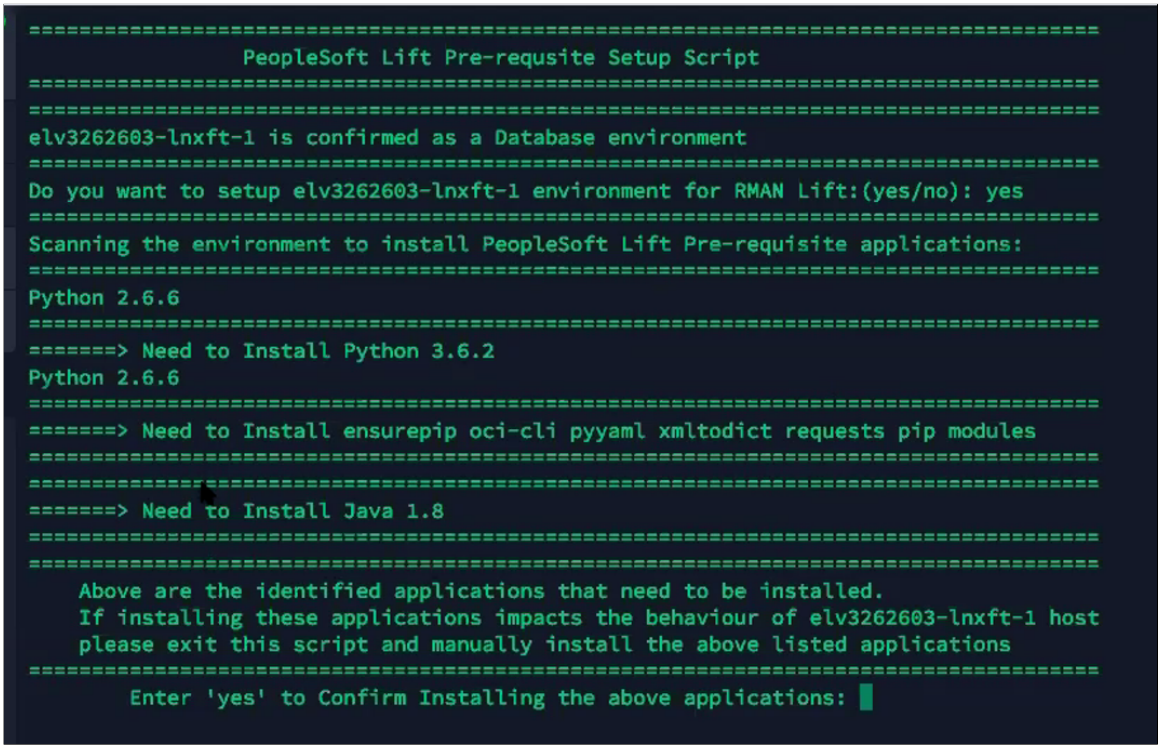


- Database environment (answer yes at above prompt)

  The system will scan the environment and indicate the applications that need to be installed.

  Image: Example PeopleSoft Lift Prerequisite Setup Script for Database Environment

  This example illustrates applications that are required for a database lift.



- To confirm installing the applications, enter yes at the prompt.

  ```
  Enter 'yes' to Confirm Installing the above applications:
  ```

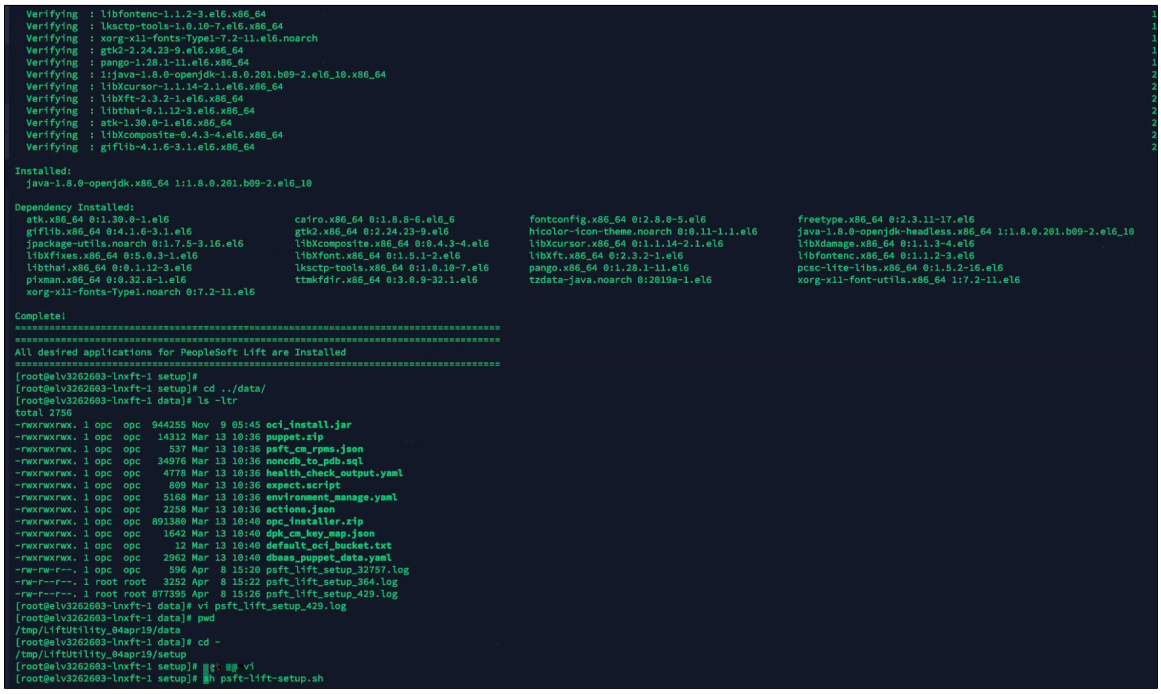

> ***Warning!*** If installing the applications impacts the behavior of your environment, then enter no. You will need to install the applications manually.

During installation of the prerequisite applications the utility will prompt for user confirmation, in order to continue installing certain dependencies. Not installing dependencies may result in Lift failure.

When all the applications are successfully installed, you will get a message “Complete!”.

Image: Example Lift Prerequisites Complete

This example illustrates all desired applications for PeopleSoft Lift are installed.



You can list the files and view the logs that were created for the install. The logs located at <Lift_Utility>/data/psft_lift_setup_<PID>.log

When you are ready to run the Lift Utility, it will verify that all the prerequisites have been installed.

Manually Installing Lift Prerequisites

Note: Please use the manual method in case the automated method fails to install all prerequisites.

In the On Premise PeopleSoft instance, you must perform the following steps to manually install the lift prerequisites:

1. Extract the Lift Utility in a certain path on the respective application and database instance:

   ```
   mkdir -p <LIFT_UTILITY_PATH>
   unzip LIFT_UTILITY.zip -d <LIFT_UTILITY_PATH>
   ```

2. Install Python 3.6:

a. Remove any old Python files present within the lift base directory by executing the command.

```
rm -rf <LIFT_UTILITY_PATH>/lnx_python
mkdir -p <LIFT_UTILITY_PATH>/lnx_python
```

b. Install the prerequisites by executing the following commands:

```
sudo yum install gcc
sudo yum install libffi-devel
sudo yum install openssl-devel
sudo yum install zlib
sudo yum install wget
```

c. Download Python 3.6.2 by executing the following commands:

```
cd <LIFT_UTILITY_PATH>
wget https://www.python.org/ftp/python/3.6.2/Python-3.6.2.tgz
tar xzf Python-3.6.2.tgz
cd Python-3.6.2.tgz
```

d. Configure and compile the source by executing this command:

```
./configure --prefix=<LIFT_UTILITY_PATH>/lnx_python
make altinstall
```

e. Create a soft link for the Python executable by running the following commands:

```
cd <LIFT_UTILITY_PATH>/lnx_python
ln -s bin/python3.6 python
```

f. Set environment variables. Do the following:

```
export PYTHON_HOME=<LIFT_UTILITY_PATH>/lnx_python
export PYTHONPATH=<LIFT_UTILITY_PATH>/lnx_python
export PATH=<LIFT_UTILITY_PATH>/lnx_python/bin:<LIFT_UTILITY_PATH>/lnx_py⇒
thon/:$PATH
export LANG=en_US.utf-8
export LC_ALL=en_US.utf-8
```

g. Install PIP with this command:

```
<LIFT_UTILITY_PATH>/lnx_python/python -m ensurepip
```

3. Install the below PIP packages.

a. Install the oci-cli package with this command:

```
pip install oci-cli
```

b. Install PYYAML with this command:

```
pip install pyyaml
```

c. Install XMLTODICT with this command:

```
pip install xmltodict
```

4. Install Java version 1.8 (JRE) using Java Official Documentation.

Verify Java is Installed by running the below commands.

```
$ java -version
```



```
    java version "1.8.0_144"
    Java(TM) SE Runtime Environment (build 1.8.0_144-b01)
    Java HotSpot(TM) 64-Bit Server VM (build 25.144-b01, mixed mode)
$ echo $JAVA_HOME
    /usr/lib/jvm/java-1.8.0-openjdk/jre
```

5. Generate the Oracle Cloud Infrastructure Auth Token. See Generating Oracle Cloud Infrastructure Auth Token.

Performing Application Lift

Application Lift means lifting the middle tier which consists of the Application Server, Web Server and Process Scheduler of PeopleSoft Application.

1. Use only the PeopleSoft Admin user (for example, psadm2) to perform Application Lift.
2. Make sure to have sufficient free disk space for Application Lift (based on PS_APP_HOME and PS_CUST_HOME size). A minimum disk space of 10GB is required.
3. Ensure PS_APP_HOME and PS_CUST_HOME directories are available.
4. Ensure that the user running the Lift utility has the permission to create files or directories at the user's home directory, Lift utility directories, and the destination directory where the DPKs are saved, /tmp , PS_APP_HOME, and PS_CUST_HOME directories.

Note: Installing OCI-CLI is a prerequisite for the lift utility. See Installing Lift Prerequisites

---

To perform the one-step Lift automation procedure for the application:

1. Download the Lift utility from the Lift and Shift page. For this, perform the following:
   a. Navigate to the Lift and Shift tile.
   b. Copy the “LIFT_UTILITY.zip” utility to the target machine to perform lift.

   Note: If you have recently updated Cloud Manager with any PRPs that has fixes to the lift utility, then SSH to the Cloud Manager instance and delete the stale zip file form /tmp/LIFT_UTILITY.ZIP.

   ---

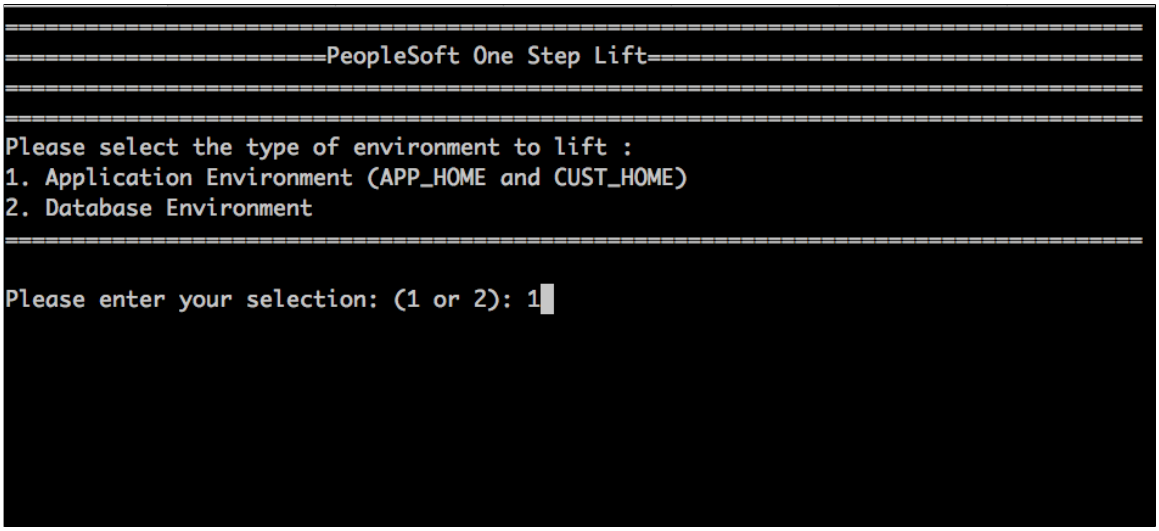
2. Navigate to the below folder after extracting the LIFT_UTILITY.zip and set permissions:

```
chmod -R 777 <LIFT_UTILITY_PATH>
cd <LIFT_UTILITY_PATH>/setup
```

3. For Linux, run the **sh psft-osl.sh** command to perform lift.
4. Select 1 at the prompt to select the type of environment to lift.

Image: Application Environment Lift prompt

This example illustrates the prompt to lift the Application Environment Lift prompt.



5. To create the PeopleSoft App Server DPK, you need to provide the database name (or PDB name in case of Oracle 12c or higher multi-tenant database) and destination directory.

Note: If the utility is unable to fetch the data from the environment (for example, app_type/ oracle_home), it will prompt the user to input the same.

---

6. Choose any one of the below options:

   1. Create and Save DPK in APP/DB Environment.

   2. Create, Save DPK in APP/DB Environment and Upload the DPK to Oracle Cloud Infrastructure (Object Storage).

7. If you select option 1. Create and Save DPK in APP/DB Environment, you will need to manually upload the DPK to Object Storage. See Uploading the DPK Manually to Oracle Cloud Infrastructure.

8. If option 2 to upload the DPK to Oracle Object Storage is selected, then the script prompts the user to input the Oracle Cloud tenancy credentials as mentioned below in order to upload the DPK once created:

   See Locating OCI Credentials

   – Oracle Cloud Infrastructure Region Name

   – Oracle Cloud Infrastructure Tenancy Name

   – Oracle Cloud Infrastructure Tenancy ID

   – Oracle Cloud Infrastructure User ID

   – Private Key Location, indicates the API signing private key that was created during CM configuration and must be copied to the instance where lift utility will be run. This input refers to the full path to the file.

– Passphrase, refers to the passphrase that was used to encrypt the API signing keys.

Note: You need to manually copy the key file or copy the key file contents and save locally in the machine where you perform the lift. This is the corresponding Private Key to the Public Key that was set in the API Keys of the user setting.

9. After Application Lift is complete, following Application DPK will be created based on the PeopleTools version on the application instance.

   – For 8.55: APP-DPK-<platform>-<app_type>-<db_name>-1of2.zip

   – For 8.56/8.57/8.58: APP-DPK-<platform>-<app_type>-<db_name>-1of3.zip.

   Note: The APP-DPK*-3of3.zip will not be created as part of the Lift utility, however the APP-DPK*-3of3.zip DPK will be available from the PeopleTools DPK when the shift is triggered from Cloud Manager.

The Lifted DPKs created are available in the destination directory. If you had chosen to create and upload DPK to Oracle Object Storage, then the uploaded DPKs are available in Oracle Object Storage and listed in the Lift and Shift page of Cloud Manager.

Performing the Database Lift

The Database lift means lifting the database of PeopleSoft instance as a hot backup using RMAN.

Note: Database Lift using hot backup can only be performed on a database instance that has access to the internet.
It is recommended to bring the database patch level of the on-premise environment equivalent to that of the database patch level of the Oracle Database Cloud Service before starting the Lift and Shift process. If the patch levels are different, then Cloud Manager will try to either rollback or update the patch. It is possible that there could be some incompatibilities during lift and shift due to rollbacks or updates. Users will then need to manually verify and rectify it.

Installing OCI-CLI is a prerequisite for the lift utility. See Installing Lift Prerequisites

Considerations Before Running Database Lift

1. Lift can be performed on the DB instance (Local Lift) only.
2. Ensure to use only the Database owner user (for example, oracle) to perform DB Lift.
3. Ensure to have sufficient free disk space for DB Lift based on DB size.
4. Oracle versions 12.1.0.1.0 and higher are supported.
5. Ensure to take the back up of your Database environment and the RMAN configurations before performing DB Lift. Optionally, it is recommended to use a clone of the environment for the Lift operation.

   Note: During the Lift process, the ORACLE Database will not be shut down.

6. Ensure to back up the ORACLE_HOME.
7. Ensure that the user running the lift utility has permission to create files/directories at the user's home directory, Lift utility destination directory where the DPKs are saved, /tmp, and ORACLE_HOME directory.

Note: If you want to encrypt the database before lifting using TDE, see Encrypting Tablespaces Using Transparent Data Encryption.

Using RMAN for Hot Backup Database Lift

RMAN Lift and Shift supports the following Oracle Databases:

- Oracle 12c, 18c and 19c
- Container Databases
- Unicode and Non-Unicode Databases
- TDE enabled Database
- Database on ASM

Note: During Lift and Shift with RMAN the Oracle Database Cloud Backup Module (ODCBM) is used under the hood to perform full RMAN Backup and Restore operations.

During Database Lift with RMAN the Lift Utility will create a fresh Bucket in the OCI Object storage and then the RMAN Backup of the source (On Premise) Database environment will be compressed and encrypted before being wired to the bucket in the OCI Object Storage. Along with the RMAN backup the "APP-DPK-<platform>-<app_type>-<db_name>-2of<X>.zip" is created to capture the sqlpatches, database parameter file and other metadata information.

The "APP-DPK-<platform>-<app_type>-<db_name>-2of<X>.zip" will be small, since we are not packaging the Database files (*.dbf) within this zip.

RMAN Lift and Shift does not support:

- RAC Database
- RMAN (L1) Incremental Backup.

Note: It is recommended that the DB Tier Database is started with a spfile.
Ensure the Database “Archive Log Mode” is enabled (Oracle support Doc ID 371139.1).
Ensure the proxy (if needed) is correctly specified and the proxy authentication does not have any special characters.
To perform an RMAN Lift of a PeopleSoft environment that was already lifted using the older version of Cloud Manager (Lift Utility), it is recommended to delete the existing Lifted DPK from the Cloud Manager “Lift and Shift” UI and then trigger a RMAN lift for the same.

Running Lift Using Hot Backup (RMAN)

To perform the Lift using Hot Backup:

1. Navigate to the Lift and Shift tile.
2. Download and copy the “LIFT_UTILITY.zip” to the target machine to perform lift.

   Note: If you have updated Cloud Manager with PRP (find PRP name/number), then SSH to Cloud Manager VM and delete the stale zip file from /tmp/LIFT_UTILITY.zip.

3. Navigate to the below folder after extracting the LIFT_UTILITY.zip and set permissions:

   ```
   chmod -R 777 <LIFT_UTILITY_PATH>
   cd <LIFT_UTILITY_PATH>/setup
   ```

4. Export Java home.

   ```
   export JAVA_HOME=/tmp/java18/jre
   ```

5. For Linux, run the **sh psft-osl.sh** command to perform lift.
6. At the prompt “Do you want to Lift the Application Environment”, enter “N” to Lift the DB instance.
7. At the prompt input the following:

   – Container Database name (applicable only for Multitenant database)

   – Database name

8. Performing Lift using Hot Backup requires the OCI details:

   See Locating OCI Credentials

   – Oracle Cloud Infrastructure Region Name

   – Oracle Cloud Infrastructure Tenancy Name

   – Oracle Cloud Infrastructure Tenancy ID

   – Oracle Cloud Infrastructure User ID

   – Private Key Location, indicates the API signing private key that was created during CM configuration and must be copied to the instance where lift utility will be run. This input refers to the full path to the file.

   – Passphrase, refers to the passphrase that was used to encrypt the keys.

   Note: You need to manually copy the key file or copy the key file contents and save locally in machine where you perform a lift. This is the corresponding Private Key to the Public Key that was set in the API Keys of the user setting.

   – OCI User name

   – OCI Auth Token

   Note: Ensure not to delete this OCI Auth Token (for the user) from OCI console. Since the User name/Token will be used for Lift and Shift process. The OCI Auth Token is also required for an on-premise to Cloud refresh.

– OCI Infrastructure Compartment ID (OCID)

9. To create the PeopleSoft Database DPK, you need to provide the following:

   – Container Database name (Applicable only for Oracle 12c, 18c and 19c Multitenant database)

   – Database name

   – Number of channels (threads) for RMAN backup (Value between 1–8)

   – TDE KeyStore (Wallet) Password (If TDE is enabled on source Database)

   – RMAN Backup Encryption Password (If TDE is not enabled on source Database)

   – DB environment Proxy Host (* If Any)

   – DB environment Proxy Port (* If Any)

   – Destination Directory

   Note: If the utility is unable to fetch the data from the environment, it will prompt the user to input the same.

10. The script will then display the details captured from the user and prompts for the user's confirmation to proceed. The utility allows the user to modify the above listed inputs, if required.

11. The entire execution is logged into psft_lift_session_<session_name>_<session_count>_<PID>.log file.

12. After DB Lift is complete, the following DB DPK will be created based on the PeopleTools version on the database instance.

    – For PeopleTools 8.55: APP-DPK-<platform>-<app_type>-<db_name>-2of2.zip.

    – For PeopleTools 8.56/8.57/8.58: APP-DPK-<platform>-<app_type>-<db_name>-2of3.zip.

    Note: The APP-DPK*-3of3.zip will not be created as part of the Lift utility, however the APP-DPK*-3of3.zip DPK will be available from the PeopleTools DPK when the shift is triggered from Cloud Manager.

Uploading the DPK Manually to Oracle Cloud Infrastructure

During the process to upload the lifted APP DPKs to OCI Object Storage, if you chose to only create and save the DPK in the APP environment, you will need to manually upload the DPKs.

To manually upload the DPKs to OCI Object Storage:

1. Set the following environment variables:

   a. export PYTHON_HOME=<*LIFT_UTILITY_PATH*>/lnx_python.

   b. export PYTHONPATH==<*LIFT_UTILITY_PATH*>/lnx_python.

c. export PATH=$PATH:=<*LIFT_UTILITY_PATH*>/lnx_python/bin.

2. Create an OCI_Config file with the below contents:

   a. [DEFAULT]

   b. user=<*user OCID*>

   c. fingerprint=<*Finger print*>

   d. key_file=<*private key file location*>

   Note: You can use the same API Signing Key pair that was created when setting up Cloud Manager, or you can create a new one. If you create a new pair then, you must add the newly created public API key under the User Settings using OCI UI.

   e. pass_phrase=<*Passphrase for the private key*>

   f. tenancy=<*tenancy OCID*>

   g. region=<*region name*>

   For example:

   Image: Example of OCI_Config file

   Example of OCI_Config file.

```
[DEFAULT]
user=ocid1.user.oc1..xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
fingerprint=f2:b1:01:87:04:fb:7c:1c:06:44:45:b7:59:16:eb:7f
key_file=/tmp/key.pem
pass_phrase=Kt@125G*jsad986#
tenancy=ocid1.tenancy.oc1..aaaaaaaayy35pigxxxxxxxxas3tlt42nxg4idzrsui52gma5a
region=us-ashburn-1
```

3. If you are uploading for the first time, create the container **psft_oci_las** with the following command:

```
<LIFT_UTILITY_PATH>/lnx_python/bin/oci --config-file /tmp/oci_config os bucket⇒
 create -ns <tenancy name> --name psft_oci_las --compartment-id <Compartment I⇒
D>.
```

   For example,

```
<LIFT_UTILITY_PATH>/lnx_python/bin/oci --config-file /tmp/oci_config os bucket⇒
 create -ns mycloud --name psft_oci_las --compartment-id ocid1.compartment.oc1⇒
..aaaaaaxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```

4. Run the following command to upload the APP DPK. Replace the variables in the command with the actual file and path names:

   Note: The <Bucket Name > should be *psft_oci_las*. Please do not specify any other bucket name.

```
<LIFT_UTILITY_PATH>/lnx_python/python upload_dpk_to_oci.py -d <Tenancy Name> -⇒
c psft_oci_las -s <Source folder containing DPK file> -t <Target Folder Name>-⇒
```

```
f <INI file location generated during lift operation> -g <Full path of oci con⇒
fig file>
```

Variable	*Description*
-d	Tenancy name to which the DPKs will be uploaded to.
-c	psft_oci_las - The container to which the DPKs will be uploaded. This value should not be changed.
-s	Source folder where the DPK files are saved during lift.
-t	Target folder Name on OCI. Should be Platform/AppType/DBName where AppType is application type [HCM,FSCM, ELS, ELM, CRM] and DBName is the name of the database. For example: linux/HCM/MYHCMDB. **Important!** Please ensure the target folder name to be as shown in the example above. There must be no preceding or trailing '/' in the target folder path.
-f	INI file location that was generated during lift operation.
-g	Path to OCI config file that will be used to connect to OCI to upload DPKs.

Locating OCI Credentials

When performing the Lift process, you will be prompted for OCI credentials.

Locating Oracle Cloud Infrastructure Tenancy and Region Name

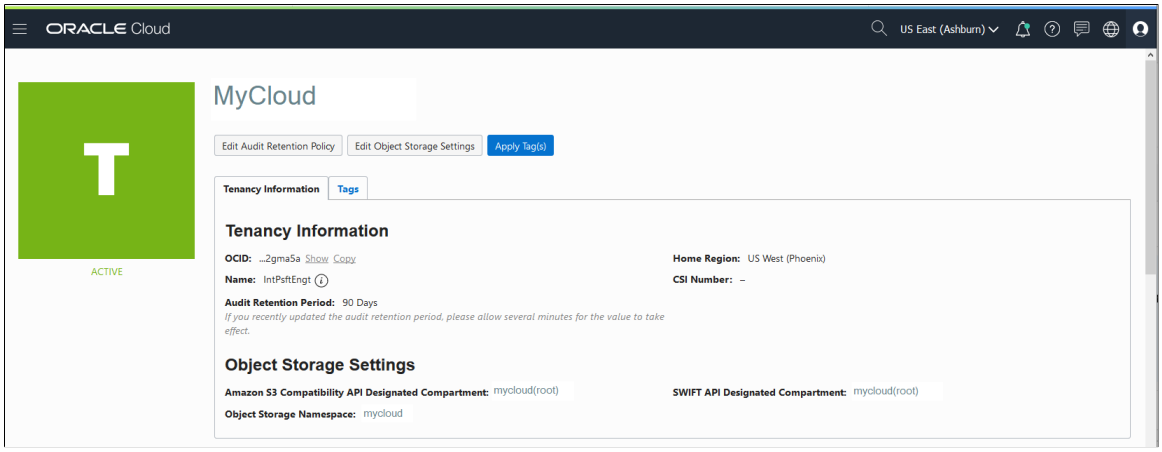
From the OCI home page, use the navigation menu in the upper left to navigate to your cloud resources.

To view the tenancy details, open the Profile Menu and click Tenancy:<your_tenancy_name>.

Profile menu

Image: Tenancy and Region

This example illustrates the fields and controls on the Tenancy and Region.



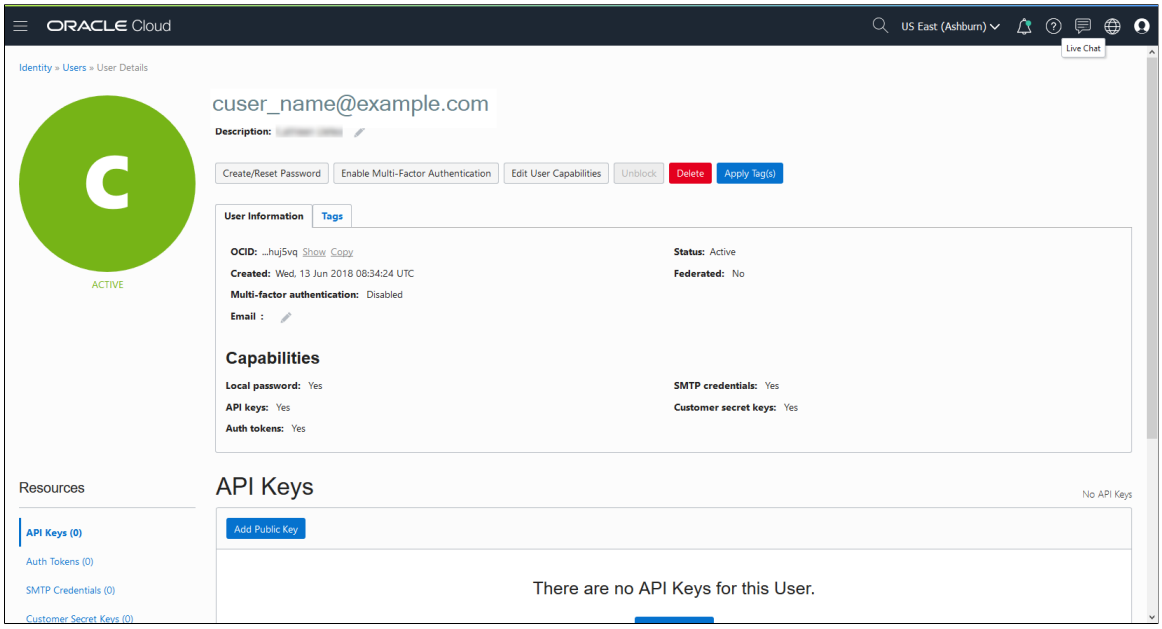
You can use the Copy link to copy the tenancy OCID.

Locating Oracle Cloud Infrastructure User ID

To view the user details open the Profile Menu and click User Settings.

Image: User Information page

This example illustrates the fields and controls on the User Information page.



You can use the Copy link to copy the user OCID.

Locating Oracle Cloud Infrastructure Fingerprint

To locate the OCI fingerprint:

1. Open the Profile Menu and click User Settings.

2. Select API keys from the menu displayed on the left.

Image: API Keys

This example illustrates the API Keys page, which contains the fingerprint.

Generating Oracle Cloud Infrastructure Auth Token

To generate the OCI Auth Token:

1. Click Profile Menu in the top-right corner of the Console, and then click User Settings.
2. Select Auth Tokens from the menu displayed on the left.
3. Click on "Generate Token" and save the Auth Token displayed.

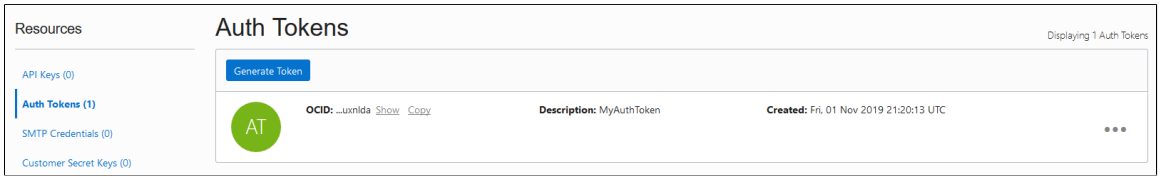
Important! Please ensure to note or save the Auth Token immediately as you will not be able to retrieve the Auth Token once the page is closed.

This Auth Token will be needed for performing Lift and Shift.

Note: Please refrain from deleting the Auth Token after performing the Lift as this new token will be used to perform Shift. If Auth Token is deleted after performing a Lift, you will need to generate a fresh Auth Token and perform a fresh Lift .

Image: Auth Tokens

This example illustrates Auth Tokens page in OCI console.



Deleting Oracle Cloud Infrastructure Bucket and Objects

To delete the OCI Bucket Objects and the Bucket for RMAN Lift:

1. Delete all OCI Bucket Objects (This does not prompt for confirmation (--force))

```
oci os object bulk-delete -ns <Tenancy_Name> -bn <Bucket_Name> --config-file <⇒
oci_config> --force
```


2. Delete all OCI Bucket

```
oci os bucket delete -ns <Tenancy_Name> --name <Bucket_Name>  --config-file <o⇒
ci_config>
```

Example:

```
Tenancy_Name = Intxxxxx

Bucket_Name = PSPDB_1348135976_25092018

oci_config = <oci_config_filepath>

oci_config_filepath:

 [DEFAULT]
 user=ocid1.user.oc1..aaaaaaaas2j6qedkoucwpfgdku7e7cinwue2mz6vqv6nfmk2zjinb4bv⇒
skha
 fingerprint=36:d6:c7:9b:d4:21:d7:ad:10:70:4f:58:b7:70:0f:fb
 key_file=/tmp/key.pem
 pass_phrase=XXXXXXXXXX
 tenancy=ocid1.tenancy.oc1..aaaaaaaayy35pigzces6ly7aslibgt7a4u7o3tlt42nxg4idzr⇒
sui52gma5a
 region=us-ashburn-1
 oci_username=xxxxx.xxxx@oracle.com
 oci_token=YYYYYYYYYYYYY
 oci_tenancy_name=intxxxxx
```

Using the Shift Process to Provision the Migrated Environment on the Oracle Cloud

Use the Shift process to deploy packaged environment in Oracle Cloud.

Prerequisites

- The Lift and Shift topology must be modified with the required size and disk capacity of the database and middle-tier nodes. If shifting to DBaaS, then modify the Lift and Shift - DBaaS topology.

  Note: The disk space of the database node must be configured based on the size of the lifted database. The recommended disk space on the database node is at least 2.5 times the lifted database size.

- During the Shift process, Cloud Manager can update the PeopleTools patch of the lifted environment. To update the PeopleTools patch during shift, make sure to have the required PeopleTools DPK already downloaded and available in the repository.
- The Shift process makes use of the latest PeopleSoft Image for the application type. For example, if your lifted environment is an HCM environment, then make sure you have the latest HCM PeopleSoft Image downloaded in the repository.
- Before shifting, the Lift and Shift related topologies must be edited and saved to add shape name and disk capacity where applicable.

  See Editing an Existing Topology

Note: Verify the Lift and Shift topology; be sure to select the right topology based on the choice of database to be created on Compute or on DBaaS. You also need to verify the sizing and disk space based on the lifted DPK size and desired environment, a minimum allocation should be provided. For database node, you need to provide a size that is equivalent to 2.5 times of the actual lifted DPK size (not zipped).

- For Exadata database:

  You need to add Cloud Manager SSH public key on all nodes. See Administering Oracle Database Exadata Cloud Service

  On the Infrastructure Setting page, click the Refresh OCI Metadata button to sync the Exadata DB Systems provisioned in OCI. After refreshing the metadata, the instance will appear in the DB Systems section on the provisioning page.

- The DB Admin password and the Wallet password are the same and if the customer wishes to change the Wallet password they would need to do that manually.
- The database operator Ids used during the Shift operation should have specific permissions to perform various actions. The permissions are listed below:
  - For ACM (Automated Configuration Manager)— ACM administrator
  - For IB (Integration Broker)— Integration administrator
  - For ES (Elastic Search)— Search Administrator, Search Server, Search Developer
  - For Process Scheduler — PeopleSoft Administrator, ProcessSchedulerAdmin, ReportDistAdmin
  - For Portal — PeopleTools, Portal Administrator
- Supported databases are listed in the Support Matrix for Shift Provisioning on Target Database posted on the PeopleSoft Cloud Manager Homepage.

Pages Used to Provision the Migrated Environment on the Oracle Cloud

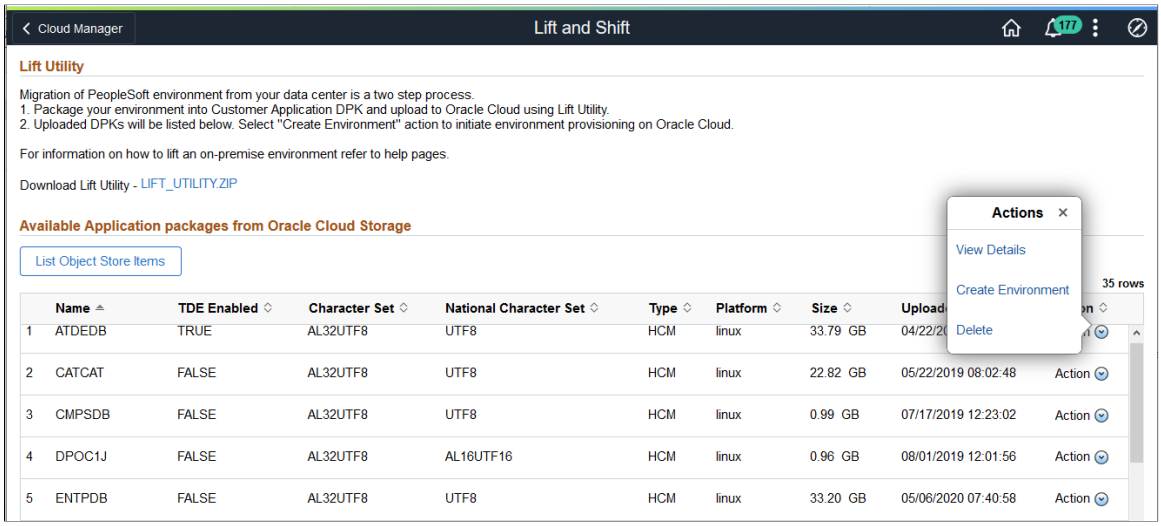
Page Name	*Definition Name*	*Usage*
Lift and Shift – Create Environment Wizard	ECL_LAS_GENERAL_FL	Use the Lift and Shift – Create Environment wizard to perform shift operation by means of a guided process.
Lift and Shift – Advanced Options Page	ECL_LAS_ADV_FL	Use Lift and Shift – Advanced Options page for defining target database details.
Lift and Shift – Custom Attributes Page	ECL_LAS_CUSTATR_FL	Use Lift and Shift – Custom Attributes page for defining the custom attributes as per the lifted environment.
Lift and Shift – Review and Submit Page	ECL_LAS_REVIE_FL	Use Lift and Shift – Review and Submit page to review and submit the entered environment details.

Lift and Shift Page

Once an environment is lifted, it will be available on the Lift and Shift page. Click the List Object Store Items button to view all items.

Image: Lift and Shift page

This example illustrates the fields and controls on the Lift and Shift page. You can find definitions for the fields and controls later on this page.



For description of this page see Lift and Shift Page

Lift and Shift actions:

View Details — Click to verify the lift details. The type of the DB zip file (2of3.zip or 2of2.zip file) will be *db_rman*.

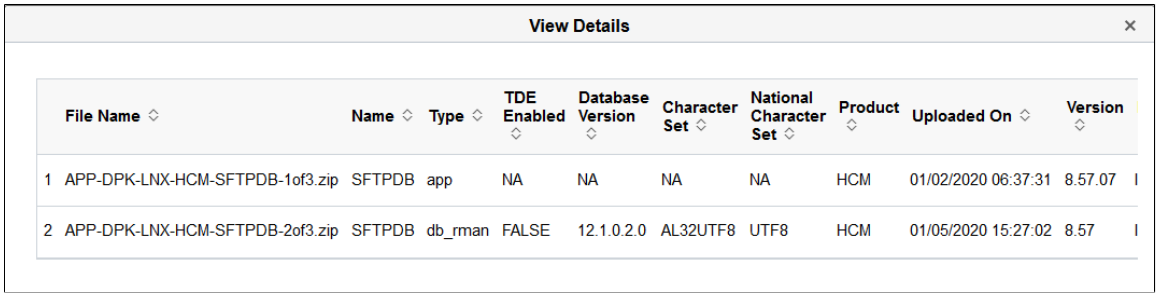
Create Environment — Click to Shift the environment.

See Lift and Shift – Create Environment Wizard.

Delete — Click to delete.

Image: View Details

This example illustrates the fields and controls on the View Details page, showing the type as db_rman for the database zip file.



Lift and Shift – Create Environment Wizard

Use the Lift and Shift – Create Environment wizard (ECL_LAS_GENERAL_FL) to perform the Shift operation. The Shift operation facilitates provisioning a new environment using the lifted DPKs.

In Lift and Shift provisioning, you can:

- Select the desired topology based on DB on Oracle Cloud (Compute or DBaaS).
- Modify the sizing and disk space.

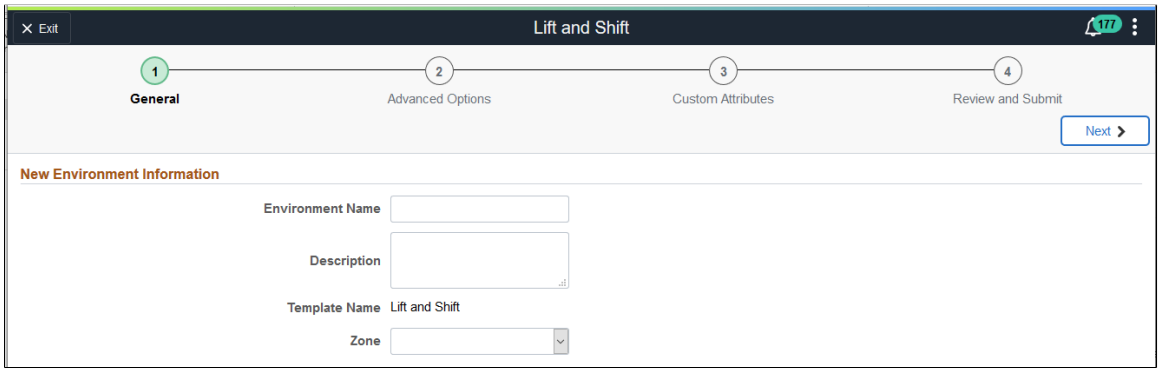
Note: The Database type must be set to DEMO on the Lift and Shift template. This field does not appear in the lift and shift provision pages.

Navigation

Click the Related Action button corresponding to the lifted application. Select Create Environment option. By default, the Lift and Shift - General Details page is displayed.

Image: Lift and Shift - Create Environment Wizard

This example illustrates the fields and controls on the Lift and Shift - General Details page.



Environment Name — Enter the name of the environment which you want to create.

Note: Length of environment name and identity domain name should not exceed 25 characters.

Description — Enter a description for the environment.

Template Name — Displays the default template to be attached with the environment.

Zone — Select the zone on which the environment should be created.

Lift and Shift – Advanced Options Page

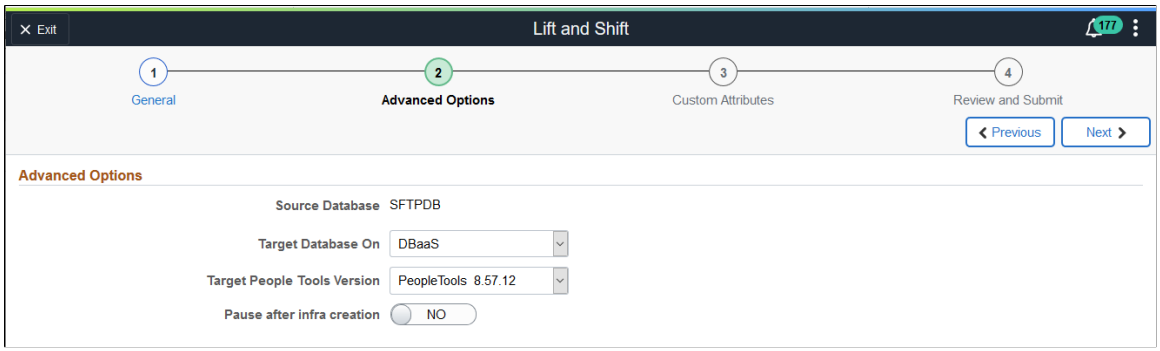
Use the Lift and Shift – Advanced Options page (ECL_LAS_ADV_FL) for defining target database details.

Navigation

Click step 2 or Next at the top of the Lift and Shift guided process.

Image: Lift and Shift – Advanced Options Page

This example illustrates the fields and controls on the Lift and Shift – Advanced Options page. You can find definitions for the fields and controls later on this page.



Target Database On

Select the Target Database On (Compute or DBaaS).

Note: For TDE enabled environments, Target Database On is DBaaS which cannot be changed.

Target PeopleTools Version

Select the PeopleTools version to be applied on the environment.

Pause after infra creation

Select Yes for the environment provisioning to pause after completion of the Infrastructure task. This provides the user the opportunity to do additional setup, actions, or operations on the newly created environment outside of Cloud Manager before proceeding with the PeopleSoft deployment.

Note: When you are ready to proceed to the PeopleSoft deployment, select Deploy from the related actions on the Environment tile.

Select No (default) to continue provisioning the environment when the infrastructure layer is complete.

Lift and Shift – Custom Attributes Page

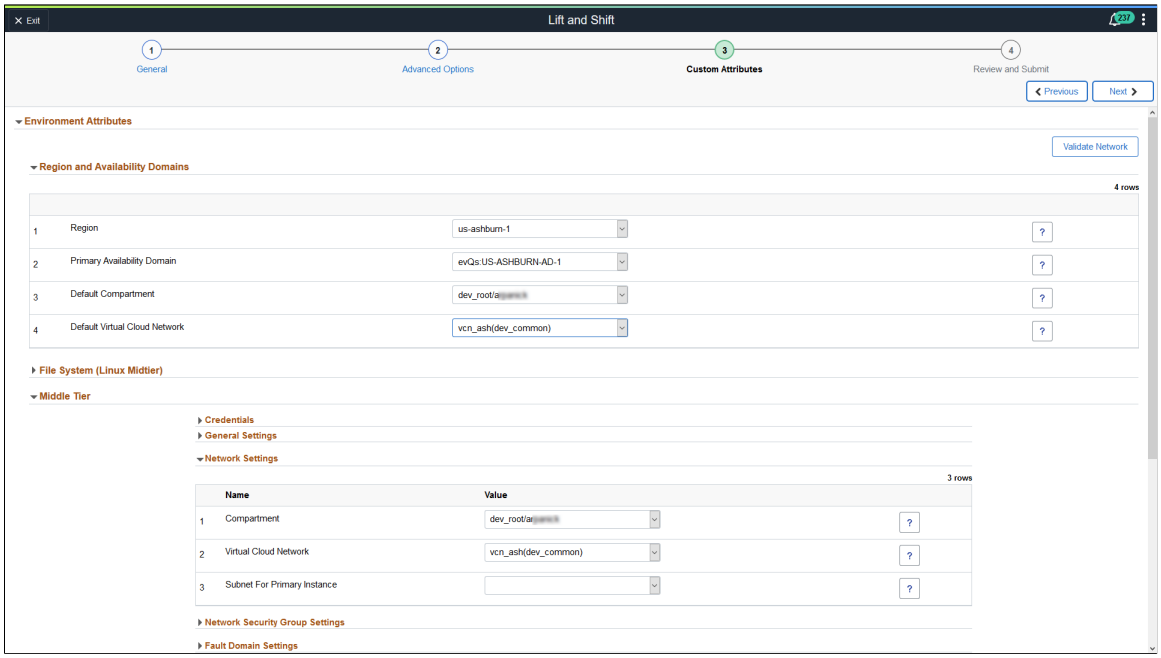
Use Lift and Shift – Custom Attributes page for defining the custom attributes as per the lifted environment.

Navigation

Click step 3 or Next at the top of the Lift and Shift guided process.

Image: Lift and Shift – Region and Availability Domains

This example illustrates the fields and controls on the Lift and Shift – Region and Availability Domains. You can find definitions for the fields and controls later on this page.



The Network Settings defaults to the compartment and VCN in the Region and Availability Domains section, these values can be changed for each tier.

See Configuring Region and Availability Domainsand Configuring Network Settings.

Image: Lift and Shift – Middle Tier Section

This example illustrates the fields and controls on the Lift and Shift – Middle Tier Section.

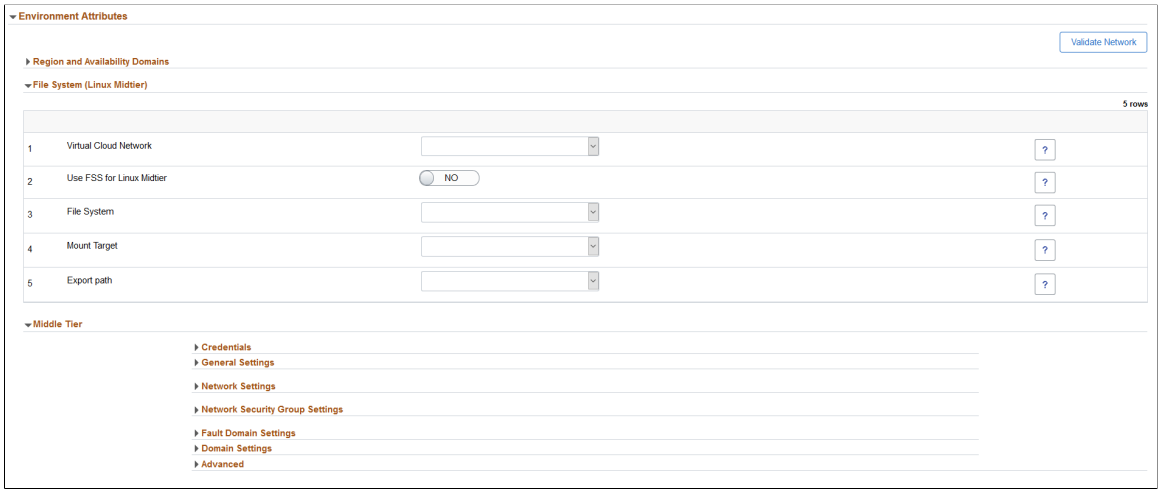


Image: Lift and Shift – DB Systems Section

This example illustrates the fields and controls on the Lift and Shift – DB Systems Section.

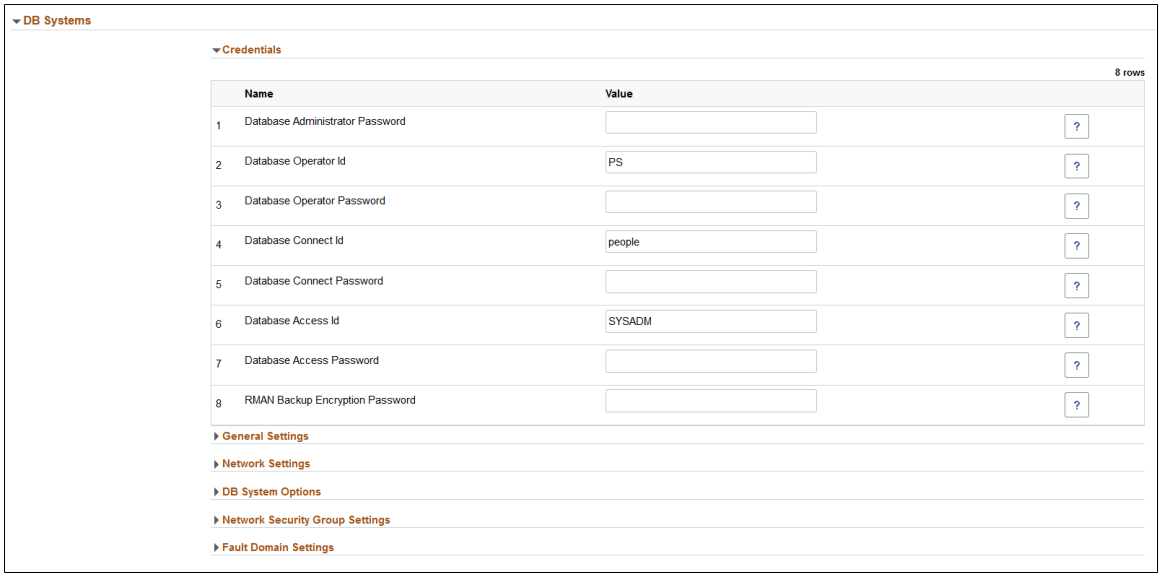
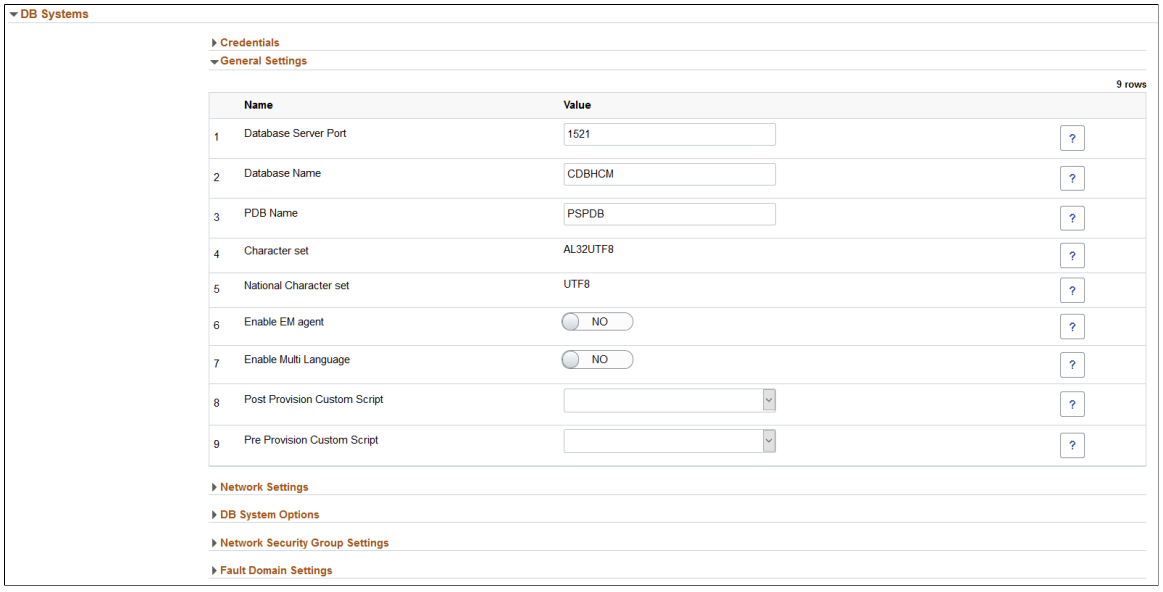


Image: Lift and Shift – DB Systems General Settings

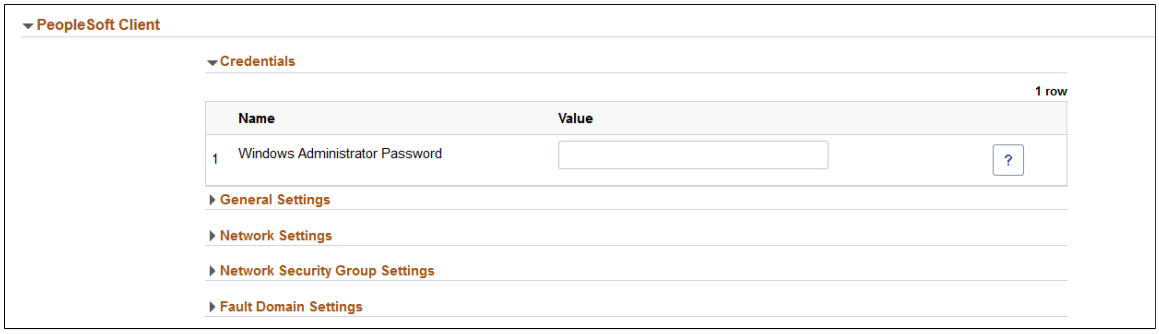
This example illustrates the fields and controls on the Lift and Shift – DB Systems General Settings. You can find definitions for the fields and controls later on this page.



Note: When creating a new shifted environment of a lifted RMAN backup, you must provide a different CDB name than the CDB name of the source database on which the RMAN lift was performed. The shift will fail if the same CDB name is used.

Image: Lift and Shift – PeopleSoft Client Section

This example illustrates the fields and controls on the Lift and Shift – PeopleSoft Client Section.



Enter the custom attributes as per the lifted on-premise environment. It is recommended that the custom attribute values entered on this page match the on-premise configuration.

For details on custom attributes, see Environment Attributes Details for OCI Environments Page.

Character Set Section

The Character Set and National Character Set attributes are configured with values same as the on-premise database configuration.

Note: The database character sets to be used for the Shift operation are AL32UTF8 and National Character Set AL16UTF16. Possible values of National Character Set when character set is AL32UTF8 are AL16UTF16 and UTF8. There can be multiple possible values of character set such as UTF8 WE8ISO8859P15. If shifting to DBaaS, you need to modify the character sets based on the database selected.
If the customer is using the Cloud Manager UI to initiate a DBCS Shift; the “DBaaS Charset” and “DBaaS National Charset” configuration (under Database Tier section) should match with the “Charset” and “National Charset” of the Database environment where the DB Lift operation is performed.
If there is any mismatch in the Charset data, the DBCS shift will fail.
To find the Charset and National Charset information from the lifted environment, run the below SQL commands on the DB (lifted) environment.
select VALUE from nls_database_parameters where parameter='NLS_CHARACTERSET';
select VALUE from nls_database_parameters where parameter='NLS_NCHAR_CHARACTERSET';
Output:
SQL> SELECT value$ FROM sys.props$ WHERE name = 'NLS_CHARACTERSET' ;
VALUE$
AL32UTF8
SQL> SELECT value$ FROM sys.props$ WHERE name = 'NLS_NCHAR_CHARACTERSET';
VALUE$
UTF8

Lift and Shift – Review and Submit Page

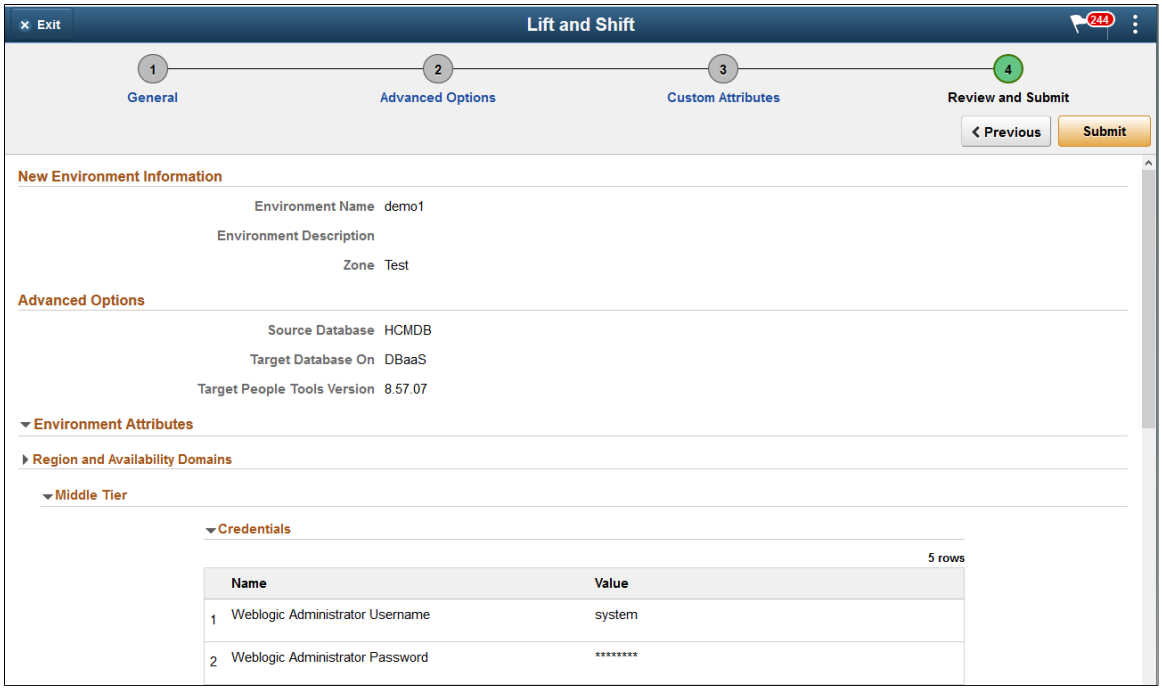
Use the Lift and Shift – Review and Submit page (ECL_LAS_CUSTATR_FL) to review and submit the entered environment details.

Navigation

Click step 4 or Next at the top of the Lift and Shift guided process.

Image: Lift and Shift – Review and Submit page

This example illustrates the fields and controls on the Lift and Shift – Review and Submit page.



Review the details that were entered for the environment.

Click the Submit button to initiate the creation of a lifted environment in Oracle Cloud based on the details provided.

Once the environment is ready, you will be able to view it under the Environments tile. For details, see Environments Tile.

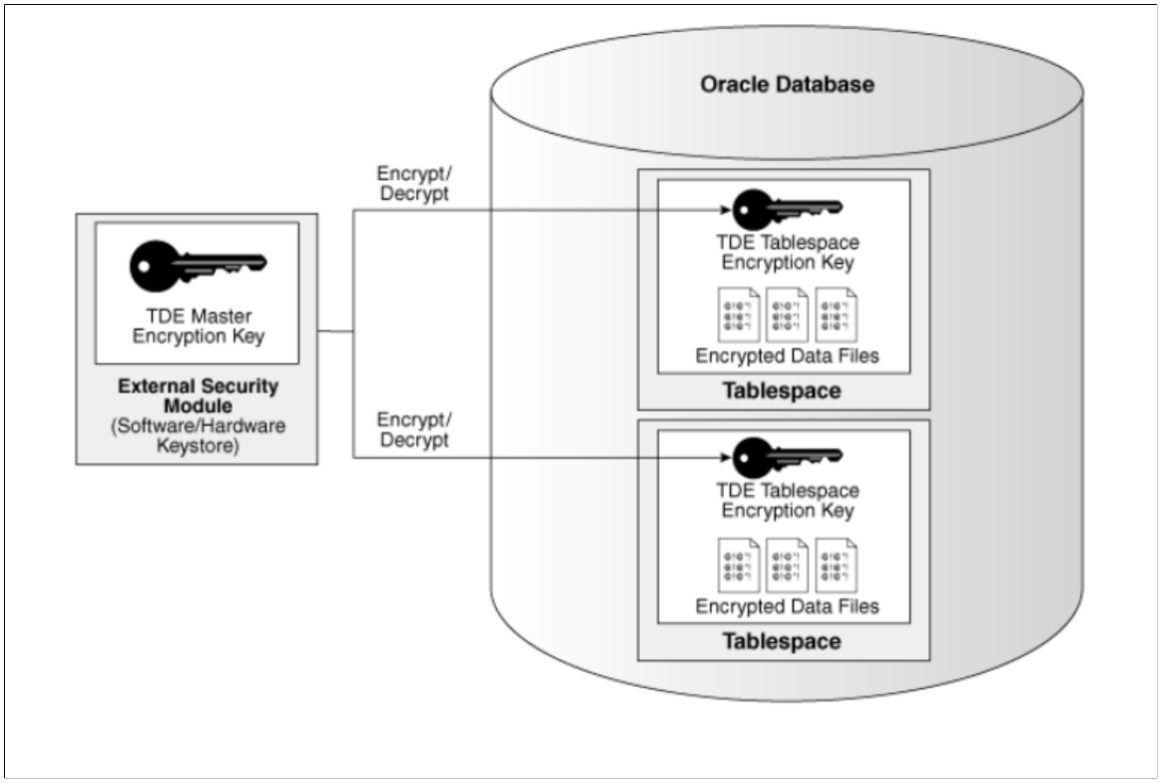
Migrating TDE Enabled Database to Oracle Cloud Using PeopleSoft Cloud Manager

Transparent Data Encryption (TDE) enables customers to encrypt sensitive data, such as Personally Identifiable Information (PII), that are stored in tables and tablespaces.

After the data is encrypted, this data is transparently decrypted for authorized users or applications when they access this data. TDE helps protect data stored on media (also called data at rest) in the event that the storage media or data file is compromised.

Image: Transparent Data Encryption for Cloud Manager

This is a graphical representation of the Transparent Data Encryption for Cloud Manager.



Prerequisites

Below requirements must be satisfied to successfully migrate a TDE enabled database.

- Database being migrated must have TDE enabled and required tablespaces already encrypted.
- Minimum PeopleTools version on the on-premise environment must be 8.55.20. On-premise environments on any version of PeopleTools 8.56 and above are supported.
- Minimum PeopleTools version on the Shifted environment must be 8.55.20.
- Database must be on Oracle 12c , 18c or 19c container.
- Must be a Unicode, non-RAC and non-ASM database.
- Must have a subscription to OCI DBaaS.
- Migration to Compute instance is not supported.
- Remote lift is not supported on TDE.

Lifting TDE Encrypted Database

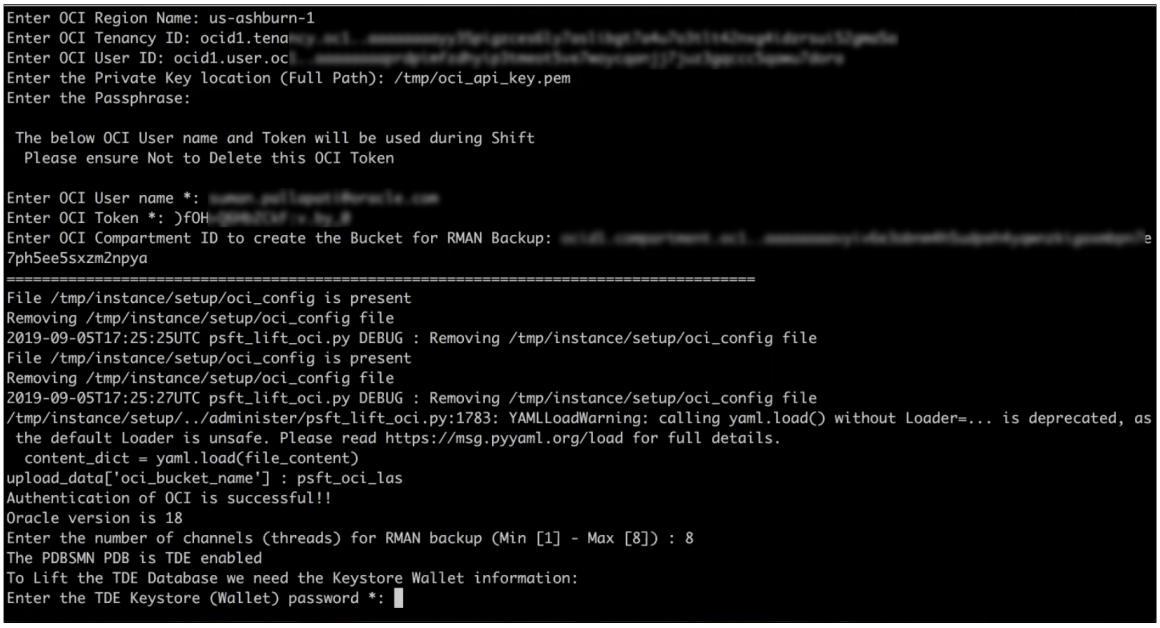
After the lift process is completed, DPKs are created and the TDE Encryption Keys are exported to a file. This exported file must be securely stored and later provided as input when deploying the lifted DPKs.

1. Download the latest lift utility.

2. Copy and extract the utility on the on-premise environment.
3. Run the lift utility to package database and middle-tier environment into DPKs. The Lift utility when triggered on a TDE Enabled Database prompts for TDE Keystore (Wallet) Password.

   Image: Lift Utility for TDE enabled database

   This example illustrates the Lift Utility for TDE enabled database which prompts for the TDE Keystore (Wallet) password..



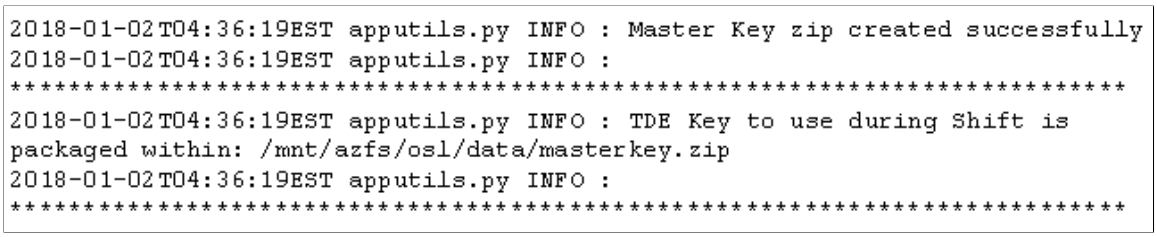
4. Lift utility uploads the DPKs to Oracle Cloud Infrastructure Object Storage.

   See Running Lift Using Hot Backup (RMAN) .

5. The TDE encryption wallet directory will be packaged on the on-premise system in a zip file under /<LIFT_UTILITY_PATH>/data/masterkey.zip. The lift log file will have the path to the zip file as shown in the example below. This zip file must be backed up and available when shifting.

   Image: Lift Log File

   Lift Log File (/<Lift_Utility>/data/psft_lift_session_<PDBNAME>_<SESSIONID>_<PID>.log)



Shifting TDE Encrypted Database

After the lifted DPKs are uploaded to Oracle Cloud Infrastructure Object Storage, navigate to the Lift and Shift page in Cloud Manager and click the button to ‘List Object Store Items’ to refresh the list. Follow below steps to deploy the lifted DPKs.

1. Securely copy the TDE encryption key export file (masterkey.zip, this should be accessible for psadm2 users) to Cloud Manager instance using your favorite SCP tool.

   Note: The length of the path to the zip file must be less than 30 characters.

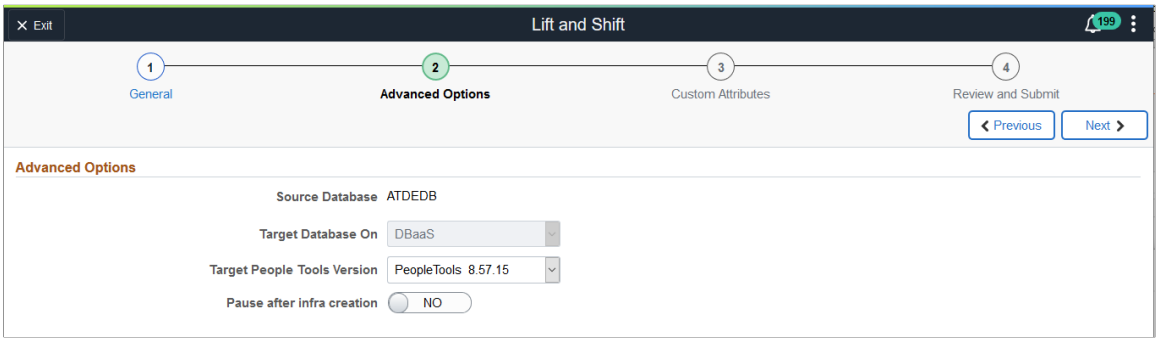
2. Identify the lifted DPK that must be shifted and initiate shift process by selecting 'Create Environment' in the Actions menu.

3. Provide all the New Environment Information and click Next.

4. In Advanced Options, 'Target Database On' Option is set to DBaaS. Compute option is not supported when migrating a TDE encrypted database. Select the PeopleTools patch version and click Next.

   Image: Lift and Shift – Advanced Options page

   This example illustrates the fields and controls on the Lift and Shift – Advanced Options page.



   Note: Minimum PeopleTools version on the Shifted environment is 8.55.20.

5. In Custom Attributes page, TDE related inputs are listed under DB Systems > Credentials. Provide the path to the masterkey.zip file from step 1 as input to TDE Master Key file location and the secret password. Provide all other required inputs and click Next.

   Note: User is only prompted for TDE Wallet password during Lift, however during Shift the user will be prompted for both TDE Wallet and Master Key secret passwords. Master key secret password is user specific with no restrictions.

   Image: TDE Specific Fields in Custom Attributes Page

   This example illustrates the fields and controls on the TDE Specific Fields in Custom Attributes Page.

6. Finally, review all inputs and submit the request to start provisioning the lifted DPKs.

Shifting to RAC on DBaaS

Cloud Manager only supports shift to RAC on DBaaS.

Before shifting the database to RAC, you must modify the Lift and Shift - DBaaS topology with the required shape, and disk capacity of the database and middle-tier nodes.

Note: The VM shape needs to be supported for RAC (2-node DB system). During Shift, Multi node RAC provisioning needs DHCP Options to be set as "DNS Type: Internet and VCN Resolver" for database subnet.

See Editing an Existing Topology

In order to shift to RAC in OCI, follow the procedure for shifting the migrated environment to the Cloud. See Using the Shift Process to Provision the Migrated Environment on the Oracle Cloud .

- On the Lift and Shift – Advanced Options page, select *DBaaS* for Target Database On field.

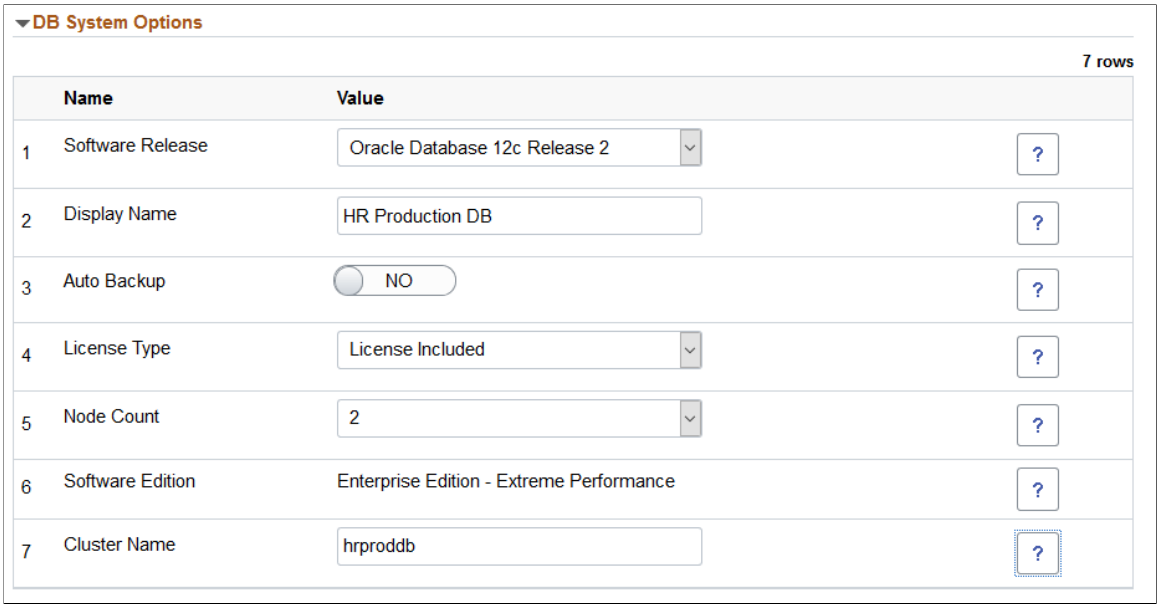
  Note: Refer to the Support Matrix for Shift Provisioning on Target Database posted on the PeopleSoft Cloud Manager Home Page.

- On the DB System Options page, the Node Count must be 2.

  The number of nodes in the database system depends on the shape you select. The shape selected in the topology must support 2 nodes.

  Image: DB System Options

  This example illustrates the fields and controls on the DB System Options.



Encrypting Tablespaces Using Transparent Data Encryption

Note: The procedure explained below to encrypt an existing database must be performed on the source environment before performing the lift.

This topic summarizes the procedure to enable Transparent Data Encryption (TDE) Tablespaces Offline Encryption for an Oracle PeopleSoft Applications database. This process is referred to as using the *Fast Offline Conversion* method to convert existing clear data (residing in non TDE encrypted tablespaces) to TDE encrypted tablespaces. In order to use this feature, the PeopleSoft Applications database requires downtime, as the tablespace(s) to be encrypted need to be temporarily offline. As the encryption is transparent to the application, code does not have to be rewritten, and existing SQL statements work as they are. Transparent also means that any authorized database session can read the encrypted data without any problem: the encryption only applies to data-at-rest, meaning the database data files and any backups of them.

This new functionality, introduced in Oracle release 12.2, is enabled by a patch for 12.1.0.2 that can be downloaded from Oracle Support. See My Oracle Support Knowledge Document 2148746.1 for the specific patch number(s) along with instructions on how to access the patch. Once installed, the patch enables offline, in-place TDE conversion of data files. This process is the recommended Oracle Maximum Availability Architecture best practice for converting to TDE with minimal downtime and the least complexity.

Prerequisites

- This procedure can be used with Oracle PeopleSoft Applications Database – on Enterprise Edition - Version 12.1.0.2 through 19c.
- Refer to My Oracle Support Knowledge Document 2148746.1 for the most recent information on the patch required to enable this process, and the procedure to apply it to an Oracle PeopleSoft Applications database.
- Understand TDE implications and restrictions and develop a process for maintaining wallets and keys. Refer to the *Oracle Database Advanced Security Administrator's Guide* for further details.
- Ensure the compatible database parameter is set to the appropriate database version, 12.1.0.2 or above.
- Always take a full backup of your database before starting the procedure.

TDE Offline Datafile Encryption Restrictions

The following restrictions apply to implementing Tablespace Encryption using Fast Offline Conversion:

- It can only be performed for application tablespace data files. SYSTEM, SYSAUX, UNDO and TEMP tablespaces cannot be encrypted.
- External Large Objects (BFILEs) cannot be encrypted using TDE tablespace encryption because these files reside outside the database. PeopleSoft applications do not utilize BFILEs.

Procedure to Perform TDE Tablespace Offline

To perform TDE Tablespace Offline Encryption for an Oracle PeopleSoft Applications database, follow the steps below:

1. Shut down application server processes.
   Shut down all Applications server processes and make sure all jobs are completed cleanly before continuing further. Users should be prevented from using the Applications database until the encryption process is completed.

2. Source your Oracle PeopleSoft Applications Database Oracle Home.

3. Create a wallet by specifying the wallet location in the sqlnet.ora file under the $TNS_ADMIN directory:

   a. Add the following entry to the sqlnet.ora:

   ```
   ENCRYPTION_WALLET_LOCATION = (SOURCE = (METHOD = FILE) (METHOD_DATA = (DI⇒
   RECTORY = $ORACLE_HOME/admin/TDE/$ORACLE_SID)))
   ```

   b. Create the corresponding directory manually:

   ```
   $ mkdir -p /$ORACLE_HOME/admin/TDE/$ORACLE_SID
   ```

   c. Check wallet location and status:

   ```
   $ sqlplus / as sysdba;
   SQL>select * from V$encryption_wallet;
   ```

4. Create a Keystore in the wallet.

   ```
   SQL>ADMINISTER KEY MANAGEMENT CREATE KEYSTORE '/$ORACLE_HOME/ADMIN/tde/$ORACLE⇒
   _SID' IDENTIFIED BY "<Strong password>";
   ```

5. Open the Keystore create in step 4. As we are in a multitenant environment, we have to specify CONTAINER=ALL in order to set the keystore in all the PDBs:

   ```
   SQL>ADMINISTER KEY MANAGEMENT SET KEYSTORE OPEN IDENTIFIED BY PASSWORD CONTAIN⇒
   ER=ALL;
   ```

6. Set the master encryption key:

   ```
   SQL>ADMINSTER KEY MANAGEMENT SET KEY IDENTIFIED by "<Strong password>" CONTAIN⇒
   ER=ALL;
   ```

   Note: The password must be enclosed in double quotes as shown.

7. Bounce the database:

   ```
   SQL> shutdown normal;
   SQL> exit;
   ```

8. Startup the database normally, ensuring that the wallet is open:

   ```
   sqlplus "/ as sysdba"
   SQL>startup;
   SQL>ADMINISTER KEY MANAGEMENT SET KEYSTORE OPEN IDENTIFIED BY "<Strong passwor⇒
   d>" CONTAINER=ALL;
   ```


9. Switch to the PeopleSoft PDB.

```
SQL> ALTER SESSION SET CONTAINER=<PDBNAME>;
```

10. Identify all the temporary and undo tablespaces in the database:

```
SQL>select tablespace_name from dba_tablespaces where contents='TEMPORARY' and⇒
 STATUS='ONLINE';
SQL>select tablespace_name from dba_tablespaces where contents='UNDO' and STAT⇒
US='ONLINE';
```

11. While still in the PDB, generate three scripts which will be used perform the TDE offline data conversion.

    ALTDATAFILESOFFLINE.SQL

    ALTDATAFILESENCRYPT.SQL

    ALTDATAFILESONLINE.SQL

    a. Script one takes specific data files offline. Create a script file with the following statements and save file as generatealtdatafilesoffline.sql.

```
sqlplus "/ as sysdba"
SET LINESIZE 256
SET HEADING OFF;
SET TERM OFF;
SET FEED OFF;
SPOOL ALTDATAFILESOFFLINE.SQL
select 'alter database datafile '''||b.file_name|| ''' offline;'
from dba_tablespaces a, DBA_DATA_FILES b
where a.tablespace_name not in ('SYSTEM','SYSAUX','TEMP','PSTEMP','PSGTT0⇒
1')and a.tablespace_name=b.tablespace_name
;
Spool off
Exit
If you call the generation script GENERATEALTDATAFILESOFFLINE.SQL using @⇒
 from SQLPLUS, then you will not have to do any additional editing of the⇒
 generated script.
SQL>alter session set container=<PDBNAME>
System altered.
SQL>@generatealtdatafilesoffline.sql
Disconnected from Oracle Database 12c Enterprise Edition Release 12.1.0.2⇒
.0 - 64bit Production
With the Partitioning, OLAP, Advanced Analytics and Real Application Test⇒
ing options
$
```

    b. Script two offline encrypts data files offline. Create a script file with the following statements and save file as generatealtdatafilesencrypt.sql.

```
sqlplus "/ as sysdba"
SET LINESIZE 256
SET HEADING OFF;
SET TERM OFF;
SET FEED OFF;
SPOOL altdatafilesencrypt.sql
select 'alter database datafile '''||b.file_name|| ''' ENCRYPT;'
from dba_tablespaces a, DBA_DATA_FILES b
where a.tablespace_name not in ('SYSTEM','SYSAUX','TEMP','PSTEMP','PSGTT0⇒
1')and a.tablespace_name=b.tablespace_name
;
Spool off
Exit
If you call the generation script GENERATEALTDATAFILESENCRYPT.SQL using @⇒
```



```
 from SQLPLUS, then you will not have to do any additional editing of the⇒
 generated script.
SQL>alter session set container=<PDBNAME>;
System altered.
SQL>@generatealtdatfilesencrypt.sql
Disconnected from Oracle Database 12c Enterprise Edition Release 12.1.0.2⇒
.0 - 64bit Production
With the Partitioning, OLAP, Advanced Analytics and Real Application Test⇒
ing options
$
```

c. Script three brings data files back online. Create a script file with the following statements and save file as generatealtdatafilesonline.sql.

```
sqlplus "/ as sysdba"
SET LINESIZE 256
SET HEADING OFF;
SET TERM OFF;
SET FEED OFF;
SPOOL altdatafilesoonlineexec.sql
select 'alter database datafile ’’’||b.file_name|| ’’’ online;'
from dba_tablespaces a, DBA_DATA_FILES b
where a.tablespace_name not in ('SYSTEM','SYSAUX','TEMP','PSTEMP','PSGTT0⇒
1')and a.tablespace_name=b.tablespace_name
;
Spool off
Exit

If you call the generation script GENERATEALTDATAFILESONLINE.SQL using @ ⇒
from SQLPLUS, then you will not have to do any additional editing of the ⇒
generated script.

SQL>alter session set container=<PDBNAME>;
System altered.
SQL>@generatealtdatafilesonline.sql
Disconnected from Oracle Database 12c Enterprise Edition Release 12.1.0.2⇒
.0 - 64bit Production
With the Partitioning, OLAP, Advanced Analytics and Real Application Test⇒
ing options
$
```

d. Then get back to root or the CDB level.

```
SQL> ALTER SESSION SET CONTAINER=CDB$ROOT;
```

e. Close the PDB. We want the state to be in 'MOUNT' mode.

```
SQL> ALTER PLUGGABLE DATABASE <PDBNAME> CLOSE IMMEDIATE;
```

f. Switch to the PeopleSoft PDB.

```
SQL> ALTER SESSION SET CONTAINER=<PDBNAME>;
```

12. Bring all the specified tablespaces offline by connecting to SQL*Plus as sysdba, and executing the script altdatafilesoffline.sql.

```
$ sqlplus / as sysdba
SQL> @altdatafilesoffline.sql;
```

13. Encrypt your datafiles by running the altdatafilesencrypt.sql offline encryption script from SQL*Plus as sysdba:

```
$ sqlplus / as sysdba
SQL>@altdatafilesencrypt.sql;
```

Note: If you have a large number of data files, you can parallelize their encryption by creating sub-scripts and running the sub-scripts from parallel SQL*Plus sessions.

---

14. Bring all the specified tablespaces online by connecting to SQL*Plus as sysdba, and executing the script altdatafilesonline.sql.

```
$ sqlplus / as sysdba
SQL> @altdatafilesonline.sql;
```

Note: Some tablespaces may take time to show as online. These are probably tablespaces that are encrypted.

Check the status of tablespace encryption by connecting to SQL*Plus / as sysdba and running the query shown:

```
$ sqlplus / as sysdba
SQL>select tablespace_name, encrypted from dba_tablespaces;
```

Note: Unless an auto login keystore is created, every time the database is started up, the wallet will need to be opened as in Step 8 above.

For 12c, to make the wallet auto login, run the following command:

```
$ sqlplus / as sysdba
$ administer key management create AUTO_LOGIN keystore from keystore "<Wallet ⇒
Path>" identified by "<Wallet Password>";
```

Bounce the database.

Chapter 7

Using Zero Downtime Migration to Migrate Environment to Cloud Manager

Understanding Zero Downtime Migration (ZDM)

Zero Downtime Migration (ZDM) gives you a quick and easy way to move on-premises databases and Oracle Cloud Infrastructure Classic instances to Oracle Cloud Infrastructure, Exadata Cloud at Customer, and Exadata Cloud Service without incurring any significant downtime, by leveraging technologies such as Oracle Active Data Guard.

For information on ZDM see Zero Downtime Migration 19.2

Using Zero Downtime Migration to migrate your database involves creating a backup of the source database and restoring it to the target database in OCI.

Once the database is migrated to OCI, you can import the DB System in Cloud Manager and add the middle tier node.

Migrating Environment Using Zero Downtime Migration (ZDM)

To migrate an environment to Cloud Manager using ZDM, perform the following steps:

1. Create a DB System in OCI.
2. Use ZDM to migrate the database to the DB System in OCI.
3. Import the DB System environment in Cloud Manager.
4. Perform an application lift to lift ps app home and ps cust home.
5. Add middle tier node to the running database environment.

Creating a DB System in OCI

Refer to Creating DB System to create the DB System.

The DB System needs to be accessible to Cloud Manager. Keep the following in mind when creating the DB System:

- Passwords used while creating DB System should be same as source database.
- Container Database (CDB) Name should be same as source database.
- Oracle Database software version should be the same as the source database.

- Cloud Manager must be able to access the DB System.

  It is not necessary for Cloud Manager and the DB System to be in the same VCN, however if they are in different VCNs, then VCN peering has to be done before the database import.

  See VCN Peering.

- Cloud Manager SSH public key must be added to the DB System in order for the import to work.

  Add the SSH key with one of these methods:

  - OCI Console, see Creating DB System.
  - SSH to DB System, see Connecting to a DB System and add the Cloud Manager key.

Using ZDM to Migrate the Database to the DB System in OCI

Prerequisites

- ZDM tool is installed and configured.

  See Zero Downtime Migration 19.2.

- DB System created in OCI.

  See Creating a DB System in OCI

- Source and Target Database environments must be accessible by ZDM tool.

Migrating the Database

Follow the steps in the ZDM documentation for Migrating Your Database with Zero Downtime Migration.

Note: Migration method in the ZDM response file should be "MIGRATION_METHOD=BACKUP_RESTORE_OSS".

Importing the DB System Environment

Import the DB System Environment. See Importing Environment for Add DB System Node.

Perform an Application Lift

Perform an application lift to create the Application DPK which includes ps app home and ps cust home.

See Performing Application Lift

Adding Middle Tier Node

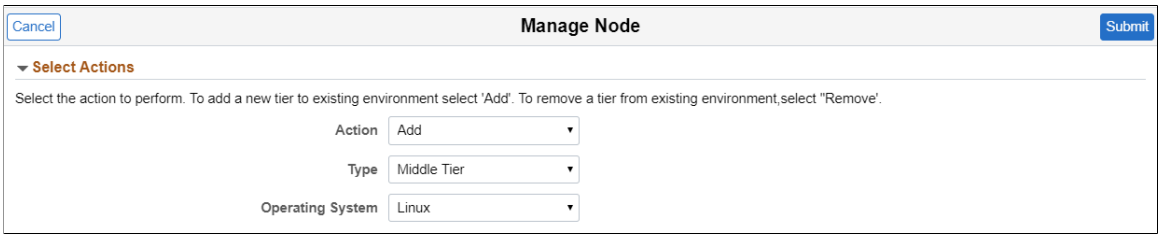
To add the middle tier node to the running database environment:

1. Select the Environments tile.

2. Select Manage Node action for your imported DB System environment.
3. Expand the Select Action section and add a middle tier node.

   Image: Add Middle Tier Node example

   This example illustrates the fields and controls on the Manage Node page to add a Linux middle tier node.

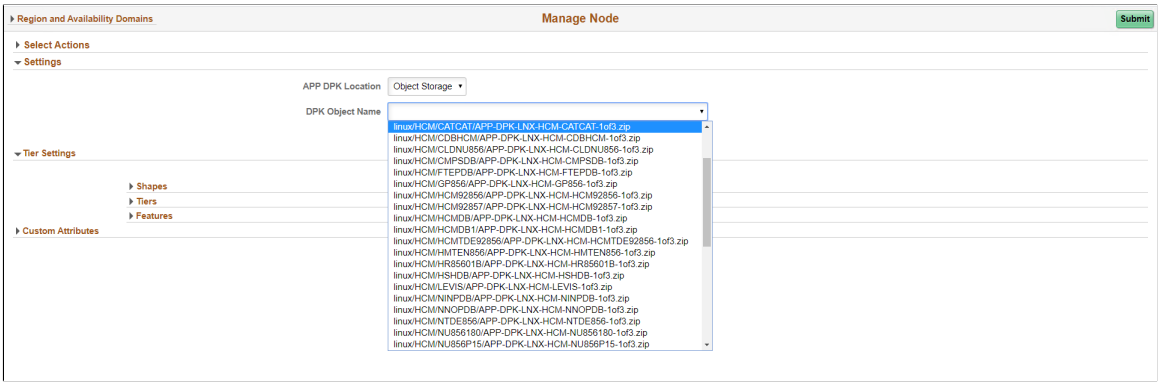


4. Expand the Settings section and select the location for the Application DPK.
   - Object Store

     When you select Object Store, the DPK Object Name drop down list will display all the application DPK files in Object Store.

     Image: Application DPK in Object Store

     This example illustrates the fields and controls on the Manage Node page where the Application DPK location is Object Store.

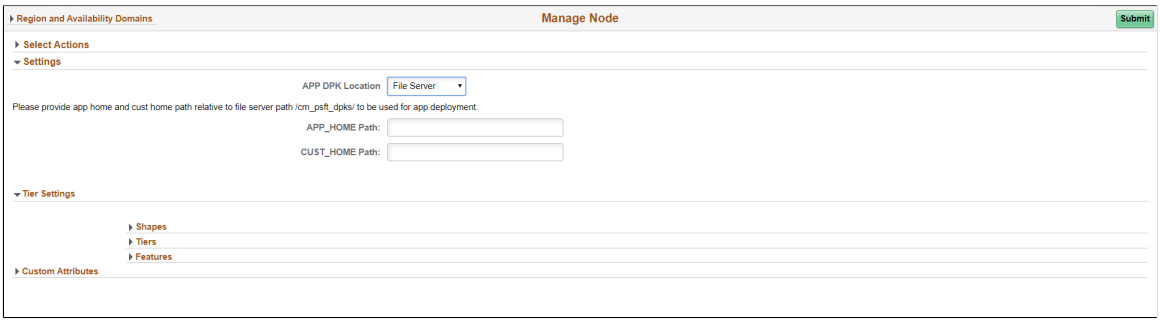


   - File Server

     If you manually copied app home and cust home to the file server provide the relative path to the file server.

Image: Application DPK in File Server

This example illustrates the fields and controls on the Manage Node page where the Application DPK location is File Server.



5. Enter the remaining required credentials and submit.

Chapter 8

Migrating Autonomous Database Environment to Cloud Manager

Migrating ATP-Dedicated Environment

To migrate a PeopleSoft autonomous database environment to Cloud Manager, perform the following steps:

1. Follow the steps in PeopleSoft Application with Oracle Database Migration Guide (Doc ID 2699931.1 to migrate the autonomous on-premise database to ATP-D (Autonomous Transaction Processing Database – Dedicated) on OCI.

   This procedure uses the Oracle Solution "MV2ADB: move data to Autonomous Database in one-click".

2. Import the ATP-D database environment in Cloud Manager.

   See the ATP-Dedicated Instance Type section in Importing Environment.

3. Lift the APP DPK to the object store using the Application Lift (see Performing Application Lift) or copy the APP_DPK to a path relative to the FSS of the Cloud Manager Instance.

4. Use Manage Node on the imported environment to add the middle tier node.

   See Managing Nodes.

5. If the source and target database have different passwords, it is recommended to reset the passwords to 12 character passwords on both source and target databases.

   Note: To support the refresh operation on Cloud Manager, it is advised to reset the passwords to 12 character passwords before migration or after migration to ATP-D.

Chapter 9

Enabling Selective Adoption in Cloud Manager

Enabling Selective Adoption in Cloud Manager

Cloud Manager enables customers to take advantage of Selective Adoption by:

- Quickly creating PUM environments in Oracle Cloud.
- Automating configuration of target databases in PUM source.

Once target databases are configured, standard procedure should be followed to apply updates to target environments. For details on the selective adoption process, refer Selective Adoption.

Before creating a new PUM source environment, a PeopleSoft administrator needs to:

1. Ensure that the latest required PI is downloaded in the repository.
2. Create a new environment template using the latest downloaded PI and PUM topology.
3. Enable user access to the newly created PUM source environment template.

Creating PUM Environments

To create a new PUM source environment using Cloud Manager:

1. Click the Create Environment button on the Environments landing page.
2. Enter the required environment attributes inputs.
3. Select the PUM source environment template to deploy.
4. Click Done.

   See Create Environment Page

Adding Targets to PUM Sources

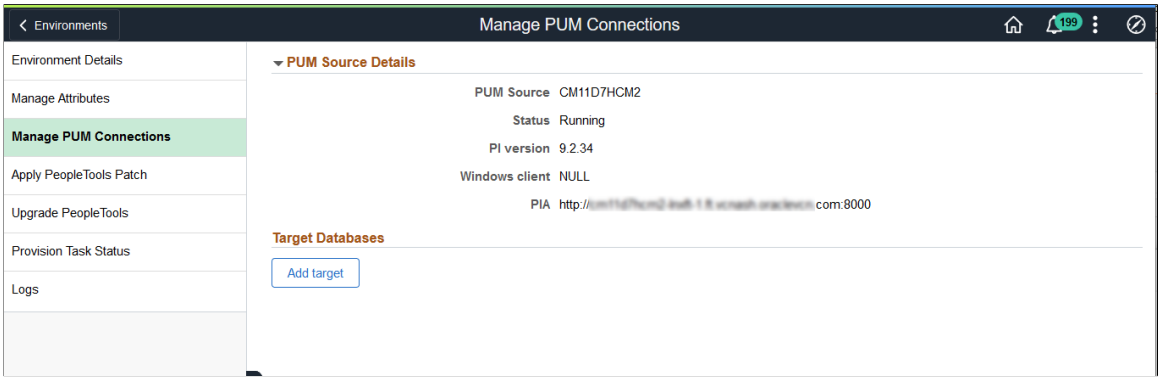
After the PUM source environment is deployed and is in a running state, you can add the target database to the PUM source by performing the following:

1. Click the Environments tile available on the Cloud Manager home page.
2. Click the Related Actions button corresponding to the PUM source environment.
3. Navigate to the Environment Details page.

4. Select the Manage PUM Connections link available on the left panel of the Environment Details page. The Manage PUM Connections page is displayed as shown.

   Image: Manage PUM Connections page

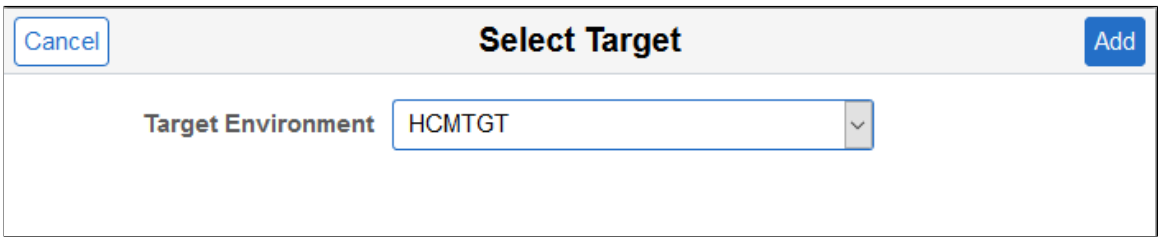
   This example illustrates the fields and controls on the Manage PUM Connections page.



5. Click the Add target button to add any environment of the same application type as the PUM source. This displays a modal window for selecting a target database as shown.

   Image: Select Target modal window

   This example illustrates the fields and controls on the Select Target modal window.



6. Select a target environment.

7. Click the Add button to add the target database.

   Adding the target database takes a few minutes to complete. The target database is configured in Change Assistant and the target database information is uploaded to the PUM source database. The status is displayed as *In Progress* when the job to add the target is running. The status is changed to *Completed* if the target is added successfully, and to *Failed* if the job did not run successfully.

Accessing Change Assistant in Windows Client

Change package can be defined, created, and applied to target environments using the Change Assistant and the PUM source PIA.

To access Change Assistant, perform the following:

1. Determine the IP address or hostname of the PeopleSoft Client that was deployed as part of the PUM source environment from the Environment Details page.

The IP address and Oracle Cloud name is displayed in PeopleSoft Client section of the Environment Details page.

2. Connect to the Windows Client using remote desktop connection.
3. To apply PRPs to PUM Source environment, you need to copy the downloaded PRPs from the file repository to the Windows Client VM. All downloaded PRPs are accessible to Windows Client VM as a samba share. To access the PRP share on the Windows VM, perform the following:
   - RDP to Windows Client VM.
   - Connect to the samba share using \\<File_Server_IP>\PRP.
   - Copy the required PRPs to D:\psft\pum_download directory on the Windows Client.
   - Use Change Assistant to apply the copied PRPs to the PUM Source environment.
4. Follow the standard selective adoption procedures by:
   - Applying PRPs to the PUM Source environment.
   - Defining the change package by connecting to the PUM source database.
   - Creating and applying the change package.

Chapter 10

Updating Cloud Manager

Updating Cloud Manager Overview

Similar to any PeopleSoft application, Cloud Manager updates are released as PeopleSoft Update Images and PRPs. Cloud Manager updates are available as part of Interaction Hub Update Images and corresponding PRPs. These updates can be applied either using an automated method or manually using selective adoption.

- Automatically Applying Updates using Manage Updates

  See Automatically Applying Updates Using Manage Updates

- Manually Applying Updates using Selective Adoption

  See Manually Applying Updates Using Selective Adoption

Note: Please backup both the boot volume and block volume of the Cloud Manager instance before applying the updates. See Using Automated Backup and Restore Utility. If Cloud Manager instance is on a previous version (image 8 or older), then use the manual method to backup, see Manually Backing Up and Restoring Cloud Manager Using Block Volume Backups for OCI.

Automatically Applying Updates Using Manage Updates

The Automated Cloud Manager Update feature facilitates automatic self-update to the latest Cloud Manager Update Image and automatic PeopleTools update or upgrade when required for the latest Cloud Manager Update image. This feature is also used to apply PRPs to the Cloud Manager image.

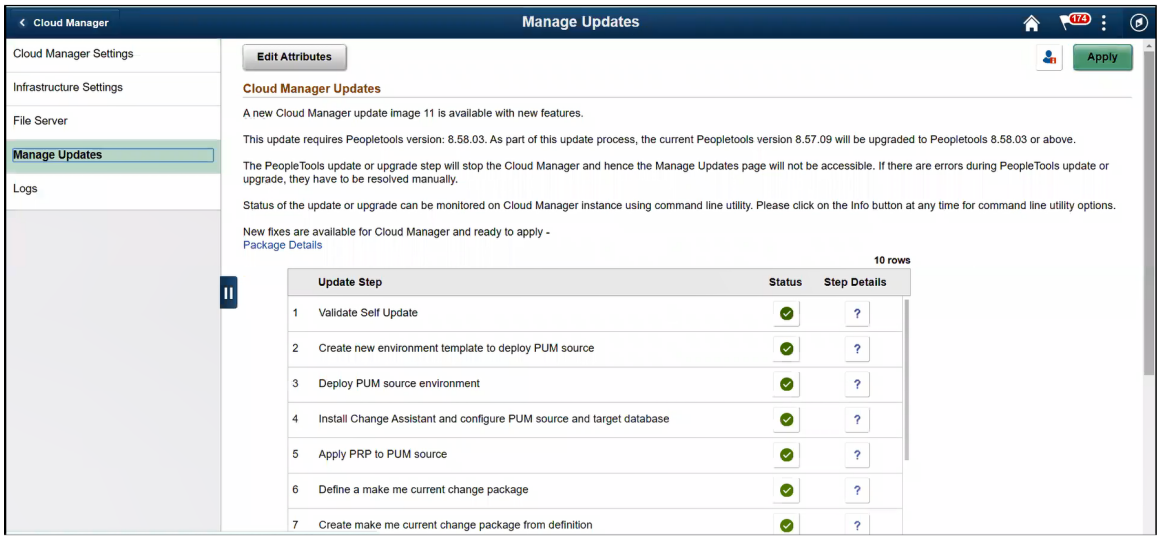
The update process will:

1. Provision a new PUM Source instance and a Windows Client
2. Apply PRPs (if any) on the PUM Source
3. Upgrade PeopleTools
4. Install and Configure Change Assistant on Windows Client
5. Define a Change Package
6. Create Change Package
7. Apply Change Package
8. Reboot domains (as needed)

Whenever there is a new Interaction Hub (IH) PI or new PRPs are available, Cloud Manager will show a notification on the Cloud Manager Update page. You need to click on the Apply button, which will ask for a set of credentials and spin up a IH PUM Source instance. Once the PUM source is up and running, the new updates will be applied to the Cloud Manager instance.

Image: Manage Updates page showing that updates are available

This example illustrates the fields and controls on the Manage Updates page showing that updates are available. You can find definitions for the fields and controls later on this page.



You need to perform the following steps prior to triggering the update:

- Subscribe to Interaction Hub (IH) download channel. The latest updates for IH must be downloaded before starting the upgrade process.

  See Download Subscriptions Page.

  Important! The latest updates for the IH channel will be downloaded based on the download interval (see Changing Download Interval) to download the updates immediately unsubscribe and re-subscribe to the IH download channel.

- Subscribe to PeopleTools version of the IH PUM source.

  Note: The Update Image manifest for the IH PUM source image will list the PeopleTools version.

- Ensure a Windows Image is available in your account.
- Configure Windows Image OCID in Cloud Manager Settings page.
- Inform users that Cloud Manager will not be available during the upgrade.
- Ensure to take a backup of Cloud Manager before updating.

Note: If the Cloud Manager update is initiated with jobs currently running, those jobs may fail. The administrator must clean up and resubmit any jobs that failed.

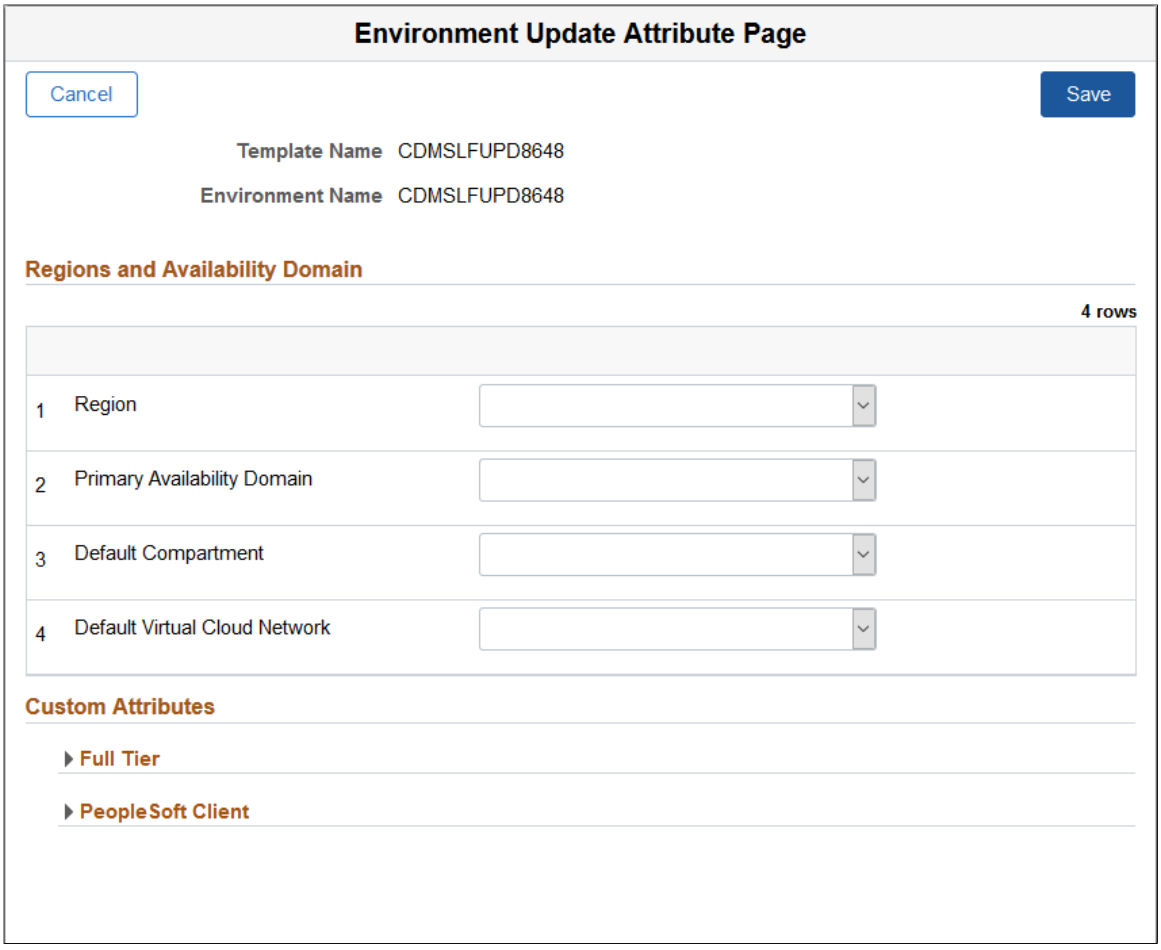
To trigger automated Cloud Manager application update, perform the following:

1. Log in to Cloud Manager as a user having PACL_CAD user role.
2. Click on Cloud Manager Settings tile, then select Manage Updates.
3. Click the Edit Attributes button to input credentials that will be used to deploy a PUM Source environment.

Note: The Database Operator Id field value should always be set as VP1.

Image: Environment Update Attribute page

This example illustrates the fields and controls on the Environment Update Attribute page.

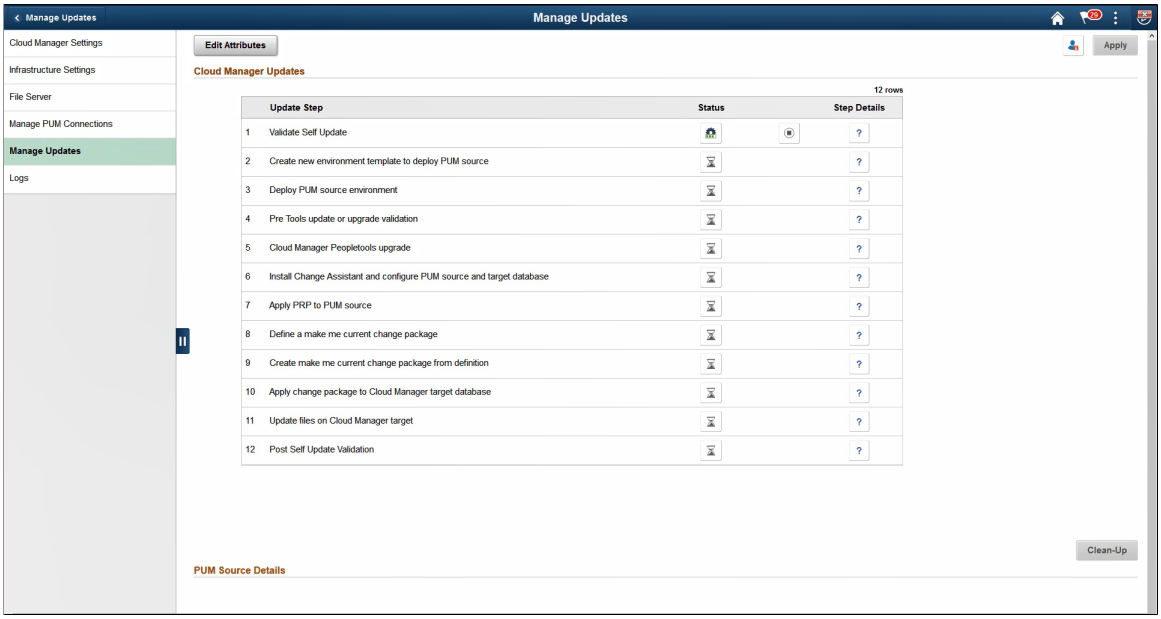


Note: Note: Starting with Cloud Manager Image 12, the Virtual Cloud Network for Full Tier and PeopleSoft Client will default to the Default Virtual Cloud Network specified in the Region and Availability Domain section. If VCN peering is set up, the VCN can be changed for the Full Tier or PeopleSoft Client. See the tutorial *Use Multiple VCNs, Multiple Compartments, or Network Security Groups with PeopleSoft Cloud Manager (Optional)*.

4. Click Save.
5. Click Apply to initiate Cloud Manger Update. The update steps and status are displayed.

Image: Manage Updates page showing Cloud Manager Update Steps

This example illustrates the Manage Updates page showing Cloud Manager Update Steps.



This table lists the update steps:

Step	***Description***
Validate Self Update	This step validates that all of the dependencies for the automation are available and the system is ready to begin the update process.
Create new environment template to deploy PUM source	In this step, a new environment template *CDMSLFUPD<randomly selected number>*is created that will be used to deploy PUM source environment using the latest PeopleSoft Image. The template name can be obtained from the Edit Attributes page. If the status is *Success* - A new template was successfully created. If the status is *Failure* - Template creation failed. In this case, the Retry is enabled. You can delete the template if it was created incorrectly and retry the step.

Step	***Description***
Deploy PUM source environment	In this step, a new PUM source environment named *CDMSLFUPD1<randomly selected number>* is created using the template that was created in the previous step. If the status is *Success* - A new PUM source is created and the details are provided in the PUM Source Details section. If the status is *Failure* - Creating a new PUM source environment failed. In this case, the Retry is enabled. Remedial Action - Clean up the failed environment and any instances from both Cloud Manager UI and Oracle Cloud Infrastructure Console that were created and retry the step. The Continue option is disabled until the clean up is complete.
Manual Step	This step is not always present. If present, this step pauses the self update and provides instructions in the task list. After completing the instructions, select to mark the task as Manually Completed.
Pre Tools update or upgrade validation	This step performs validations on the existing PeopleTools.
Install Change Assistant and configure PUM source and target database	This step executes the processes such as install Change Assistant on the PeopleSoft Client VM instance, configure Change Assistant to add source and target database, and upload target database information to PUM source. If the status is *Success* - Change Assistant is installed and configured with source and target database information. If the status is *Failure* - Failed to install or configure Change Assistant. In this case, the Retry is enabled. Remedial Action - Retry step. Alternatively choose to skip this step after configuring the source and target database manually using Change Assistant and retry.
Apply PRPs on PUM source	In this step, any PRPs that were downloaded are applied and available in Repository on the PUM source. If the status is *Success* - All PRPs were successfully applied on the PUM source environment. If the status is *Failure* - Failed to apply one or more PRPs. In this case, the Retry is enabled. Remedial Action - Retry step. Alternatively choose to skip this step after manually applying all PRPs using Change Assistant. The required PRPs will be available on the PeopleSoft Client VM, if not copy from File Server PRP share.

Step	***Description***
Define make me current change package	In this step, a new change package is defined. If the status is *Success* - Successfully defined a change package which includes all bugs for CM product code. If the status is *Failure* - Failed to define a change package. In this case, the Retry is enabled. Remedial Action - Login to Update Manager PIA of PUM source and delete the change package definition in error and retry step. The name of the definition is in the format CMCHGPKG[n], where n is the sequence number. Alternatively, create the make me current change package definition in Change Assistant. Name the change package CMCHGPKG[n], where n is the sequence number. Mark the failed step as COMPLETED MANUALLY.
Create make me current change package from definition	In this step, a change package using the definition that was created in previous step. If the status is *Success* - Successfully created a change package. If the status is *Failure* - Failed to create a change package. In this case, the Retry is enabled. Remedial Action - Retry step. Alternatively, skip the step after creating the change package manually using Change Assistant with the same name as the definition created in previous step.
Apply change package to Cloud Manager target database	In this step, the change package that was created in the previous step is applied. If the status is *Success* - Successfully applied the change package. If the status is *Failure* - Failed to apply the change package. Remedial Action - Complete the apply step manually using the Change Assistant and continue with next step. ***Warning!*** : Reapplying a change package is not recommended as it may apply the fix again.
Update files on Cloud Manager target	In this step, the new and updated files are copied to Cloud Manager target. If the status is *Success* - Successfully copied all file updates. *Failure* - Failed to copy one or more files. In this case, the Retry is enabled. Remedial Action - Retry step.
Post Self Update Validation	This step validates that the update is complete and the newly created domains are running.

When the update is complete, perform the following steps:

1. Run as root the script post_upgrade_script.sh in $PS_APP_HOME/cloud/ .

   ```
   $> ./ post_upgrade_script.sh
   ```

2. Using PSADMIN, restart application server domain, process scheduler domain and web domain on the Cloud Manager instance to ensure the latest updates are running.

3. Navigate to Cloud Manager Settings > Infrastructure Setting and click the Refresh OCI Metadata button. This will update the Fault Domain Settings.

4. The PUM Source environment can then be cleaned up using the Clean-up button.

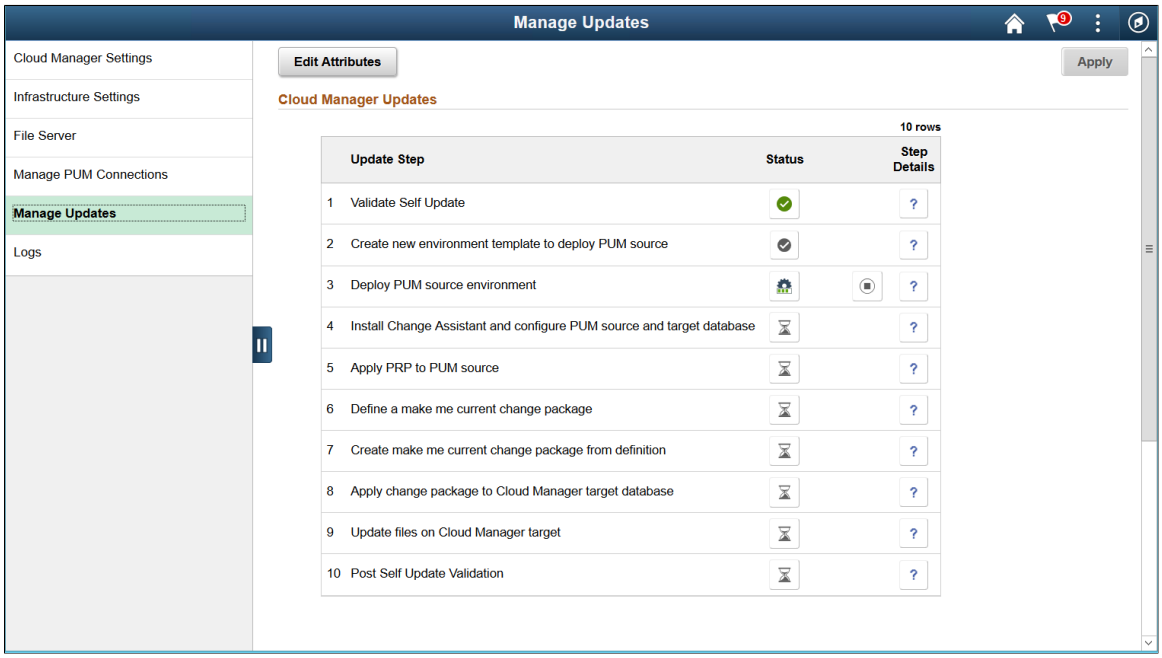
Important! The post update script must be run prior to selecting Clean-up.

Monitoring Update Steps

The status of the update is displayed on the Manage Updates page.

Image: Manage Updates Status

This example illustrates the fields and controls on the Manage Updates page when the steps are running.



Status Icons

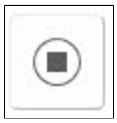
Pending

Success

In Progress

Failed

Continue



Abort

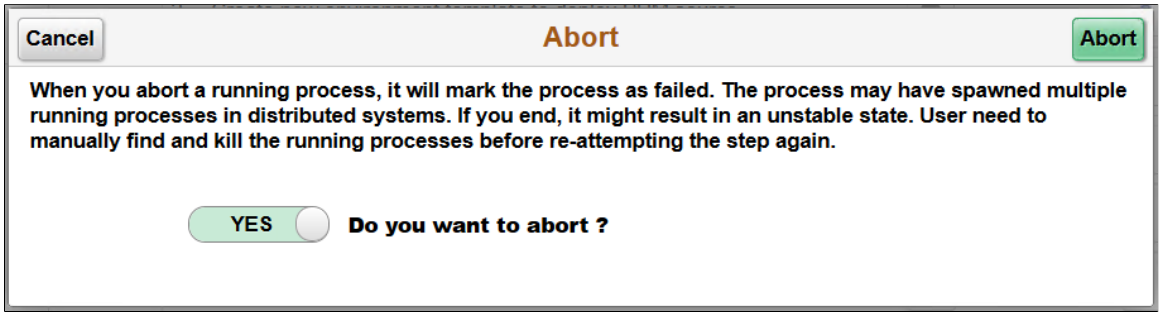
Step details

Pause

The Abort icon is shown when a step is running. When you click the Abort icon, the modal window is displayed.

Image: Abort Modal window

This example illustrates the Abort Modal window.



Caution should be used when aborting a step, it is possible that not all processes that were spawned will be aborted. It is recommended to reboot the Cloud Manager instance after aborting a process.

Failed Steps

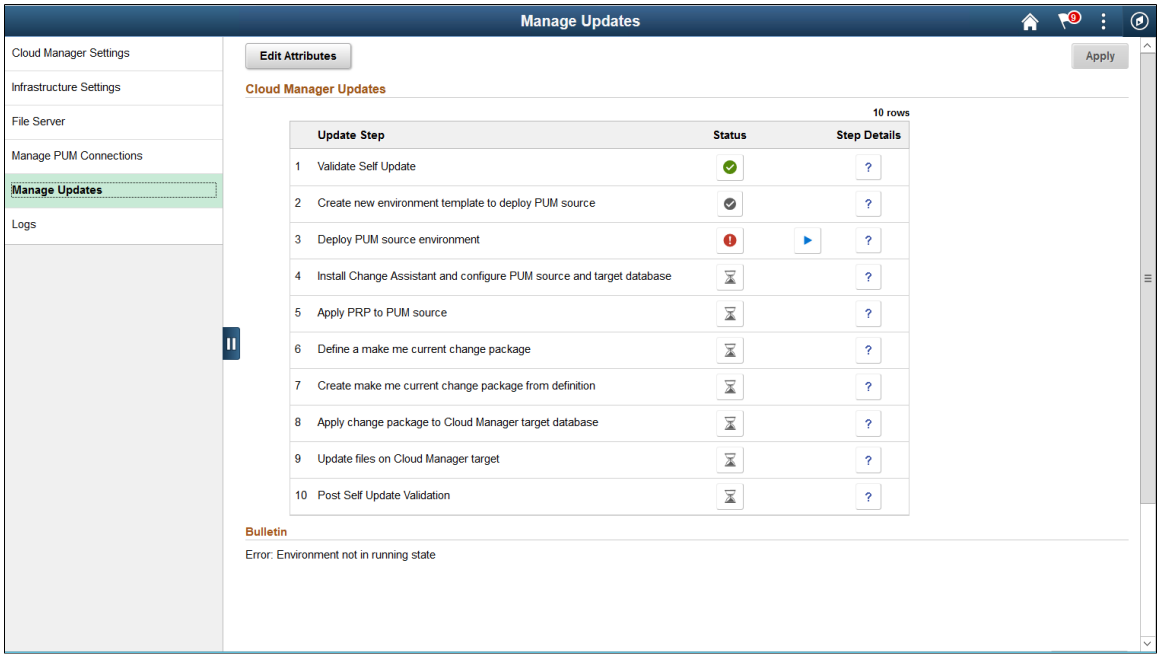
If a step fails, the process will stop and the Continue icon will appear.

An administrator must resolve the issue and come back to Cloud Manager to continue the update process. For example, if applying change package failed, then the administrator must connect to the Windows Client VM, launch Change Assistant and run the update job to completion. The administrator will then return to the Cloud Manager Update page and continue the automated update process.

All reported errors must be resolved manually by the user. After fixing or manually completing the failed step, click the Continue icon.

Image: Example: Failed Step

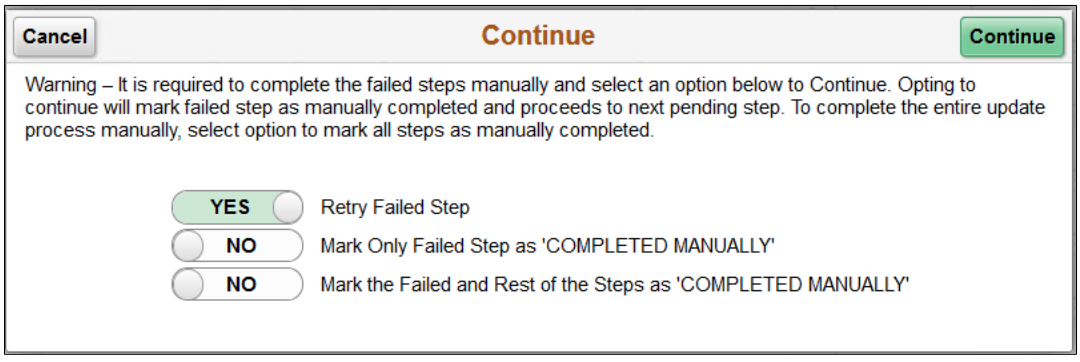
This example illustrates a failed step in the Cloud Manger Update process.



On clicking the Continue button, three options are shown as below:

Image: Options for failed step

This example illustrates the options for the failed step. You can find definitions for the fields and controls later on this page.



1. Retry Failed Step - retry the step again.
2. Mark only failed step as 'Completed Manually' - skip the failed step and continue from subsequent step to completion.

3. Mark the failed and rest of the pending steps as 'Completed Manually' - skip all steps and set update as complete.

   Note: If you mark all steps as manually complete after any failures at the step to *Install Change Assistant and configure PUM source and target database* or lower, then follow the selective adoption procedure to manually update from latest IH PeopleSoft Image.
   See Manually Applying Updates Using Selective Adoption.

After selecting 'Yes' in the Retry Failed Step field, a Continue button is displayed in the top right corner of the Continue modal window.

Monitoring PeopleTools Upgrade

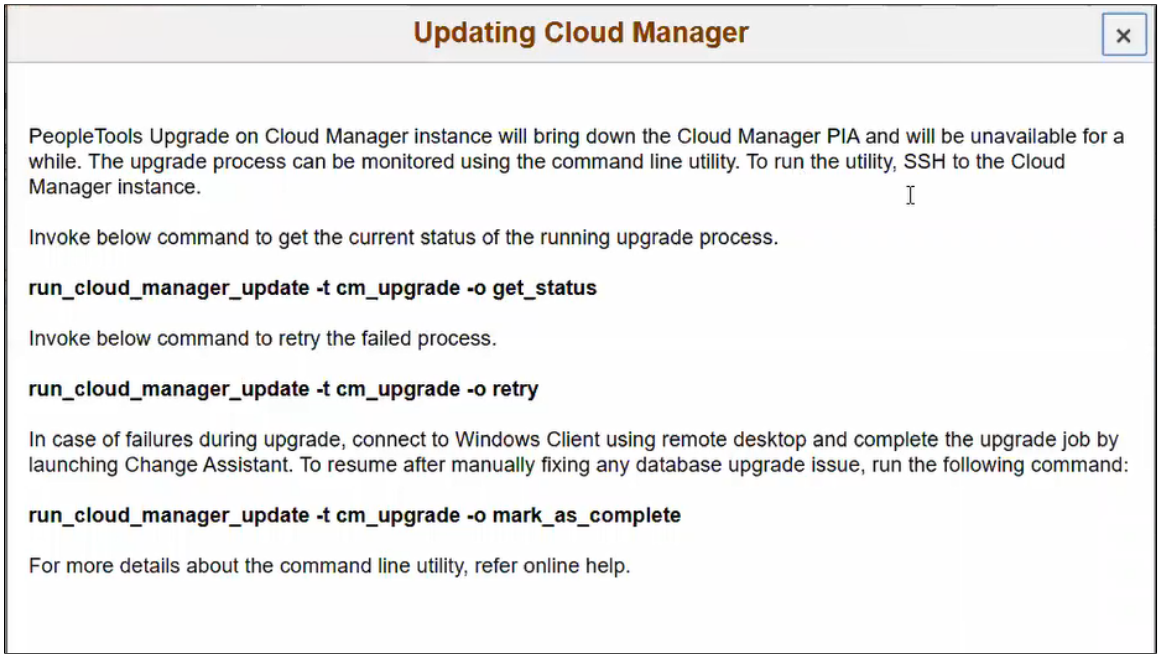
The automated Cloud Manager update process will trigger PeopleTools upgrade when the newly released Cloud Manager (IH) Update Image has a dependency on a particular PeopleTools version. During the update process, when it reaches the step to upgrade PeopleTools, the Cloud Manager PIA UI will be shutdown and the status of PeopleTools upgrade is no longer available on the UI.

To monitor the PeopleTools upgrade, you need to SSH into the Cloud Manager instance and use the PeopleTools upgrade command line.

The Info icon on the Cloud Manager Updates page, displays the command line options to use for monitoring the PeopleTools upgrade.

Image: Updating Cloud Manager modal window

This example illustrates the fields and controls on the Updating Cloud Manager modal window.



See Command Line Operations for cm_upgrade for additional information.

Manually Applying Updates Using Selective Adoption

It is highly recommended to update Cloud Manager as soon as a new image is available. Cloud Manager Image 9 to Image 11 cannot be automatically updated.

Updating to latest Cloud Manager from Cloud Manager Image 9 or lower, involves two steps. The latest version has dependencies on PeopleTools 8.58 and hence requires updating PeopleTools on the existing Cloud Manager instance.

1. Update Cloud Manager application using Selective Adoption method.

   See Updating Cloud Manager Application Using Selective Adoption

2. Upgrade PeopleTools on Cloud Manager to 8.58 using the command line utility.

   See Upgrading Cloud Manager PeopleTools Using Command Line

Updating Cloud Manager Application Using Selective Adoption

Note: Backup the Cloud Manager instance before applying updates.

To apply updates to Cloud Manager, perform the following:

1. Deploy the Interaction Hub (IH) PUM source.

   To deploy an IH PI environment using Cloud Manager, perform the following.

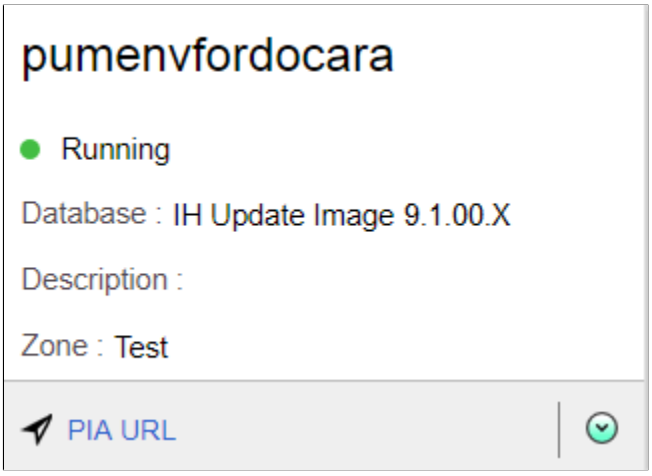
   a. Subscribe to the IH download channel. The IH 9.1 Linux channel will download IH PI and PRPs, which have Cloud Manager fixes.

   b. Create a template to deploy the PeopleSoft Interaction Hub 9.1 database on a PUM topology.

   c. Deploy a new PUM source using the newly created template.

      Image: Example Deployed PUM Source

      This example illustrates the running PUM source.



Note the Windows Client IP on the Environment Details page in the PeopleSoft Client section.

2. Modify PI Home share permissions on PUM source.

Note: This step is optional if there are no PRPs to apply.

By default, the PI Home share on PUM Source is read-only. You can verify this by accessing the PI Home (\\<PUM SRC IP>\pi_home) on the Windows client (that was deployed using PUM topology) and trying to create a folder in it. Cloud Manager PRPs need to update files on PI HOME, therefore you must modify the share permissions. Modify or add the [pi_home] section in the smb.conf file:

a. SSH to Cloud Manager.

b. From Cloud Manager ssh to the PUM source instance (pumenvfordcoara-lnxft-1)

```
[opc@pi6cmdoc ~]$ sudo su - psadm2
[psadm2@pi6cmdoc ~]$ ssh -i /home/psadm2/psft/data/cloud/ocihome/keys/cm_⇒
adm_pvt_key opc@pumenvfordcoara-lnxft-1
```

c. Set SMB password for user psadm3.

```
[opc@pumenvfordcoara-lnxft-1~]$ sudo smbpasswd -a psadm3
New SMB password:
Retype new SMB password:
```

d. Add or update pi_home share on the PUM source. Ensure the following section is changed or added in the smb.conf file as shown here:

```
[opc@pumenvfordcoara-lnxft-1~]$ sudo vi /etc/samba/smb.conf

[pi_home]
        path = /u01/app/oracle/product/pt/ps_pi_home
        writable = yes
        available = yes
        guest ok = no
        valid users = psadm3
```

Note: For OCI, please append the entire section given above in /etc/samba/smb.conf file.

e. Restart samba service

```
[opc@pumenvfordcoara-lnxft-1~]$ sudo service smb restart
Shutting down SMB services: [ OK ]
Starting SMB services: [ OK ]

[opc@pumenvfordcoara-lnxft-1~]$
```

f. Open firewall to allow samba ports on PUM source using below command.

```
[opc@pumenvfordcoara-lnxft-1~]sudo iptables -I INPUT -p tcp -m state --st⇒
ate NEW -m tcp --dport 137 -s 0.0.0.0/0 -j ACCEPT

[opc@pumenvfordcoara-lnxft-1~]sudo iptables -I INPUT -p tcp -m state --st⇒
ate NEW -m tcp --dport 138 -s 0.0.0.0/0 -j ACCEPT

[opc@pumenvfordcoara-lnxft-1~]sudo iptables -I INPUT -p tcp -m state --st⇒
ate NEW -m tcp --dport 139 -s 0.0.0.0/0 -j ACCEPT

[opc@pumenvfordcoara-lnxft-1~]sudo iptables -I INPUT -p tcp -m state --st⇒
ate NEW -m tcp --dport 445 -s 0.0.0.0/0 -j ACCEPT

[opc@pumenvfordcoara-lnxft-1~]sudo service iptables save
```

g. Enable secure linux to allow samba share.

```
[opc@pumenvfordcoara-lnxft-1~]sudo chcon -t samba_share_t /u01/app/oracle⇒
/product/pt/ps_pi_home
```

3. RDP to the windows client of PUM source.

   Windows Client IP can be determined by going into the Environment Details page and looking at PeopleSoft Client section.

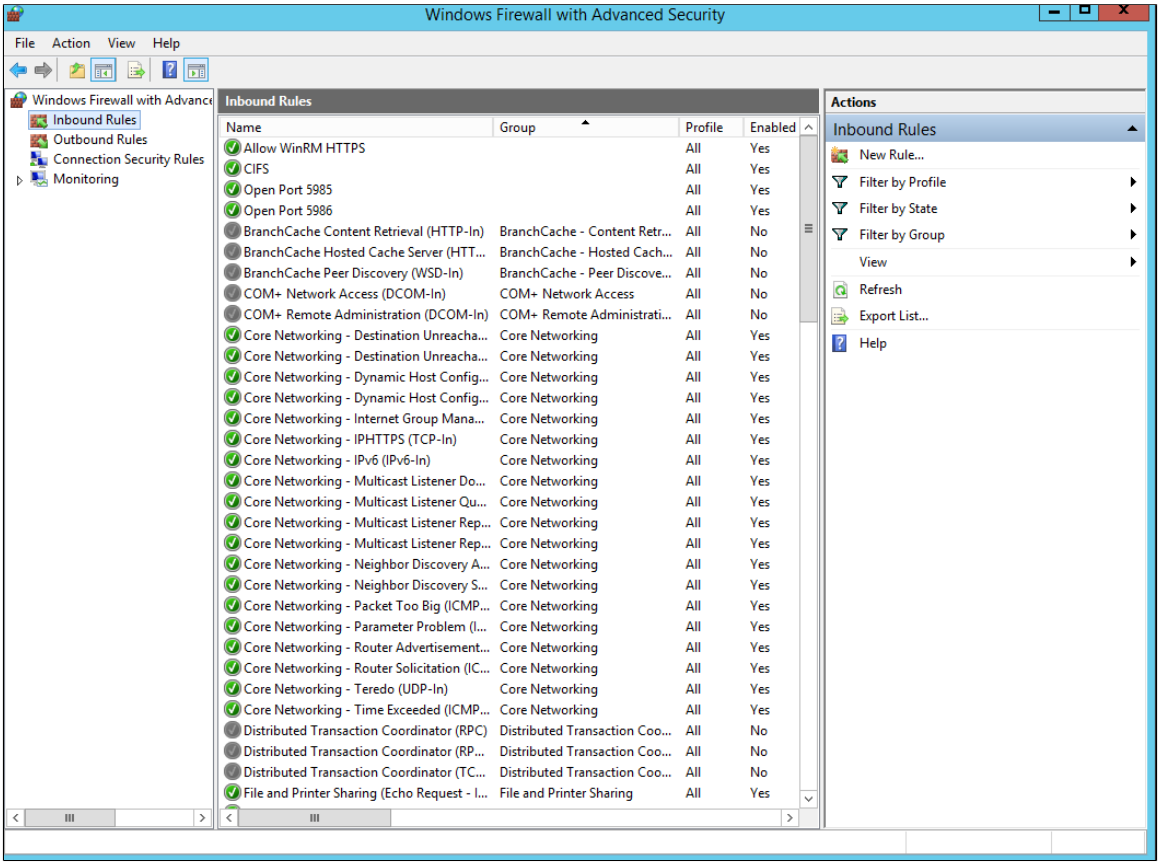
4. Configure Windows firewall (if not already configured)

   Add new rule(CIFS) to open ports 137,138,139,445. This is an optional step if its already configured this can be skipped. To manually add the rules:

   a. In Windows Client Navigate to Start >Windows Firewall with Advanced Security

      Image: Windows Firewall with Advanced Security

      This example illustrates the Windows Firewall with Advanced Security window.

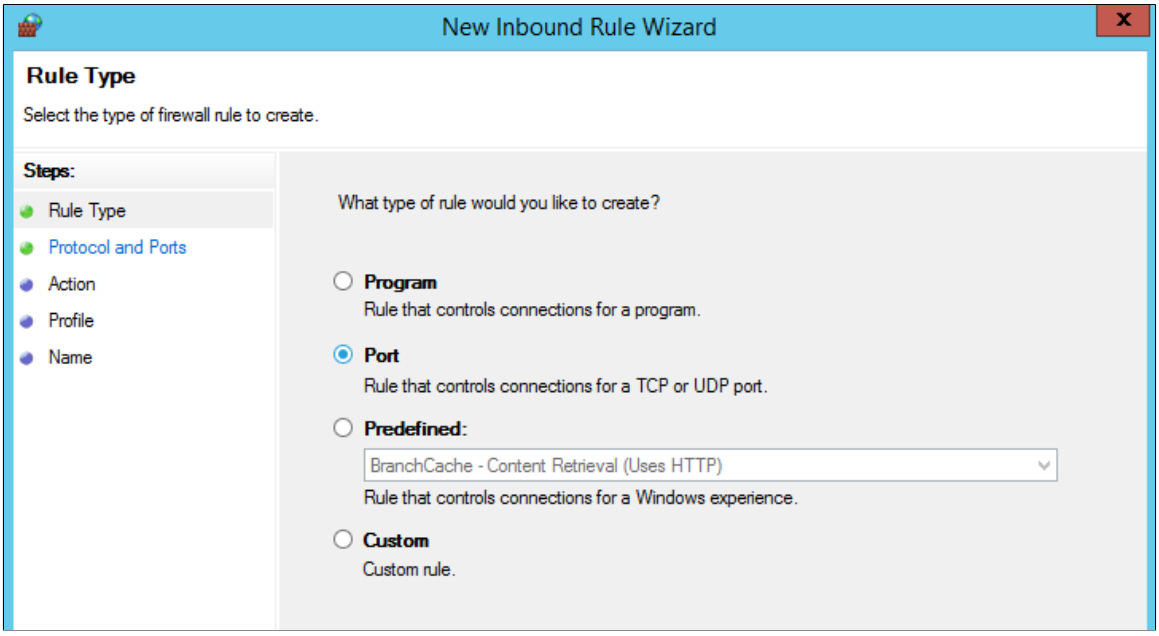


   b. Click Inbound Rules > New Rules.

   c. On the Rule Type window, select Port and click Next.

Image: New Inbound Rule Wizard

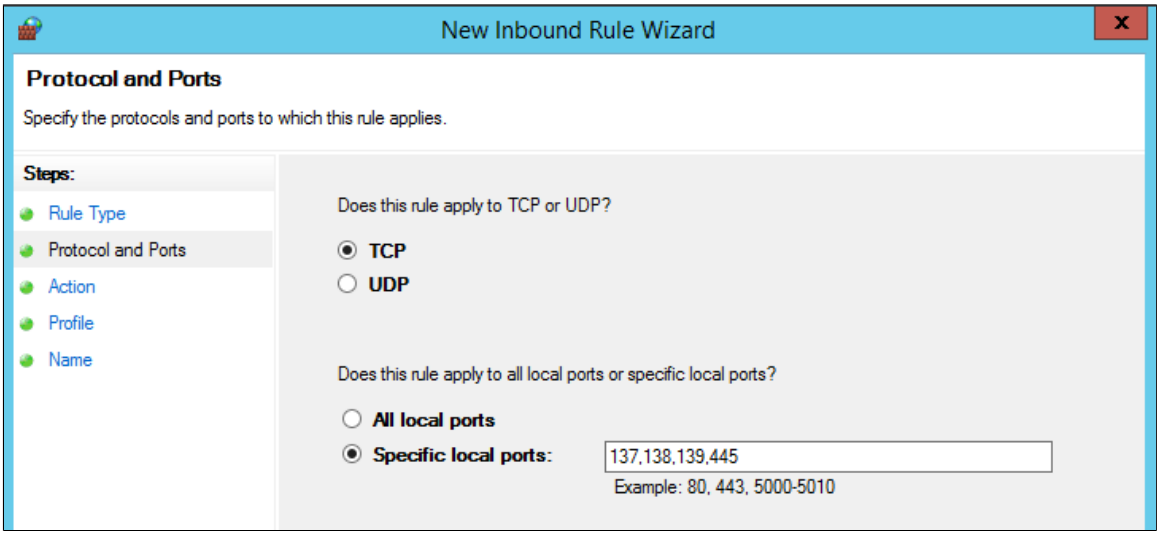
This example illustrates the New Inbound Rule Wizard window.



d. On the Protocol and Ports window, select TCP and Specific local ports. Enter ports 137,138,139,445 and Next.

Image: New Inbound Rule Wizard – Protocol and Ports

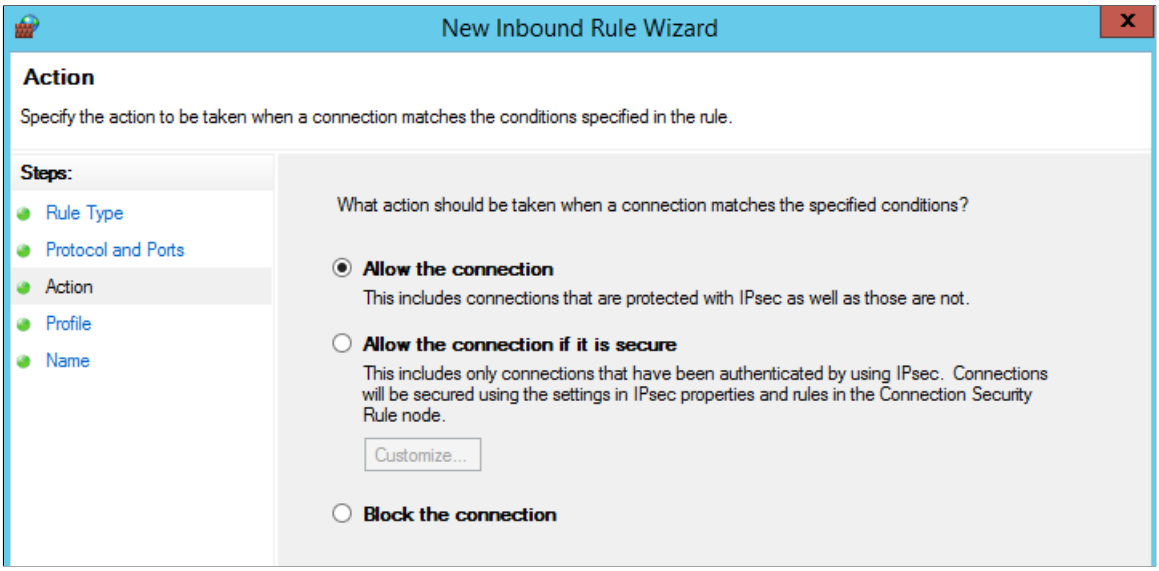
This example illustrates the specific local ports required for Cloud Manager access to Windows client.



e. On the Action window, select Allow the connection and click Next.

Image: New Inbound Rule Wizard – Action window

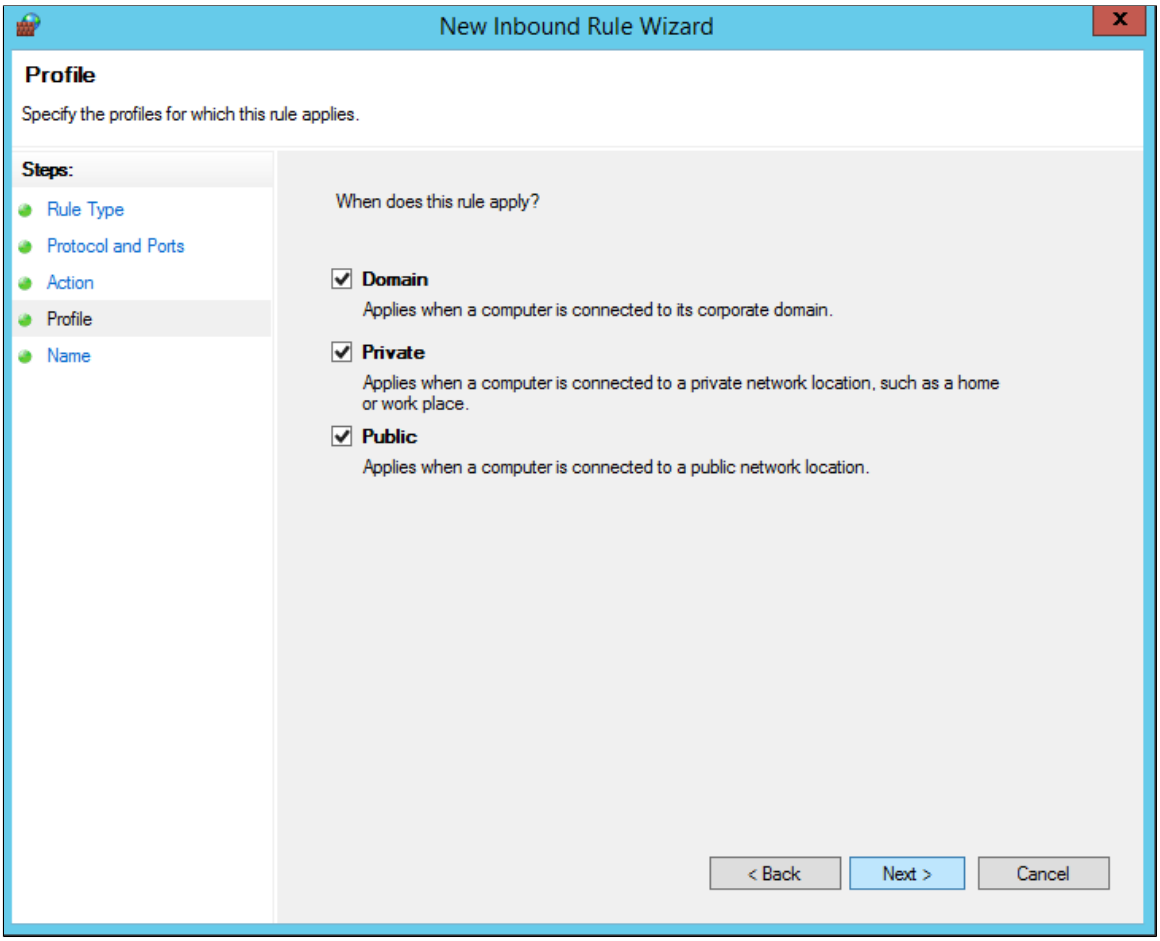
This example illustrates the fields and controls on the New Inbound Rule Wizard – Action window.



f. On the Profile window, select when the rule applies and click Next.

Image: New Inbound Rule Wizard – Profile window

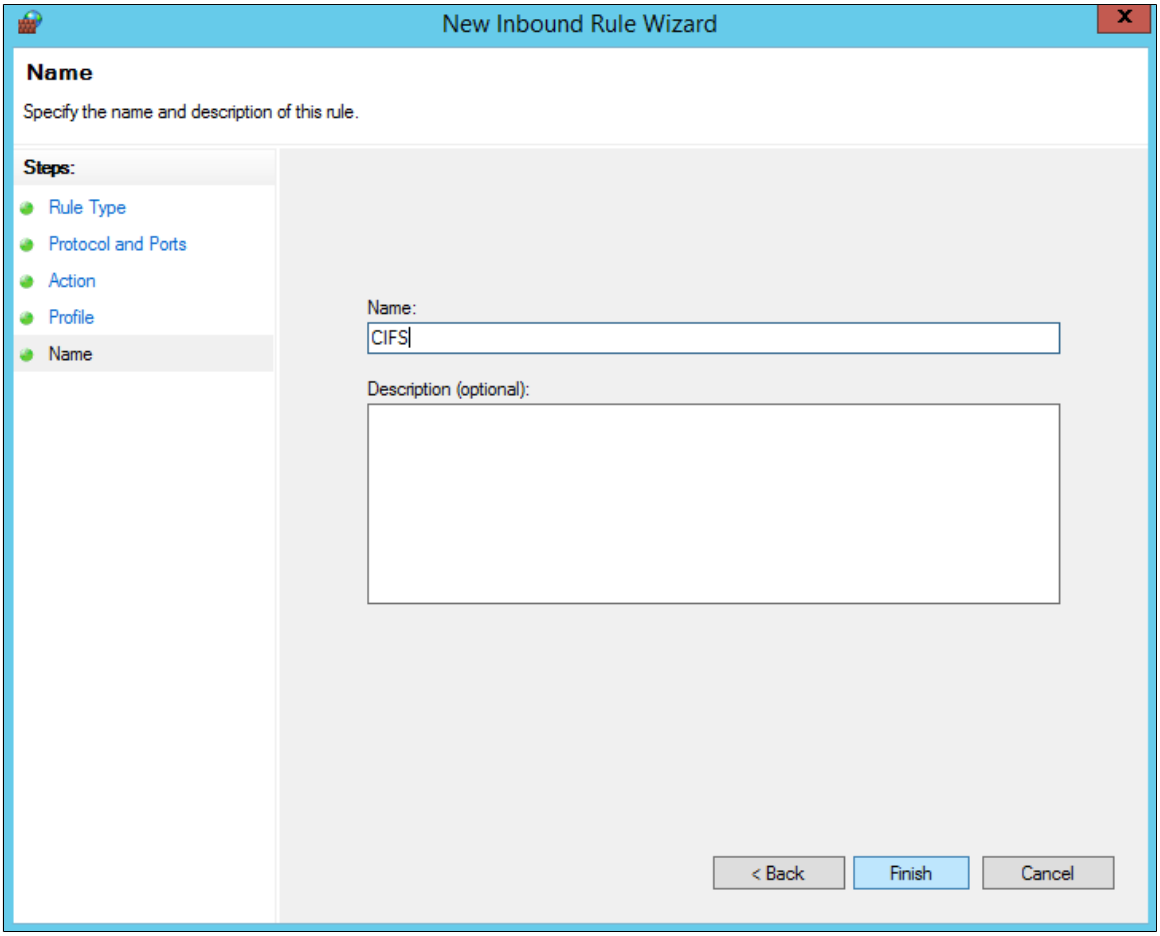
This example illustrates the fields and controls on the New Inbound Rule Wizard – Profile window.



g. On the Name window, provide the name as *CIFS* and Finish.

Image: New Inbound Rule Wizard – Name window

This example illustrates the fields and controls on the New Inbound Rule Wizard – Name window.

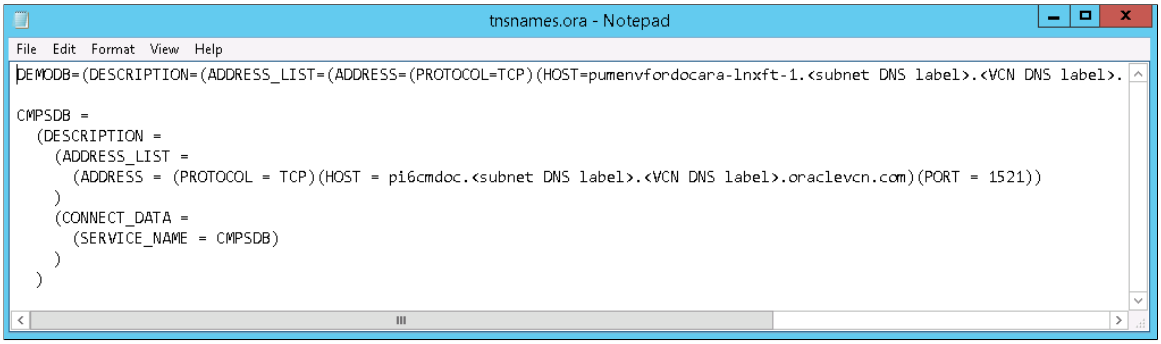


5. In Windows Client, provide the tns entry of PUM source and Cloud Manager target database in D:\oracle\product\12.1.0\client_1\network\admin\tnsnames.ora.

   In this example DEMODB is the PUM source database and CMPSDB is the target Cloud Manager database.

   Image: Example tnsnames.ora file

   This example illustrates the tnsnames.ora file that contains the source and target databases.



Note: The tnsnames.ora file would include the actual subnet and vcn names.

6. Install the required version of PeopleTools Client (PTC) on the Windows Client if the installed version is different from what is required for Selective Adoption. For example, when updating from Cloud Manager Image 8 or lower to Cloud Manager Image 9, PeopleTools Client must be used from PeopleTools 8.56.12 onwards. Obtain the DPK from file server or download from My Oracle Support. The PTC DPK on the file server can be accessed on the Windows Client using CIFS Share - \\<FileServer_Pvt_IP>\u01\app\oracle\product\dpk\linux\IH\09\IH-910-UPD-009-OVA_5of13.zip \PTC-DPK-WIN8.56.12-1of1.zip.

   To install the PeopleTools Client:

   a. Extract the PTC-DPK-WIN8.56.12-1of1.zip file to a directory. This directory will contain SetupPTClient.bat.

   b. Open a command window running as administrator.

   c. Change directory to the location where you unzipped PTC-DPK-WIN8.56.12-1of1.zip file.

   d. Run SetupPTClient.bat -t.

   e. Answer yes when asked if you want to deploy PeopleTools client.

   f. Specify an installation directory, the RDBMS, and other information for your environment. The default installation directory is C:\PT<release_number>_Client_<database_type>.

   g. At the prompt Please make your selection for the Tools Client deployment, specify option 3 -None of the above to install PeopleTools client PS_HOME.

   h. Answer n (no) when asked if you want to install Change Assistant.

   Note: Do not install PeopleTools Client under D:\psft. This path is used by Cloud Manager for deployment automation. Choose a different path when installing PeopleTools Client manually on a Windows Client that was provisioned by Cloud Manager.

7. Configure Cloud Manager target and IH PUM source databases manually in Change Assistant.

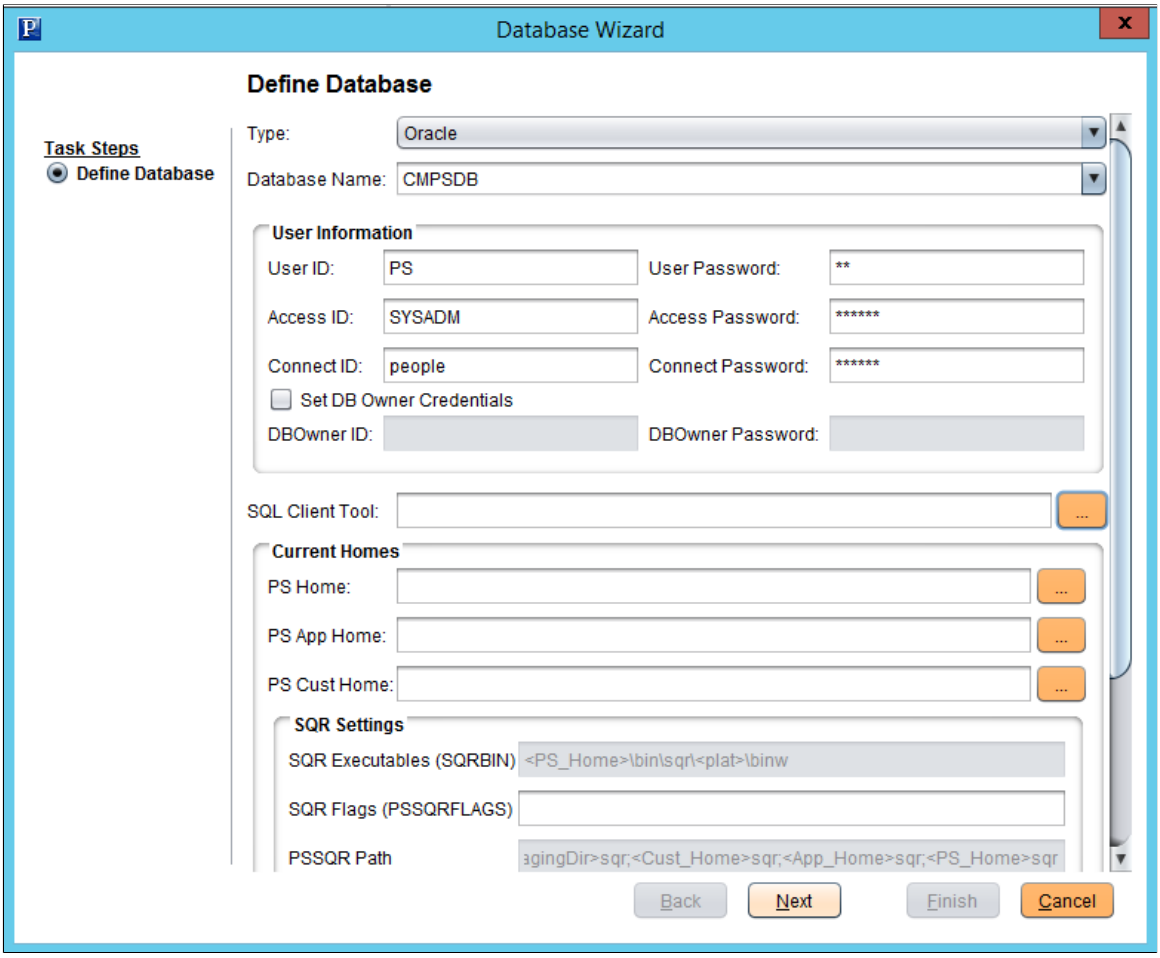
   To configure the source and target databases in Change Assistant:

   a. In Windows Client, launch Change Assistant as administrator.

   b. In Change Assistant select File, New Database.

Image: Define Database

This example illustrates the fields and controls on the Define Database page. You can find definitions for the fields and controls later on this page.



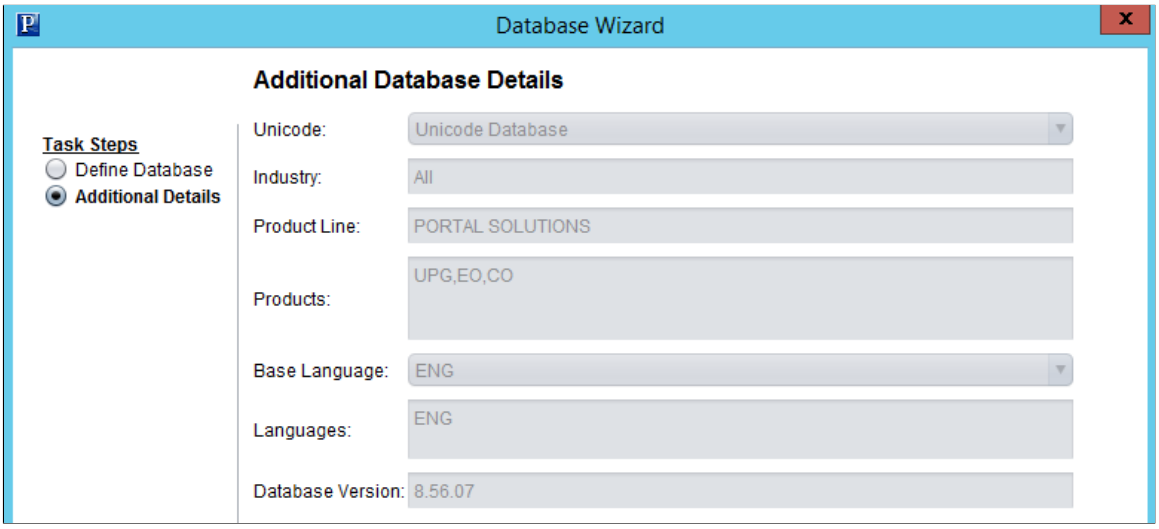
Type	Database type is Oracle.
Database Name	Enter the name of the database.
User ID and **Password**	Enter the PeopleSoft User ID and password for the database that used during the Cloud Manager bootstrap process.
Access ID and **Password**	Enter the Access ID and password for the database that used during the Cloud Manager bootstrap process.
ConnectID and **Password**	Enter the ConnectID and password for the database that used during the Cloud Manager bootstrap process.
SQL Client Tool	Browse for SQL client tool in D:\oracle\product\12.1.0\client_1\bin\sqlplus.exe.
Current Homes **PS Home**	Enter the location of your current PS_HOME
Current Homes **PS App Home**	Enter the location of your current PS_APP_HOME

Current Homes **PS Cust Home**	Enter the location of your current PS_CUST_HOME
SQR Settings **SQR Executables (SQRBIN)**	The SQRBIN value is read only and derived from the PS Home and platform setting.
SQR Settings **SQR Flags (PSSQRFLAGS)**	By default, the -ZIF parameter is to set the full path and name of the SQR initialization file, SQR.INI
SQR Settings **PSSQR Path**	This field is read-only and will contain the path that is used in Change Assistant.

c. Click Next, to bring up Additional Database Details window.

Image: Additional Database Details window

This example illustrates the fields and controls on the Additional Database Details window.



d. Review the window and click Next.

e. On the Confirm Settings page, click Finish.

f. Repeat steps b thru e to define the PUM source database.

Note: To confirm both databases have been defined in Change Assistant, select File, Open Databases. You will see two databases defined.

---

8. Configure Change Assistant Options for Updates.

To configure Change Assistant Options for Updates:

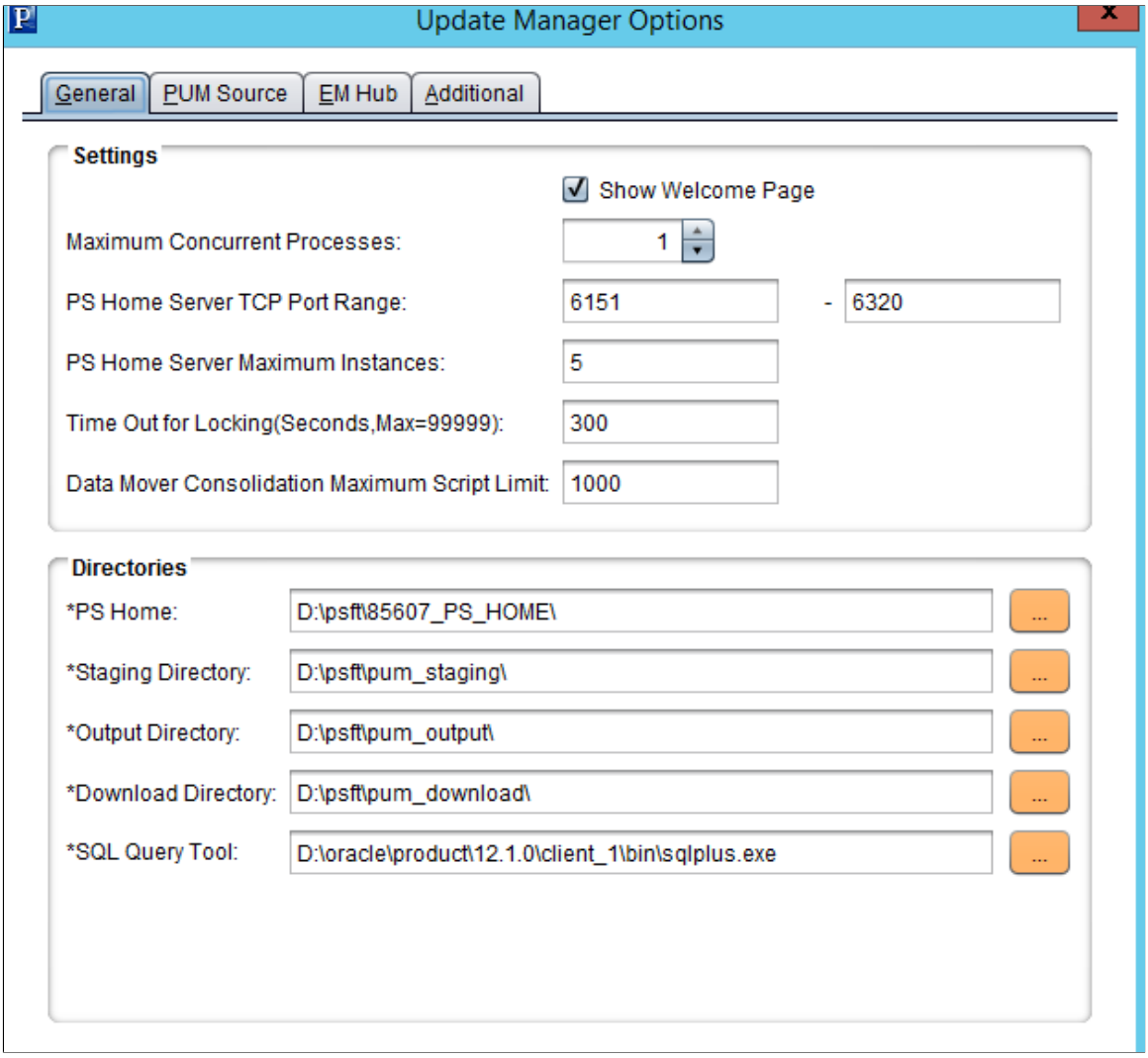
a. Create directories in the Windows client for pum_staging, pum_output and pum_download under D:\psft\.

b. In Change Assistant, select Tools, Options.

c. On the General tab, enter the directories.

Image: Update Manager Options – General page

This example illustrates the fields and controls on the Update Manager Options – General page. You can find definitions for the fields and controls later on this page.

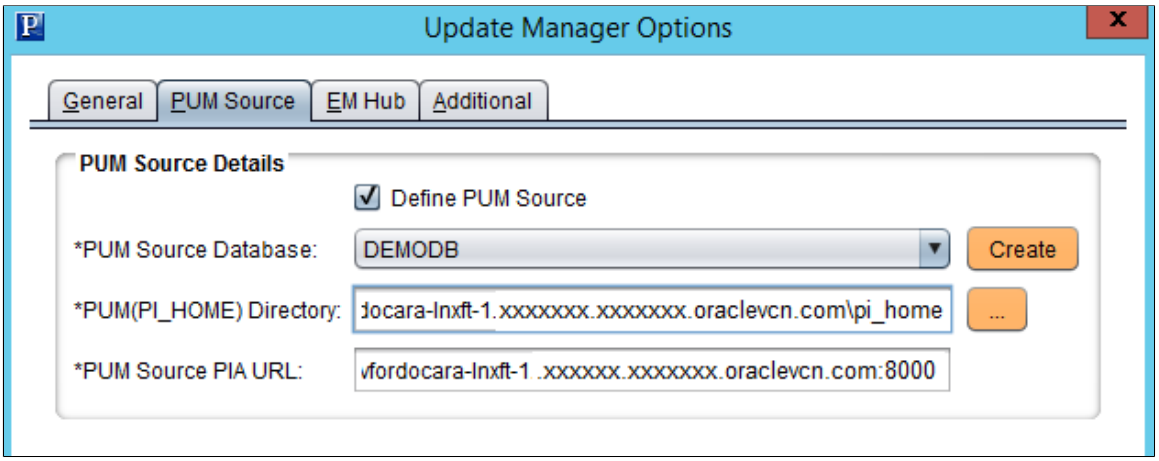


PS Home	Enter the full path for PeopleTools client installed on the Windows Client machine.
Staging Directory	Enter the staging directory defined in step a.
Output Directory	Enter the output directory defined in step a.
Download Directory	Enter the download directory defined in step a.
SQL Query Tool	Enter the path to sqlplus.exe.

d. On the PUM Source page, enter the PUM Source information.

Image: Update Manager Options – PUM Source page

This example illustrates the fields and controls on the Update Manager Options – PUM Source page. You can find definitions for the fields and controls later on this page.



Define PUM Source Select this check box to define the PUM Source.

PUM Source Database Select the PUM source database from the drop down list.

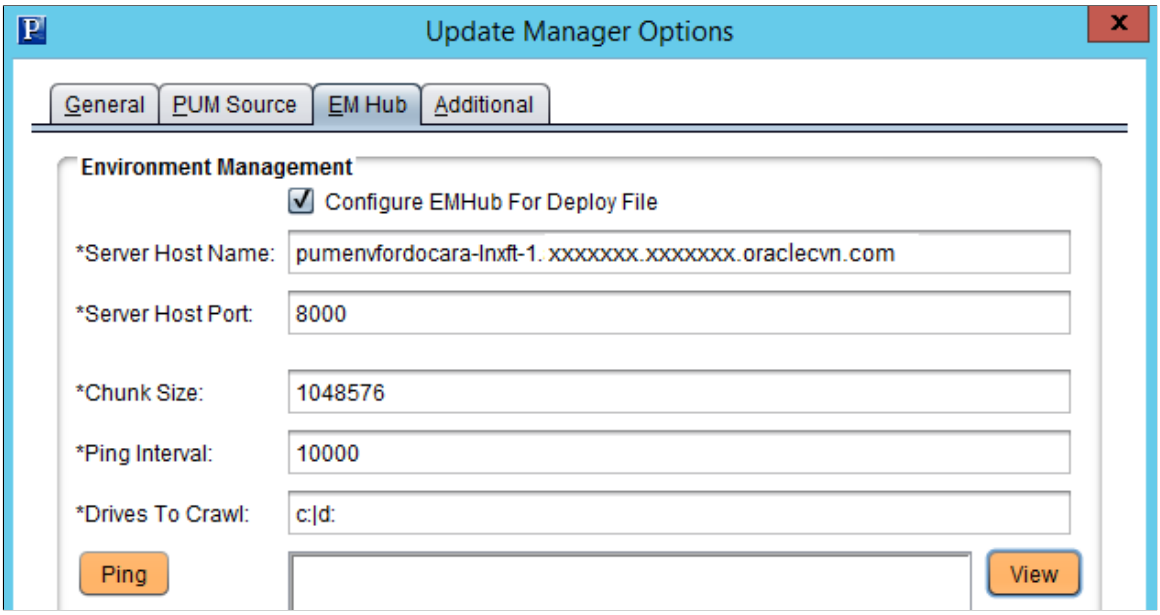
PUM(PI_HOME) Directory Use the share that was modified in step 2. Access the share path on the windows client and verify access. Use directory path as shown in the address bar of the explorer window.

PUM Source PIA URL Enter the URL to sign on to the PUM Source.

e. On the EMHUB page, enter the EMHub information.

Image: Update Manager Options – EM Hub page

This example illustrates the fields and controls on the Update Manager Options – EM Hub page. You can find definitions for the fields and controls later on this page.



Configure EMHub For Deploy File Select this check box if you want to use EMHub for file deploy.

Server Host Name Enter PUM source server host name.

Server Host Port Indicates the port in which to connect to the Environment Management hub.

9. Backup Cloud Manager.

   Take a Cloud Manager backup before applying any updates. See Understanding Cloud Manager Backup and Restore.

10. Apply PRPs to the IH PUM source.

    If there are PRPs to be applied on the PUM source, copy all PRPs to the Windows Client under the D:\psft\pum_download location. PRPs must be copied from the file server share.

    To copy the PRPs to the file share:

    a. Identify the private IP address of file server on the Instances tab in the Oracle Compute Cloud Service Console.

    b. Log on to the Windows Client of the environment.

    c. Connect to the samba share using \\<File_Server_IP>\PRP.

       User will be prompted for user name and password that was configured in step 2.

Note: In OCI, if the samba share is not accessible on the Windows client VM, check the ingress security rules for the samba share on the subnet where the windows client is connected. In OCI, the Cloud Manager subnet must allow incoming connections from the subnet on which the PUM source is set up.

d. Copy the required PRPs to D:\psft\pum_download directory on the Windows Client.

e. In Change Assistant, select Tools, Apply PeopleSoft Release Patchset.

f. Verify the download location is set to the directory used in step c (D:\psft\pum) and click Next.

g. Select all PRPs to be applied and click Next.

Note: In some cases, selecting and applying all PRPs together might show errors. In such a case, select one PRP at a time and apply individually.

h. Change Assistant will verify that the package is compatible with the PI version. If it is not compatible, you will receive a message to Apply Compatible Packages Only.

i. Click OK to apply only compatible packages and Change Assistant will verify the PRPs.

j. Click Next and you will see the summary page.

k. Click Finish. The Change Assistant job is created. Run this job as you would any other change package.

11. Start PSEMAgent on target Cloud Manager.

    To start PSEMAgent:

    a. Change ownership of PSEMAgent dir from psadm1 to psadm3.

```
[psadm3@c6e65e ~]$ chown -R psadm3:appinst /opt/oracle/psft/pt/ps_home8.5⇒
6.07/PSEMAgent/
[psadm3@c6e65e ~]$ cd /opt/oracle/psft/pt/ps_home8.56.07/PSEMAgent/
[psadm3@c6e65e PSEMAgent]$ ll
total 44
-rwxr-xr-x 1 psadm3 appinst  2742 Sep 11  2015 StartAgent.sh
-rwxr-xr-x 1 psadm3 appinst  2426 Sep 11  2015 StopAgent.sh
drwxr-xr-x 8 psadm3 appinst  4096 Jan  6 05:11 envmetadata
drwxr-xr-x 2 psadm3 appinst  4096 Sep 23 06:11 lib
```

    b. Configure the agent configuration properties file. The configuration. properties file is located in the ps_home directory/PSEMAgent/envmetadata/config.

    This is an example of the configuration.properties file:

```
#hubURL= this is the host and port the agents talk to
hubURL=http://pumenvfordcoara-lnxft-1.<subnet DNS label>.<vcn DNS label>.⇒
oraclevcn.com:8000/PSEMHUB/hub
agentport=5283

#ping interval in milliseconds for the peer to contact the hub for new me⇒
ssages
pinginterval=10000

#Windows directories need to use the forward slash ('/') character. For m⇒
ultiple directories, use a '|' character as separator
```



```
windowsdrivestocrawl=c:|d:
unixdrivestocrawl=/opt/oracle/psft/pt|/home/psadm2/psft/pt/8.56

#The time interval in hours for the hub to issue a recrawl command to the⇒
 agents
recrawlinterval=24

#The time interval in hours for the hub to issue a revalidate command to ⇒
the agents
revalidateinterval=6

#Setting for large file transfer.default is 1024 * 1024 bytes
chunksize=1048576
```

c. Export PS_APP_HOME before starting agent.

```
$ export PS_APP_HOME=/opt/oracle/psft/pt/ps_app_home.
```

d. Start PSEMAgent using user psadm3.

```
$ /opt/oracle/psft/pt/ps_home8.56.07/PSEMAgent/StartAgent.sh
```

Optionally run the agent in background by appending & to the above command.

12. Upload target database information to IH PUM source.

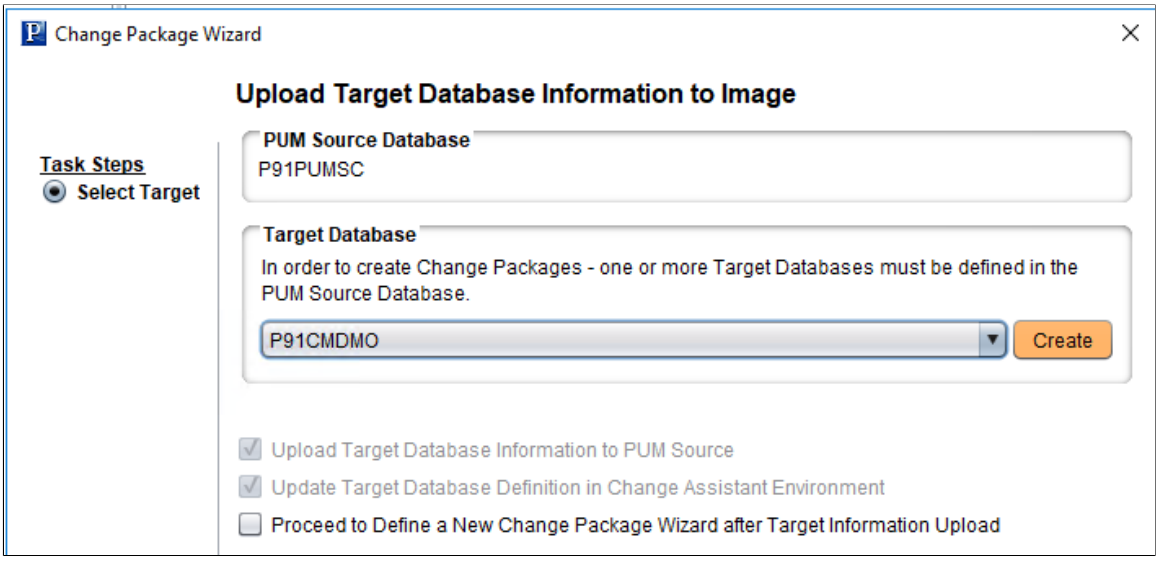
To upload target database information:

a. In Change Assistant, upload the target database information. Select Tools, Upload Target Database Information to Image.

b. Select the target database from the drop-down.

Image: Upload Target Database Information to Image

This example illustrates the fields and controls on the Upload Target Database Information to Image.



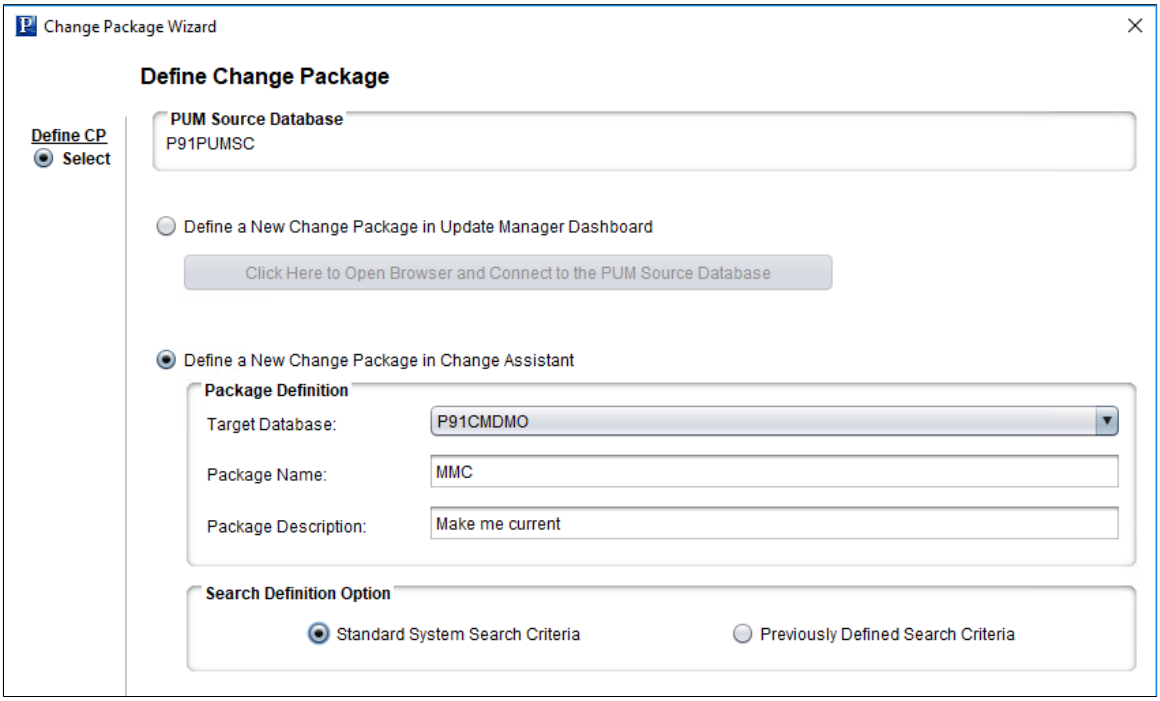
c. Click Finish.

Target Database information is uploaded.

13. Define a make me current change package in Change Assistant..
    a. Select Tools, Define Change Package.
    b. Select Define a New Change Package in Change Assistant radio button.
    c. Enter the package information.
    d. Select Standard Search Option Criteria radio button.

    Image: Define a New Change Package in Change Assistant

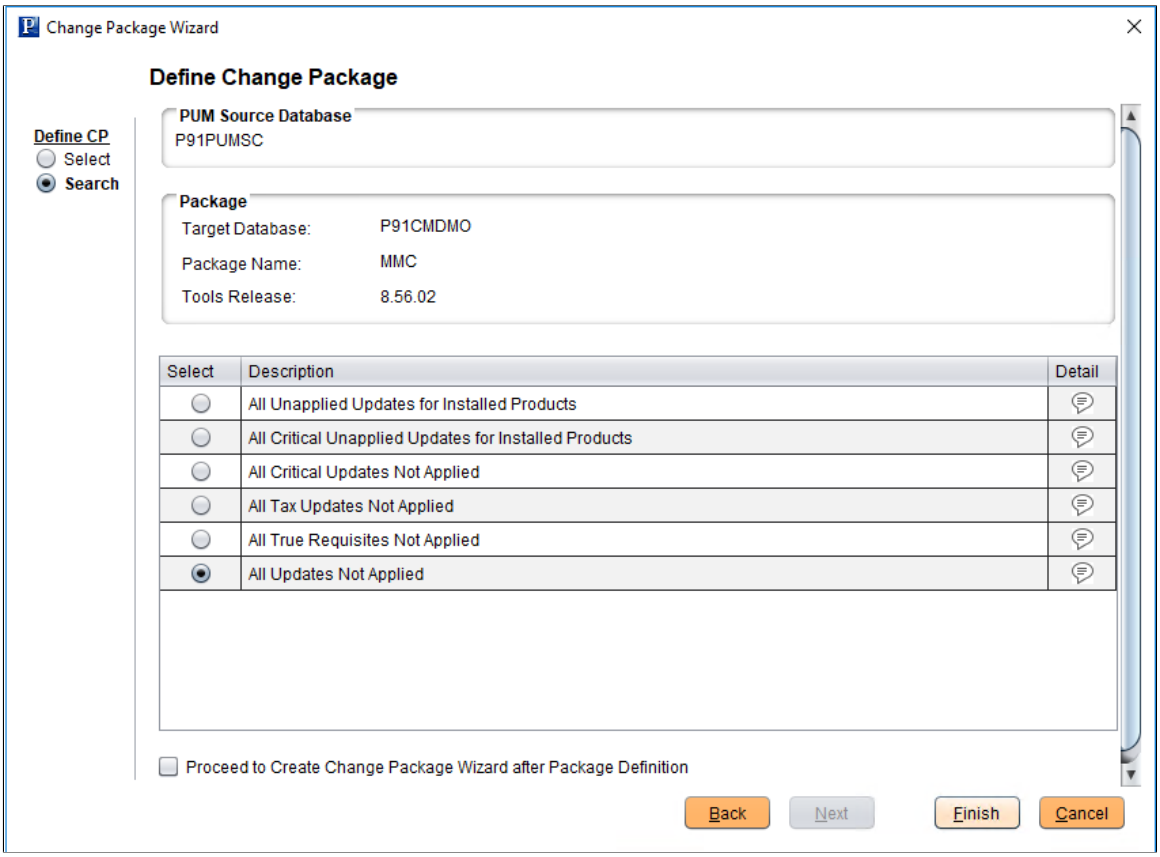
    This example illustrates the fields and controls on the Define Change Package in Change Assistant with Define a New Change Package in Change Assistant selected.



    e. Click Next.
    f. Select All Updates Not Applied.

Image: All Updates Not Applied

This example illustrates the fields and controls on the Define Change Package page with the option All Updates Not Applied selected.



Optionally, select the Proceed to Create Change Package Definition check box to create the change package. If this option is selected, the Next button is enabled.

g. Click Finish.

14. Create change package in Change Assistant.

To create the change package in Change Assistant:

Note: If you selected the Proceed to Create Change Package Definition check box in step 13, the change package is already created and you can skip this step.

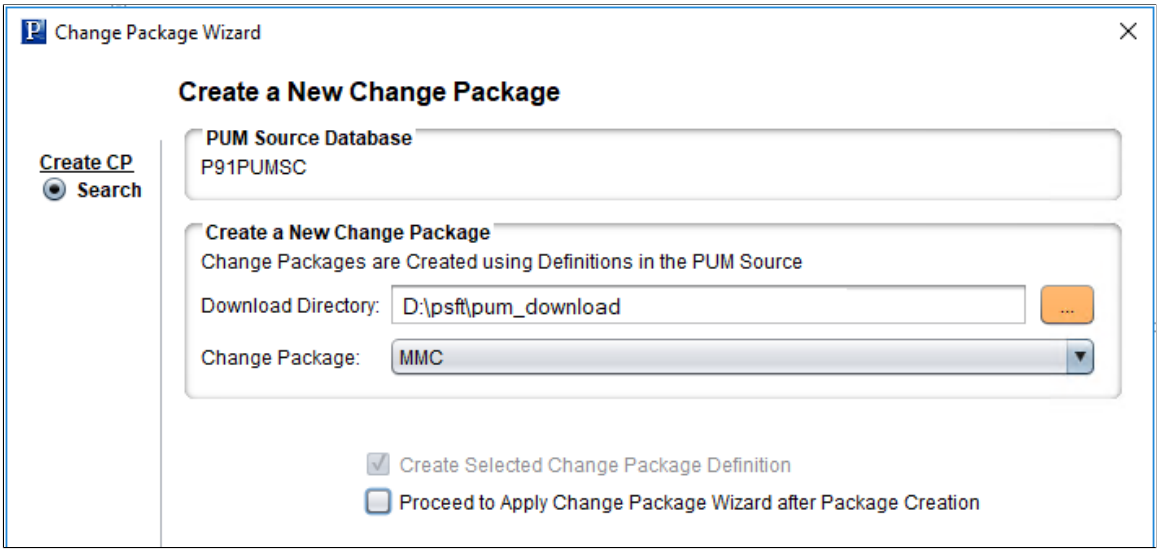
---

a. Select Tools, Create Change Package.

b. Select the change package definition that was just created in PUM and click Finish.

Image: Create a New Change Package page

This example illustrates the fields and controls on the Create a New Change Package page. You can find definitions for the fields and controls later on this page.



Optionally select the proceed to Apply Change Package Wizard after Package Creation.

c. Click Finish.

The change package is generated in the Download Directory.

15. Apply change package in Change Assistant.

To apply the generated change package:

a. Select Tools, Apply Change Package.

b. Select the change package to apply. Apply type is Initial Pass.

c. Click Next.

d. Select the target database (your target Cloud Manager database) from the drop-down and click Next.

e. Ensure there are no errors in the compatibility click and click Next.

f. On the Summary page, click Finish.

g. When the job is complete, there will be a confirmation. If there are any errors found while executing the job, those must be manually fixed.

16. Manually copy the customization script.

Copy a post update customization script from the PUM source instance to the target Cloud Manager instance. Use scp to copy.

a. SSH to Cloud Manager VM.

b. Change to root user $sudo bash.

c. Securely copy the customization script.

```
scp -i /home/psadm2/psft/data/cloud/ocihome/keys/cm_adm_pvt_key opc@<pum_⇒
src_hostname>:<pum_source_base_dir>/pt/ps_pi_home/cl/Unix/AppBatch/bse/cl⇒
oud/cm_update_customization.sh  $PS_APP_HOME/cloud
```

Where:

pum_src_hostname	Hostname of PUM source instance. The hostname can be determined in the Environment Details page for the PUM source environment.
PS_APP_HOME	Path to PS_APP_HOME on Cloud Manager. For example: /opt/oracle/psft/pt/ps_app_home.
pum_source_base_dir	PeopleSoft deployment directory. The base directory can be determined in the Manage Attributes page, under Manage Environment > Full Tier > Other Attributes PeopleSoft Deployment Path. This is a mandatory input.

17. Run the customization script to complete the updates on target Cloud Manager.

The script does the following tasks:

- Update files from PUM source
- Synchronize code to File Server
- Cleanup old jar files
- Restart the domains

To execute the post update utility script for MMC package updates, perform the following steps:

If you are running Cloud Manager in OCI:

a. Login to Cloud Manager VM.

b. Change to root user $sudo bash.

c. Change directory to /opt/oracle/psft/pt/ps_app_home.

d. Execute the cm_update_customization.sh script as root user with ps_app_home directory as current working directory.

```
$ sudo bash
$ cd /opt/oracle/psft/pt/ps_app_home/
$ sh cloud/cm_update_customization.sh <pum_source_host_name> <pum_source_⇒
base_dir>
```

Where:

pum_source_host_name	Hostname of PUM source instance. The hostname can be determined in the Environment Details page for the

	PUM source environment. Do not use a fully qualified hostname. This is a mandatory input.
pum_source_base_dir	PeopleSoft deployment directory. The base directory can be determined in the Manage Attributes page, under Manage Environment > Full Tier > Other Attributes PeopleSoft Deployment Path. This is a mandatory input.

18. Reboot Web (PIA) Server domain.
19. Verify changes on Target Cloud Manager

    You need to manually verify the modifications done on the target Cloud Manager.

    For more details on Change Assistant configurations, refer to online help for Change Assistant and Update Manager.

Once Cloud Manager is upgraded proceed to step 2 Upgrading Cloud Manager PeopleTools Using Command Line.

Upgrading Cloud Manager PeopleTools Using Command Line

The Cloud Manager command line option can be used for triggering the PeopleTools upgrade and monitoring the upgrade status. This command line utility can be used to upgrade PeopleTools for Cloud Manager instances that are on PeopleTools bel0w 8.58. If self update was used (Cloud Manager Image 10 to Image 11), the PeopleTools upgrade is included in the process. For Cloud manager 9 and below, a PeopleTools upgrade is required.

Note: If you are running Cloud Manager Image 8 or lower, you must upgrade to Cloud Manager Image 11 using selective adoption to obtain the command line utility for automated PeopleTools upgrade.

To use the command line utility to upgrade PeopleTools:

1. Subscribe to the PeopleTools download channel. Ensure that the download is complete.

   For example: Interaction Hub PI 9.1.11 has PeopleTools version 8.58.03, therefore you must subscribe to PeopleTools 8.58 Linux download channel with a minimum patch version of 8.58.03. To determine the PeopleTools version on the IH PUM Source, SSH into the IH PUM Source, switch user to psadm2 and run **psadmin -v** command. See Accessing Provisioned Environments
2. Log into the Cloud Manger machine using SSH.
3. Create a response file.

   See Creating Response File
4. Backup Cloud Manager instance. See Using Automated Backup and Restore Utility.

   Important! The backup will be available in case of any failures in the PeopleTools upgrade process, allowing you to restore to this point.

   ---

5. Run the command line to execute the upgrade.

```
run_cloud_manager_update -t <task_name>  -o <operation_name > -r <response_fil⇒
e.json>
```

Example: run_cloud_manager_update -t cm_upgrade -o execute -r /tmp/cm_update_rsponse_file.json

See Command Line Operations for cm_upgrade

Understanding the Command Line

The command line has the following Hierarchy:

```
Command > Task > Operation > Subtask >Activity
```

- Command

  The command is **run_cloud_manager_update**.

- Task

  For Cloud Manager Image 9, the only supported task is **cm_upgrade** [-t option].

- Operation

  Multiple operation s [-o option] are available for a task. For cm_upgrade operations see Command Line Operations for cm_upgrade

- Subtasks

  Each operation contains one or more subtasks. See Subtasks for PeopleTools Upgrade [PTU] in Cloud Manager Instance.

- Activity

  Each subtask may have multiple activities.

Command Line Operations for cm_upgrade

The task *cm_upgrade* is used to perform a PeopleTools Upgrade [PTU] in Cloud Manager instance. The input values are given as response file. The format is:

```
run_cloud_manager_update -t cm_upgrade  -o <operation_name> -r <response_file.json>⇒
```

This table lists the operation/subtask details.

Operation Type [-o]	***Description/Details***
execute	This operation is used for executing the current task. If the response file is present it will read the response file and that will be used for creating the input values for the task execution.

Operation Type [-o]	*Description/Details*
get_status	This operation is used to display the current task status in the console. The status will show the execution status at the activity level. -v [verbose] option can be used for the detailed status. The activity status will be updated, only after the execution completes. The statuses supported by activities are: • PENDING/UNKNOWN • SUCCESS • FAILURE
retry	This operation is used for rerunning failed activities. This can be executed with or with out a response file. The response file should be used when the task execution failed due to input value error and the response file has been updated. Retry will: • Check if a response file is provided. If provided the response file is used for creating input data. If the response file is not provided, the utility will get the input data from the previous or failed run. • Automatically determine the current activity name in failure state. • Execute the rollback step for the current failed activity and skip all other successful activities and subtasks. • Execute the activity from the failed step forward.. **Note:** In the status summary RETRY is displayed for the activity that was in a failed state. In verbose summary, the activity status will be the current failed status. Once the execution of the activities completes, the activity status and task status will be updated properly.
mark_as_complete	This operation is used to mark an activity as manually fixed. The user manually fixes the failed activity and then runs this operation. This operation will then skip the current failed activity and mark it as MANUAL_SUCCESS, then resume to next subtask. **Note:** The status summary will show the MANUAL_SUCCESS status for the particular sub task . In verbose status the activity status is not changed. This is because the task or activity is not rerun, therefore the verbose status display the old status.
mark_all_steps_complete	This operation is used to skip all the subtask execution in case of failure. In this case the user can manually fix all pending and failed subtasks. **Note:** The status summary will show the MANUAL_SUCCESS status for the particular subtask . In verbose status the activity status will be the current status [in FAILED / PENDING/SUCCESS state]. Since the subtask or activity is not rerun, the verbose status displays the old status.

Subtasks for PeopleTools Upgrade [PTU] in Cloud Manager Instance

The **cm_upgrade** task is used to perform a PeopleTools Upgrade [PTU] in Cloud Manager instance. The input values should given as response file. This task will upgrade PeopleTools on the Cloud Manager instance with no manual stop.

The following sub tasks are performed.

1. Validate the Cloud Manager PTU response file input values.

   The validation activity (PsftCMUpdateValidationActivity) will validate:

   - WinRm connectivity to the Windows client instance
   - Windows client user id and password
   - File server validation
   - Current PeopleTools version
   - PeopleTools DPK for the new PeopleTools version
   - Database information in TNS entry
   - PIA port - http and https
   - psftserver values and jolt port in wls config
   - WLS port and Jolt port in Application domain
   - Operator id/password
   - WLS admin is/password
   - Web profile user id/password
   - DB admin password
   - Operator id and password
   - Connect id and password
   - Access id and password
   - All user input mandatory values

2. Take a backup of current CM_PS_HOME and PS_CFG_HOME.

   The activity to prepare for the update (PsftPrepareCMUpdateActivity) will:

   - Backup of PS_HOME and PS_CFG_HOME
   - Back up of PTU specific files.
   - Copy the PTC and ODC DPK from CM DPKs to the file server.

3. Stop the Cloud Manager psft domains.

   The activity to shut down PSFT domains (PsftCMDomainRestartActivity) will execute.

4. Cloud Manager PTU upgrade process.

   This subtask contains multiple activities:

- Copy the Cloud folder from Cloud Manager file server to Windows client.
- Install the PeopleTools client for current CM PeopleTools version.
- Install the PeopleTools client for new CM PeopleTools version.
- Configuration Change Assistant for CM PeopleTools Upgrade process.
- Trigger the Change Assistant PTU command line process.

5. Cloud Manager PTP update process.

   This subtask contains multiple activities:

   - Copy the Cloud folder from Cloud Manager file server to Windows client.
   - Install the PeopleTools client for new CM PeopleTools version.
   - Configuration Change Assistant for CM PeopleTools Update process.
   - Trigger the Change Assistant PTP command line process.

6. Uninstall the Cloud Manager middle tier.

   The activity to uninstall the middle tier will:

   - Uninstall middle tier from the Cloud Manager instance.
   - Call the puppet clean up command using the root user.

7. Re-provision the Cloud Manager middle tier.

   This subtask contains multiple activities:

   - Provision middle tier:
     - Installation of new PeopleTools middle tier in the Cloud Manager middle tier.
     - Restore old configuration files in Cloud Manager.
     - Restore log4j, open ssl, puppet config and execution scripts.
     - Will do Cloud Manager specific configuration in Cloud Manager puppet yaml file and will trigger the Cloud Manager specific puppet profiles.
     - Use puppet apply execution using root user for recreating the middle tier.
   - Place holder for doing the post MT creation steps, if any.

8. Cloud Manager PTU post update settings.

   The activity for PTU post update settings will:

- Post the upgrade task.
- Execute the application engine program for notifying the UI about the execution status.

9. Restarting the Cloud Manager domains.

   The activity will restart all Cloud Manager psft domains.

Creating Response File

Create a json file that includes all the mandatory values, the other values will be discovered in job execution. If the mandatory values are not included in the response file, job execution will throw an error.

This is an example of the response file containing the mandatory values:

```
{
  "pum_source": {
    "windows_client": {
      "private_ip": "<windows_client private IP>",
      "remote_password": "<Windows Client Password>"
    }
  },
  "pum_target": {
    "psft": {
      "access_pwd": "<Access Password>",
      "opr_pwd": "<Operator Password>",
      "admin_pwd": "<DB Admin Password>",
      "connect_pwd": "<Connect Password>",
      "gw_admin_user_pwd": "<Gateway User Password>",
      "webprofile_user_pwd": "<Web Profile User Password>",
      "weblogic_admin_pwd": "<Webserver Admin Password>"
    }
  }
}
```

The response file can also contain additional values, however the mandatory values must be included.

This is an example of a response file with additional values:

```
{
  "file_server": {
```



```
    "hostname": "anneshfsfs.ad2sub.myworldnet.oraclevcn.com"
  },
  "pum_source": {
    "windows_client": {
      "host_name": "win_client_hostname",
      "private_ip": "10.0.6.244",
      "remote_password": "Psoft123##Psoft123"
    }
  },
  "pum_target": {
    "psft": {
      "opr_id": "CLADM",
      "connect_id": "people",
      "access_id": "SYSADM",
      "weblogic_admin_user": "system",
      "gw_admin_user": "administrator",
      "db_name": "CMPSDB",
      "db_service_name": "CMPSDB",
      "db_host": "aneesh2702.ad2sub.myworldnet.oraclevcn.com",
      "psft_server": "aneesh2702.ad2sub.myworldnet.oraclevcn.com",
      "wsl_port": "7000",
      "jolt_port": "9033",
      "pia_https_port": "8443",
      "pia_http_port": "8000",
      "db_port": "1522",
      "tools_version": "8.56.12",
      "new_tools_version": "8.57.03",
      "pi_number": "8",
      "access_pwd": "EMDBO123",
      "opr_pwd": "CLADM",
      "admin_pwd": "Passw0rd#",
      "connect_pwd": "peop1e",
      "gw_admin_user_pwd": "password",
      "webprofile_user_pwd": "WEBPROFILE_USER_PWD",
      "weblogic_admin_pwd": "WEBSERVER_ADMIN_PWD"
    }
```

```
  }
}
```

Getting Status of PeopleTools Upgrade Job

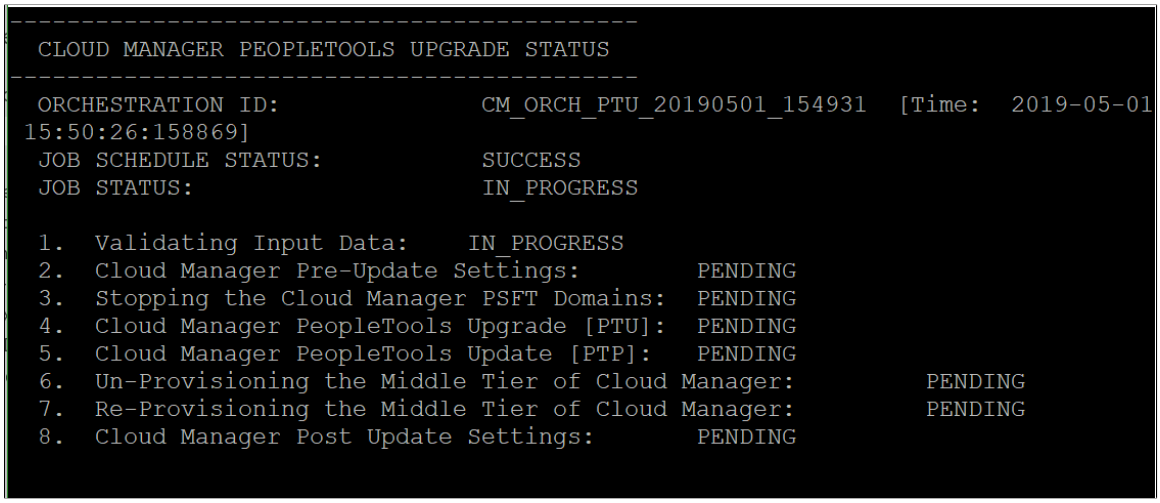
Use the following command to get the current status of the PeopleTools Upgrade:

```
run_cloud_manager_update -t CM_UPGRADE -o get_status
```

When the PeopleTools Upgrade begins, the status will show in progress and you can see what step is executing.

Image: Cloud Manager PeopleTools Upgrade Status showing in-progress.

This example illustrates Cloud Manager PeopleTools Upgrade Status.



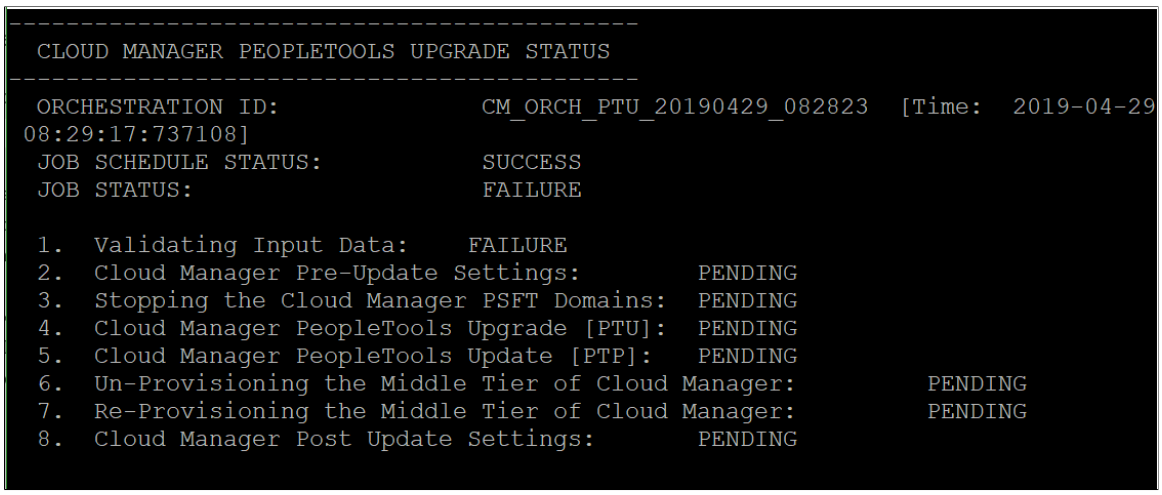
```
-----------------------------------------
 CLOUD MANAGER PEOPLETOOLS UPGRADE STATUS
-----------------------------------------
 ORCHESTRATION ID:             CM_ORCH_PTU_20190501_154931  [Time:  2019-05-01
15:50:26:158869]
 JOB SCHEDULE STATUS:          SUCCESS
 JOB STATUS:                   IN_PROGRESS

 1.  Validating Input Data:    IN_PROGRESS
 2.  Cloud Manager Pre-Update Settings:        PENDING
 3.  Stopping the Cloud Manager PSFT Domains:  PENDING
 4.  Cloud Manager PeopleTools Upgrade [PTU]:  PENDING
 5.  Cloud Manager PeopleTools Update [PTP]:   PENDING
 6.  Un-Provisioning the Middle Tier of Cloud Manager:         PENDING
 7.  Re-Provisioning the Middle Tier of Cloud Manager:         PENDING
 8.  Cloud Manager Post Update Settings:       PENDING
```

If a step fails, the status will show failure. You will need to correct the failure and either retry or mark the step as complete in order to continue.

Image: Cloud Manager PeopleTools Upgrade Status with failed step.

This example illustrates Cloud Manager PeopleTools Upgrade Status where a step has failed.

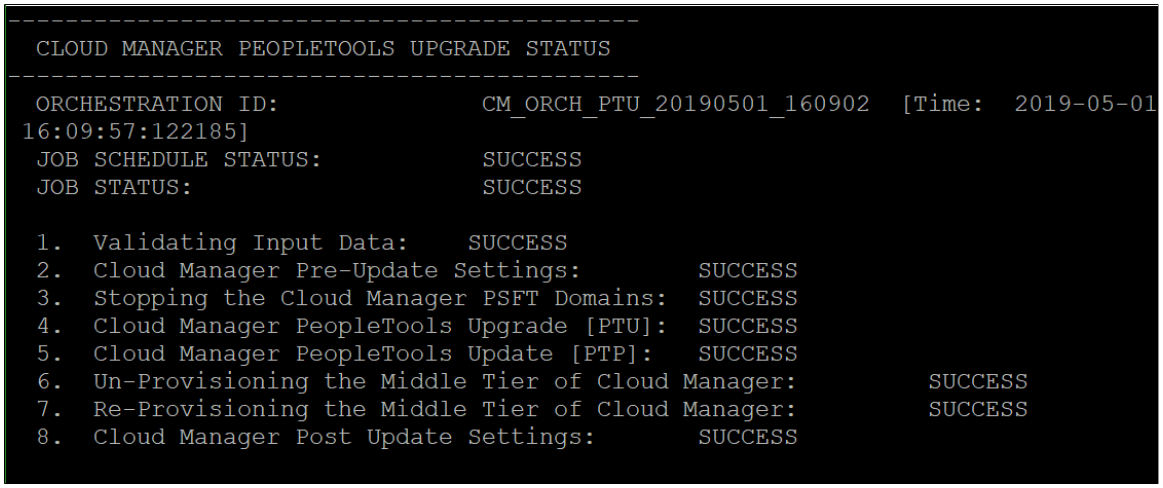


```
-----------------------------------------
 CLOUD MANAGER PEOPLETOOLS UPGRADE STATUS
-----------------------------------------
 ORCHESTRATION ID:             CM_ORCH_PTU_20190429_082823  [Time:  2019-04-29
08:29:17:737108]
 JOB SCHEDULE STATUS:          SUCCESS
 JOB STATUS:                   FAILURE

 1.  Validating Input Data:    FAILURE
 2.  Cloud Manager Pre-Update Settings:        PENDING
 3.  Stopping the Cloud Manager PSFT Domains:  PENDING
 4.  Cloud Manager PeopleTools Upgrade [PTU]:  PENDING
 5.  Cloud Manager PeopleTools Update [PTP]:   PENDING
 6.  Un-Provisioning the Middle Tier of Cloud Manager:         PENDING
 7.  Re-Provisioning the Middle Tier of Cloud Manager:         PENDING
 8.  Cloud Manager Post Update Settings:       PENDING
```


Image: Cloud Manager PeopleTools Upgrade Status

This example illustrates Cloud Manager PeopleTools Upgrade Status where all steps are successful.



Verbose

To display the verbose status, add the -v verbose option:

```
run_cloud_manager_update -t CM_UPGRADE -o get_status -v
```

This is an example of the verbose Cloud Manager PeopleTools Upgrade Status:

```
-------------------------------------------
  CLOUD MANAGER PEOPLETOOLS UPGRADE STATUS
-------------------------------------------
  ORCHESTRATION ID:              CM_ORCH_PTU_20190501_160902  [Time:  2019-05-01 16⇒
:09:57:122185]
  JOB SCHEDULE STATUS:           SUCCESS
  JOB STATUS:                    SUCCESS
  JOB DETAILS:                   Successfully completed
  JOB LOG:                       /home/psadm2/psft/data/cloud/cmlogs/envs/CLOUD_MAN⇒
AGER_INSTANCE/CM_ORCH_PTU_20190501_160902/cm_job_psft_cm_ptu_job_0_20190501_160903_⇒
out.log
  JOB SCHEDULER LOG:             /home/psadm2/psft/data/cloud/cmlogs/envs/CLOUD_MAN⇒
AGER_INSTANCE/CM_ORCH_PTU_20190501_160902/out.log
  JOB STATUS CHECK LOG:          /home/psadm2/psft/data/cloud/cmlogs/envs/CLOUD_MAN⇒
AGER_INSTANCE/CM_DATA/out_20190501.log

  1.  Validating Input Data:    SUCCESS
      TASK DETAILS:              Successfully completed
      TASK LOG:                 /home/psadm2/psft/data/cloud/cmlogs/envs/CLOUD_MANA⇒
GER_INSTANCE/CM_PTU_VALIDATE_0_20190501_160906/out.log
      1.1  CM Update Validation Process:        SUCCESS
           Details: Successfully completed

  2.  Cloud Manager Pre-Update Settings:        SUCCESS
      TASK DETAILS:              Successfully completed
      TASK LOG:                 /home/psadm2/psft/data/cloud/cmlogs/envs/CLOUD_MANA⇒
GER_INSTANCE/CM_PRE_UPDATE_0_20190501_160912/out.log
      2.1  Cloud Manager Prepare Update Process:        SUCCESS
           Details: Successfully completed

  3.  Stopping the Cloud Manager PSFT Domains:  SUCCESS
      TASK DETAILS:              Successfully completed
      TASK LOG:                 /home/psadm2/psft/data/cloud/cmlogs/envs/CLOUD_MANA⇒
GER_INSTANCE/CM_DOMAIN_STOP_0_20190501_160918/out.log
      3.1  CM Domain Restart/Stop Process:      SUCCESS
```



```
            Details: Successfully completed

  4.  Cloud Manager PeopleTools Upgrade [PTU]:  SUCCESS
      TASK DETAILS:              Successfully completed
      TASK LOG:                 /home/psadm2/psft/data/cloud/cmlogs/envs/CLOUD_MANA⇒
GER_INSTANCE/CM_PTU_UPGRADE_0_20190501_160924/out.log
      4.1  Performing PsftActivityWindowsCloudFolderSync:       SUCCESS
            Details: Successfully completed

      4.2  Performing Cloud Manager Windows Client Install Activity [Source PeopleT⇒
ools]:       SUCCESS
            Details: Successfully completed

      4.3  Performing Windows Client Install Activity:  SUCCESS
            Details: Successfully completed

      4.4  Adding Environment Info to CA:       SUCCESS
            Details: Successfully completed

      4.5  CA PTU Apply Process:        SUCCESS
            Details: Successfully completed

  5.  Cloud Manager PeopleTools Update [PTP]:   SUCCESS
      TASK DETAILS:              Successfully completed
      TASK LOG:                 /home/psadm2/psft/data/cloud/cmlogs/envs/CLOUD_MANA⇒
GER_INSTANCE/CM_PTP_UPDATE_0_20190501_160930/out.log
      5.1  Performing PsftActivityWindowsCloudFolderSync:       SUCCESS
            Details: Successfully completed

      5.2  Performing Windows Client Install Activity:  SUCCESS
            Details: Successfully completed

      5.3  Adding Environment Info to CA:       SUCCESS
            Details: Successfully completed

      5.4  CA PTP Apply Process:        SUCCESS
            Details: Successfully completed

  6.  Un-Provisioning the Middle Tier of Cloud Manager:         SUCCESS
      TASK DETAILS:              Successfully completed
      TASK LOG:                 /home/psadm2/psft/data/cloud/cmlogs/envs/CLOUD_MANA⇒
GER_INSTANCE/CM_UNPROV_MT_0_20190501_160936/out.log
      6.1  Performing Unprovision MT:   SUCCESS
            Details: Successfully completed

  7.  Re-Provisioning the Middle Tier of Cloud Manager:         SUCCESS
      TASK DETAILS:              Successfully completed
      TASK LOG:                 /home/psadm2/psft/data/cloud/cmlogs/envs/CLOUD_MANA⇒
GER_INSTANCE/CM_REPROV_MT_0_20190501_160942/out.log
      7.1  Performing Reprovision MT:   SUCCESS
            Details: Successfully completed

      7.2  Cloud Manager Post MT Reprovision Process:   SUCCESS
            Details: Successfully completed

  8.  Cloud Manager Post Update Settings:       SUCCESS
      TASK DETAILS:              Successfully completed
      TASK LOG:                 /home/psadm2/psft/data/cloud/cmlogs/envs/CLOUD_MANA⇒
GER_INSTANCE/CM_POST_UPDATE_0_20190501_160948/out.log
      8.1  Cloud Manager Post Update Process:   SUCCESS
            Details: Successfully completed
```

Troubleshooting PeopleTools Upgrade Failures

Several logs are available to assist the users in troubleshooting errors that may occur during the upgrade process.

Log	*Location/Example log file name*
JOB LOG	/home/psadm2/psft/data/cloud/cmlogs/envs/CLOUD_MANAGER_INSTANCE/CM_ORCH_PTU_20190308_054432/cm_job_psft_cm_ptu_job_0_20190308_054432_out.log
JOB SCHEDULER LOG	/home/psadm2/psft/data/cloud/cmlogs/envs/CLOUD_MANAGER_INSTANCE/CM_ORCH_PTU_20190308_054432/out.log
JOB STATUS CHECK LOG	/home/psadm2/psft/data/cloud/cmlogs/envs/CLOUD_MANAGER_INSTANCE/CM_ORCH_PTU_20190308_054607/out.log
TASK LOG	/home/psadm2/psft/data/cloud/cmlogs/envs/CLOUD_MANAGER_INSTANCE/CM_POST_UPDATE_0_20190308_054441/out.log

Note: The log file names are only examples, the file name in a customer environment will vary.

Chapter 11

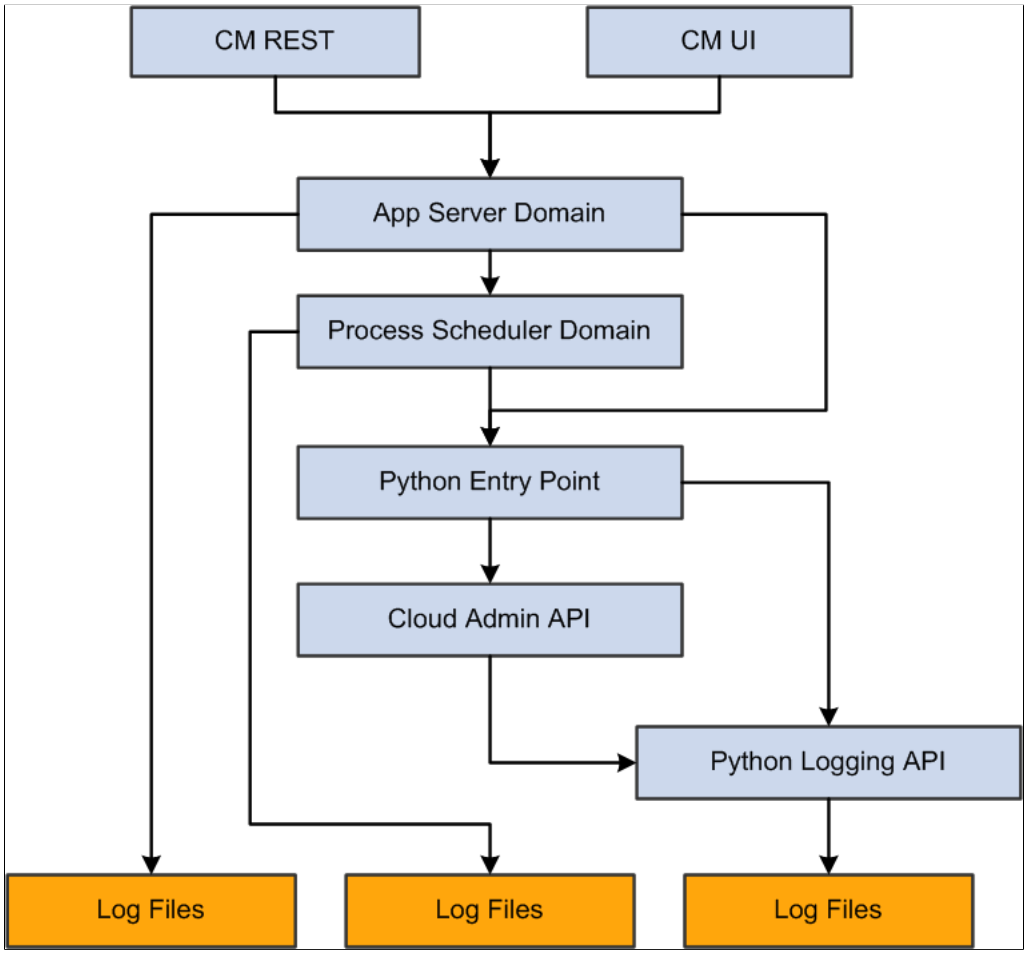
Cloud Manager Logs

Understanding PeopleSoft Cloud Manager Logs

Logs contain useful information for analyzing any environment related issues or failures that may occur in the system.

Image: Logging Process Overview in Cloud Manager

The flow diagram below illustrates an overview of logging process in Cloud Manager.



Cloud Manager logs include:

- Python logs
- Environment Action logs
- Download Manager logs

- Patching logs
- App Server Domain logs
- Process Scheduler Domain logs
- Puppet logs in Provisioned VMs
- Terraform logs

Describing Cloud Manager Logs

Python Logs

- All Python environment action logs will be under the following folder:<CM Python Log Root>/envs/
- All logs related to a particular environment <env name> will be under: <CM Python Log Root>/envs/<env name>/.The path of <CM Python Log Root> is /home/psadm2/psft/data/cloud/cmlogs.
- All logs related to the action <Type> on the environment denoted by <env name> will be under: <CM Python Log Root>/envs/<env name>/<Type>_TimeStamp
- The actions can be:
  - CREATE
  - DEPLOY (Only for OCI)
  - REMOVE
  - ACTIONS (Start, Stop, and so on)
  - ADD_TARGET
  - UPGRADE
  - BACKUP
  - RESTORE
  - CLONE
  - REFRESH

Download Manger Logs

Log files generated by the download manager are available in the following folder: <CM Python Log Root>/dm/

Note: A contextual logs UI that can be accessed from the environment details page is available in Cloud Manager for administrator and end users while debugging issues in their environments.

Since the number of folders and files under cmlogs will grow over time, an archiving process for older files is included in Cloud Manager.

Note: When the user deletes an environment, the log files are automatically moved to an archive directory, for example: CM Python Log Root>/envs/archive_dir

Cloud Manager Patching Logs

Log files generated by the Cloud Manager patch process are available as shown in this table.

Description	*Path*
Detailed log about the process to download Cloud Manager update patches.	/opt/oracle/psft/home/psadm2/psft/data/cloud/ocihome/cmpatch/logs/output.log
Detailed log about the process to apply Cloud Manager update patches.	/opt/oracle/psft/home/psadm2/psft/data/cloud/ocihome/cmpatch/logs/cmpatch_apply.log
Other database project log files, depending upon the patch	/opt/oracle/psft/home/psadm2/psft/data/cloud/ocihome/cmpatch/logs/

Application Server Domain Logs

Application Server Domain logs are written in the default application server domain logs directory. $PS_CFG_HOME/appserv/APPDOM/LOGS

Puppet Logs in Provisioned VMs

To locate puppet logs on Linux VM:

1. Logon into the provisioned VM using "opc" account with ssh.

   Use the private key corresponding to the public key provided in the My Settings page, or use the Cloud Manager administrative key available in the Cloud Manager VM. See My Settings Page

2. The log files can be found at: /home/opc/cloud/admin/scripts/cloud_setup_psft.log.

To locate puppet logs on Windows VM:

1. Log into Windows VM as administrator.
2. The log files can be found at: C:\cloud_setup_psft.txt.

PeopleSoft Cloud Manager Log Levels

The log levels that can be configured by the customer are:

- Critical
- Error
- Warning
- Debug

Note: Logging formats and levels are controlled using Python Logging configuration. The default log level is Debug.

Attribute name	*Format*	*Description*
asctime	%(asctime)s	Human-readable time when the LogRecord was created. By default this is of the form ‘2003-07-08 16:49:45,896’ (the numbers after the comma are millisecond portion of the time).
created	%(created)f	Time when the LogRecord was created (as returned by time.time()).
filename	%(filename)s	Filename portion of pathname.
funcName	%(funcName)s	Name of function containing the logging call.
levelname	%(levelname)s	Text logging level for the message ('DEBUG', 'INFO', 'WARNING', 'ERROR', 'CRITICAL').
levelno	%(levelno)s	Numeric logging level for the message (DEBUG, INFO, WARNING, ERROR, CRITICAL).
lineno	%(lineno)d	Source line number where the logging call was issued (if available).
message	%(message)s	The logged message, computed as msg % args. This is set when Formatter. format() is invoked.
module	%(module)s	Module (name portion of filename).
msecs	%(msecs)d	Millisecond portion of the time when the LogRecord was created.
name	%(name)s	Name of the logger used to log the call.
pathname	%(pathname)s	Full pathname of the source file where the logging call was issued (if available).
process	%(process)d	Process ID (if available).
processName	%(processName)s	Process name (if available).
relativeCreated	%(relativeCreated)d	Time in milliseconds when the LogRecord was created, relative to the time the logging module was loaded.
thread	%(thread)d	Thread ID (if available).
threadName	%(threadName)s	Thread name (if available).

Configurable Log Root: /home/psadm2/psft/data/cloud/cmlogs will be the Cloud Manager Python Log Root.

Changing Log Levels

The customer can edit psc_constants.py and pca_int.conf files to set the log level.

The default logging level is *Debug*. To customize it to another level, modify the following entry in the file:

```
<PS_APP_HOME>\cloud\psc_cloud\psc_utils\psc_constants.py logging_level = logging.DE⇒
BUG
```

Note: You do not need to restart the domains after the changing the log levels.

Important! In OCI, for Python logging configuration, two locations have to be configured.
cloud/pca_int.conf - This controls the log level in Download Manager and Terraform handler.
cloud/psc_cloud/psc_utils/psc_constants.py - This controls the log level in PSFT deployment code.

Terraform Logs for OCI

When Cloud Manager is used for provisioning environments, the provisioning of infrastructure is the first task that is executed. The Terraform log files generated during the execution can be found under the logs directory for the environment: /home/psadm2/psft/data/cloud/cmlogs/envs/<Environemnt Name>/CREATE_<Time Stamp>/

Log File Type	Description
tf.out	This is the Output Log, which contains the Terraform's stdout stream output.
tf.err	This is the Error Log, which contains the Terraform's stderr stream output.
out.log	This is the Driver Output generated by the Cloud Manager module that invokes Terraform.
console.log	This contains the uncaught exceptions.

Terraform Input and Output Files

The Terraform input/output files used by Cloud Manager for provisioning an environment can be found under: /home/psadm2/psft/data/cloud/ocihome/envs/<Environment Name>/

Log File Type	Description
terraform.tf.json	The .json file contains the specification of the VMs, storage volumes, database systems etc.
variables.tf	This file contains the tenancy OCID, user OCID, API key paths, finger print etc.
tf.result.json	This file contains a summary of the resources that were successfully created by Terraform.

Chapter 12

Backing Up and Restoring Cloud Manager

Understanding Cloud Manager Backup and Restore

There are two methods for backing up and restoring Cloud Manager.

1. Automated Backup and Restore Utility.

   See Using Automated Backup and Restore Utility.

2. Backup and restore using Block Volume Backups for OCI.

   See Manually Backing Up and Restoring Cloud Manager Using Block Volume Backups for OCI

Important! If your Cloud Manager instance was created using a custom fqdn, the PRESERVE_HOSTINFO field must be set to 0 before doing CM backup. If this value is not set as 0, there is a chance that the Cloud Manager restore will fail as OCI will not be able to configure the new instance with new IP details in /etc/hosts file. See tutorial *Install the PeopleSoft Cloud Manager Stack with Resource Manager*.

Warning! Backing up or restoring Cloud Manager will shutdown all services. Please ensure that no provisioning or lifecycle jobs are running. Any running jobs will be abruptly ended and may result in an unstable or unusable state.

Important! Ensure the process scheduler does not have any jobs in its queue. If there are pending jobs in the queue, those may get scheduled to run whenever a backup is restored.

Using Automated Backup and Restore Utility

The automated backup and restore utility provides the ability to create a backup of the Cloud Manager instance. This backup/restore utility provides the following options:

- Backup and restore Cloud Manager Instance block volume.
- Backup Cloud Manager Instance boot volume.
- Delete backups.
- List Cloud Manager backups in OCI.
- Create an OCI config file.

To run the automated backup and restore utility:

1. Log into Cloud Manager instance using SSH as user opc.
2. Change the directory to */home/opc/bootstrap/cm_backup_and_restore*.
3. Copy 2 files (cm_backup_restore.py and cm_backup_restore.sh) from */opt/oracle/psft/pt/ps_app_home/cloud/psc_cloud/psc_utils/* to */home/opc/bootstrap/cm_backup_and_restore*.
4. Run the shell script **cm_backup_restore.sh**.

Understanding the Backup and Restore Shell Script

For a summary of the usage and optional arguments for shell script **cm_backup_restore.sh**, use the -h option.

This is an example of the help.

Image: Example: cm_backup_restore.sh -h

This example illustrates running cm_backup_restore.sh -h.

```
[opc@smncm12r1 cm_backup_and_restore]$ sh cm_backup_restore.sh -h
usage: cm_backup_restore.py [-h] -o option [-n backupname] [-t {BLOCK,BOOT}]
                            [-c DB_ACCESS_ID DB_ACCESS_PWD PDB_NAME]

Utility to Backup/Restore storage volume of Cloud Manager Instance

optional arguments:
  -h, --help            show this help message and exit
  -o option             Provide an option to Backup/Restore/Delete/Display

                        backup       (for taking backup of the Cloud Manager Instance)
                        restore      (for restoring block volume of Cloud Manager Instance)
                        delete       (for deleting backup from OCI)
                        list         (to display list of Cloud Manager Instance backups in OCI)
                        createconfig (to create oci config file)

  -n backupname         Custom Backup Name [Optional]
                        Default format:'<Vol Type>_VOLBKP_<CM Instance Name><timestamp(ddmmyyyy)>_<timestamp(HHMMSS)>'
                        (this field is mandatory for Restore and Delete operations)

  -t {BLOCK,BOOT}       Backup Volume Type [Optional]
                        Default : BLOCK
                        (this field is required for Backup operation)

  -c DB_ACCESS_ID DB_ACCESS_PWD PDB_NAME
                        Provide Database Access Id, Password and PDB Name
                        Example <DB_ACCESS_ID> <DB_ACCESS_PWD> <PDB_NAME> (separated by space)
```

Creating Config File

You need to create a config file if:

- This is the first time you are running the automated backup and restore utility.
- You want to run the utility with different OCI user credentials.

To create the Config file:

1. Run the utility with the createconfig option and provide the Cloud Manager database Access ID and password.

   ```
   sh cm_backup_restore.sh -o createconfig -c <DB_ACCESS_ID> <DB_ACCESS_PWD> <PDB⇒
   _NAME>
   ```

2. This option will read OCI User ID, Tenancy ID, Fingerprint and Private Key File Path from database and display on screen.
3. Check the displayed values.

- If the values are correct, press *y* to confirm and the configuration file will be created.
- If you want to change the values, press *n* and provide Tenancy ID, User ID, Fingerprint, Private Key File Path, Region details to create config file.

Image: Example accepting default values

This example illustrates accepting default values.

```
[opc@smncm12r1 cm_backup_and_restore]$ sh cm_backup_restore.sh -o createconfig -c EMDBO Water123 CMPSDB
Please check whether below OCI details are correct

Tenancy OCID : 'ocid1.tenancy.oc1..aaaaaaaayy35pigzces6ly7aslibgt7a4u7o3tlt42nxg4idzrsui52gma5a'
User OCID: 'ocid1.user.oc1..aaaaaaaaprdpimfzdhyip3tmeot5ve7woycqanjj7juz3gqccc5qawu7dora'
Fingerprint of Public Key : '49:4f:45:64:2a:1c:d1:11:2f:61:6a:09:95:97:b4:74'
Private Key Path : '/home/psadm2/psft/data/cloud/ocihome/keys/oci_api_key.pem'
Region : 'us-ashburn-1'

 Enter y if above values are correct : y
2021-02-10 13:35:06 -     INFO -  406 : Created config file 'config.json'
[opc@smncm12r1 cm_backup_and_restore]$
```

Image: Example modifying default values

This example illustrates modifying default values.

```
[opc@smncm12r1 cm_backup_and_restore]$ sh cm_backup_restore.sh -o createconfig -c EMDBO Water123 CMPSDB
Please check whether below OCI details are correct

Tenancy OCID : 'ocid1.tenancy.oc1..aaaaaaaayy35pigzces6ly7aslibgt7a4u7o3tlt42nxg4idzrsui52gma5a'
User OCID: 'ocid1.user.oc1..aaaaaaaaprdpimfzdhyip3tmeot5ve7woycqanjj7juz3gqccc5qawu7dora'
Fingerprint of Public Key : '49:4f:45:64:2a:1c:d1:11:2f:61:6a:09:95:97:b4:74'
Private Key Path : '/home/psadm2/psft/data/cloud/ocihome/keys/oci_api_key.pem'
Region : 'us-ashburn-1'

 Enter y if above values are correct : n
Enter Tenancy OCID : ocid1.tenancy.oc1..aaaaaaaayy35pigzces6ly7aslibgt7a4u7o3tlt42nxg4idzrsui52gma5a
Enter User OCID : ocid1.user.oc1..aaaaaaaaprdpimfzdhyip3tmeot5ve7woycqanjj7juz3gqccc5qawu7dora
Enter Fingerprint of Public Key : 49:4f:45:64:2a:1c:d1:11:2f:61:6a:09:95:97:b4:74
Enter region : us-ashburn-1
Enter Private Key File Path : /home/psadm2/psft/data/cloud/ocihome/keys/oci_api_key.pem
2021-02-10 13:37:00 -     INFO -  406 : Created config file 'config.json'
[opc@smncm12r1 cm_backup_and_restore]$
```

Note: If config.json is already present, this utility will replace the existing one.

Creating Backups

When creating a backup of Cloud Manager, backup both block (data) volume and the boot volume. This will ensure creating a pair of time consistent backups that can be restored together when restoring the entire Cloud Manager instance in case of boot volume issues or failures.

Backups can be created using the default name which is *<Vol Type>_VOLBKP_<CM Instance Name>_<timestamp(ddmmyyyy)>_<timestamp(HHMMSS)>* or you can provide a custom name for the backup. Use the optional argument *-n <Custom Backup Name>* to create a backup with a custom name.

The default backup type is BLOCK.

Cloud Manager data is saved in two locations: Oracle Database files on data volume and configuration files on boot volume. Both must be backed-up to restore to a consistent point. The backup utility creates a full backup of both data volume as well as files on boot volume automatically.

Creating the Block Volume Backup

To create the block volume backup:

1. Run the utility with the backup option.

   ```
   sh cm_backup_restore.sh -o backup
   ```

   Note: Default value for volume type (-t) is BLOCK.

2. Optional arguments include name (-n) and volume type (-t).

   ```
   sh cm_backup_restore.sh -o backup -n SMNCM_CST_BKP_BLK
   ```

   In the above example the backup name is SMNCM_CST_BKP_BLK.

3. User will be prompted that the backup task will stop Database, Application Server, Process Scheduler and PIA services. Press *y* to continue.

4. User will be prompted to enter a passphrase for the private API signing key.

   Enter the passphrase if it exists or press enter.

5. The backup automation process will:

   - Shut down the database and domains.
   - Backup files on boot volume and save them on data volume as /opt/oracle/psft/dpks/cm_boot_vol_files.tar.gz. Files backed up include:
     - All files under PS_CFG_HOME
     - /home/psadm1/.bashrc
     - /home/psadm2/.bashrc
     - /home/psadm3/.bashrc
     - /home/oracle2/.bashrc
     - /home/esadm1/.bashrc
     - /etc/profile
     - /etc/bashrc
     - /usr/lib/systemd/system/psft-db-<DB_NAME>.service
     - /usr/lib/systemd/system/psft-appserver-APPDOM.service
     - /usr/lib/systemd/system/psft-prcs-PRCSDOM.service
     - /usr/lib/systemd/system/psft-pia-peoplesoft.service
   - Create a backup of data volume.
   - Restart the database and domains.

Example:

```
[opc@smncm cm_backup_and_restore]$ sh cm_backup_restore.sh -o backup
```

```
Backup task will stop Database, Application Server, Process Scheduler and PIA servi⇒
ces
Do you want to continue (y/n) ? y
Please Enter Private Key Pass Phrase :
2019-04-19 08:36:22 -     INFO -  408 : Compressing BOOT volume directories/files '⇒
/home/psadm1/.bashrc,/home/psadm2/.bashrc,/home/psadm3/.bashrc,/home/oracle2/.bashr⇒
c,/home/esadm1/.bashrc,/etc/profile,/etc/bashrc,/etc/init.d/psft-db,/etc/init.d/psf⇒
t-appserver,/etc/init.d/psft-prcs,/etc/init.d/psft-pia' and moving to '/opt/oracle/⇒
psft/dpks/cm_boot_vol_files.tar.gz'
2019-04-19 08:36:22 -     INFO -  418 : $PS_CFG_HOME directory '/home/psadm2/psft/p⇒
t/8.57'
2019-04-19 08:36:22 -     INFO -  427 : Compressed BOOT volume directories/files '/⇒
home/psadm1/.bashrc,/home/psadm2/.bashrc,/home/psadm3/.bashrc,/home/oracle2/.bashrc⇒
,/home/esadm1/.bashrc,/etc/profile,/etc/bashrc,/etc/init.d/psft-db,/etc/init.d/psft⇒
-appserver,/etc/init.d/psft-prcs,/etc/init.d/psft-pia,/home/psadm2/psft/pt/8.57' an⇒
d moving to '/opt/oracle/psft/dpks/cm_boot_vol_files.tar.gz'
2019-04-19 08:37:00 -     INFO -  598 : Cloud Manager Instance Backup Volume Id :oc⇒
id1.volume.oc1.iad.xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
2019-04-19 08:37:00 -     INFO -  448 : Changing DB service state to 'Stop'
2019-04-19 08:37:27 -     INFO -  481 : DB service is in 'Stop' state
2019-04-19 08:37:27 -     INFO -  448 : Changing APPSERVER service state to 'Stop'
2019-04-19 08:37:43 -     INFO -  481 : APPSERVER service is in 'Stop' state
2019-04-19 08:37:43 -     INFO -  448 : Changing PRCS service state to 'Stop'
2019-04-19 08:42:35 -     INFO -  481 : PRCS service is in 'Stop' state
2019-04-19 08:42:35 -     INFO -  448 : Changing PIA service state to 'Stop'
2019-04-19 08:42:54 -     INFO -  481 : PIA service is in 'Stop' state
2019-04-19 08:42:54 -     INFO -  875 : Created input.json for BLOCK Volume Backup ⇒
: BLOCK_VOLBKP_SMNCM_20190419_084254
2019-04-19 08:42:54 -     INFO -  876 : Creating BLOCK Volume Backup : BLOCK_VOLBKP⇒
_SMNCM_20190419_084254
2019-04-19 08:44:15 -     INFO -  897 : Created BLOCK volume backup 'BLOCK_VOLBKP_S⇒
MNCM_20190419_084254'
2019-04-19 08:44:15 -     INFO -  448 : Changing DB service state to 'Start'
2019-04-19 08:44:24 -     INFO -  481 : DB service is in 'Start' state
2019-04-19 08:44:24 -     INFO -  448 : Changing APPSERVER service state to 'Start'
2019-04-19 08:44:49 -     INFO -  481 : APPSERVER service is in 'Start' state
2019-04-19 08:44:49 -     INFO -  448 : Changing PRCS service state to 'Start'
2019-04-19 08:46:45 -     INFO -  481 : PRCS service is in 'Start' state
2019-04-19 08:46:45 -     INFO -  448 : Changing PIA service state to 'Start'
2019-04-19 08:46:46 -     INFO -  481 : PIA service is in 'Start' state
```

Creating Boot Volume Backup

Boot volume backups must be restored manually using OCI console. This backup can be used if the CM instance becomes unusable and inaccessible.

Note: When restoring a boot volume backup ensure to create the Cloud Manager instance with the same IP addresses as the original instance. The original instance must be terminated before creating a new instance. If unable to reuse the same IP address, then all references to old IP addresses in Cloud Manager application and domains must be manually updated to reflect the new IP address of the instance.

Warning! If the backup is not restored correctly, the Cloud Manager instance may not come up with the proper network configuration which could result in losing the ability to manage already provisioned environments.

To create a boot volume backup:

1. Run the utility with the backup option.

   ```
   sh cm_backup_restore.sh -o backup -t BOOT
   ```


2. Optionally you can provide a custom backup name using the -n argument..

   ```
   sh cm_backup_restore.sh -o backup -n CUSTOM_NAME -t BOOT
   ```

   In the above example the backup name is CUSTOM_NAME.

3. User will be prompted that the backup task will stop Database, Application Server, Process Scheduler and PIA services. Press *y* to continue.

4. User will be prompted to enter a passphrase for the private API signing key.

   Enter the passphrase if it exists or press enter.

5. The backup process will:

   - Shut down the database and domains.
   - Create the backup.
   - Restart the database and domains.

Example:

```
[opc@smncm cm_backup_and_restore]$ sh cm_backup_restore.sh -o backup -t BOOT
Backup task will stop Database, Application Server, Process Scheduler and PIA servi⇒
ces
Do you want to continue (y/n) ? y
Please Enter Private Key Pass Phrase :
2019-04-19 09:58:54 -     INFO -  598 : Cloud Manager Instance Backup Volume Id :oc⇒
id1.bootvolume.oc1.iad.abuwcljrhcuapoaveqp2yf2oof2pc6lsurxx4xu2fmjarjjrz4qyfkif3wpq
2019-04-19 09:58:54 -     INFO -  448 : Changing DB service state to 'Stop'
2019-04-19 09:59:14 -     INFO -  481 : DB service is in 'Stop' state
2019-04-19 09:59:14 -     INFO -  448 : Changing APPSERVER service state to 'Stop'
2019-04-19 09:59:30 -     INFO -  481 : APPSERVER service is in 'Stop' state
2019-04-19 09:59:30 -     INFO -  448 : Changing PRCS service state to 'Stop'
2019-04-19 10:04:33 -     INFO -  481 : PRCS service is in 'Stop' state
2019-04-19 10:04:33 -     INFO -  448 : Changing PIA service state to 'Stop'
2019-04-19 10:07:35 -     INFO -  481 : PIA service is in 'Stop' state
2019-04-19 10:07:35 -     INFO -  875 : Created input.json for BOOT Volume Backup :⇒
 BOOT_VOLBKP_SMNCM_20190419_100735
2019-04-19 10:07:35 -     INFO -  876 : Creating BOOT Volume Backup : BOOT_VOLBKP_S⇒
MNCM_20190419_100735
2019-04-19 10:09:17 -     INFO -  897 : Created BOOT volume backup 'BOOT_VOLBKP_SMN⇒
CM_20190419_100735'
2019-04-19 10:09:17 -     INFO -  448 : Changing DB service state to 'Start'
2019-04-19 10:09:26 -     INFO -  481 : DB service is in 'Start' state
2019-04-19 10:09:26 -     INFO -  448 : Changing APPSERVER service state to 'Start'
2019-04-19 10:09:51 -     INFO -  481 : APPSERVER service is in 'Start' state
2019-04-19 10:09:51 -     INFO -  448 : Changing PRCS service state to 'Start'
2019-04-19 10:11:47 -     INFO -  481 : PRCS service is in 'Start' state
2019-04-19 10:11:47 -     INFO -  448 : Changing PIA service state to 'Start'
2019-04-19 10:11:47 -     INFO -  481 : PIA service is in 'Start' state
```

Listing Existing Backups

To list existing block and boot volume backups:

1. Run the utility with the list option:

   ```
   sh cm_backup_restore.sh -o list
   ```

2. User will be prompted to enter a passphrase for the private API signing key.

   Enter the passphrase if it exists or press enter.

3. The list of backups is displayed.

Example:

```
[opc@smncm cm_backup_and_restore]$ sh cm_backup_restore.sh -o list
Please Enter Private Key Pass Phrase :
  BLOCK volume backup list :
   * BLOCK_VOLBKP_SMNCM_20190410_110419
  BOOT volume backup list :
   No BOOT volume backups found
```

Restoring from a Backup

Both data volume and a set of files on boot volume must be replaced from a backup to restore Cloud Manager instance to a certain back up point.

First step is to restore the data volume. To restore a block (data) volume backup the user must provide a backup name. User can list the existing backups and then select the backup to restore.

To restore a block (data) volume backup:

1. While you are still on the latest version, before restoring the data volume, generate the list of IP addresses of all managed instances provisioned by Cloud Manager. This is required later in the restore process to synchronize the '/cm_psft_dpks/cloud' directory to all managed nodes in case the files are not up-to-date. This step is required whenever restoring from a latest Cloud Manager version to an older version. For example, restoring back from Cloud Manager Image 10 to Cloud Manager Image 9.

   - SSH to Cloud Manager
   - Switch user to psadm2

     ```
     $ sudo su – psadm2
     ```

   - Change directory to PS_APP_HOME/cloud

     ```
     $ cd /opt/oracle/psft/pt/ps_app_home/cloud
     ```

   - Generate the list of IP addresses into file /home/psadm2/managedenvironments.txt

     ```
     $ get_managed_envs.sh $PS_CFG_HOME
     ```

   - Take backup of /home/psadm2/managedenvironments.txt

     ```
     $ cp /home/psadm2/managedenvironments.txt  <backup_path>
     ```

2. Run the utility with the restore option.

   ```
   sh cm_backup_restore.sh -o restore -n <backup_name>
   ```

3. User will be warned with a message that backup automation will stop Database, Application Server, Process Scheduler and PIA services. Press *y* to continue.

4. User will be prompted to enter a passphrase for the private API signing key.

Enter the passphrase if it exists or press enter.

5. The restore process will:

   - Shut down the database and domains.
   - Restore from the identified volume backup .
   - Restart the database and domains.

   Example:

```
[opc@smncm cm_backup_and_restore]$ sh cm_backup_restore.sh -o restore -n BLOCK⇒
_VOLBKP_SMNCM_20190419_084254
Restore task will stop Database, Application Server, Process Scheduler and PIA⇒
 services
Do you want to continue (y/n) ? y
Please Enter Private Key Pass Phrase :
2019-04-19 09:14:20 -     INFO -  658 : Getting BLOCK volume backup 'BLOCK_VOL⇒
BKP_SMNCM_20190419_084254' details from OCI
2019-04-19 09:14:20 -     INFO -  666 : BLOCK volume backup 'BLOCK_VOLBKP_SMNC⇒
M_20190419_084254' Id : 'ocid1.volumebackup.oc1.iad.abuwcljryiuqzxut5ldxtb2hma⇒
xgj5w65ykxukza6ztmz7odk323yiip3r7a'
2019-04-19 09:14:20 -     INFO -  824 : Creating storage volume 'StorageVol_sm⇒
ncm_19APRIL2019_0914' from Backup 'ocid1.volumebackup.oc1.iad.abuwcljryiuqzxut⇒
5ldxtb2hmaxgj5w65ykxukza6ztmz7odk323yiip3r7a'
2019-04-19 09:15:01 -     INFO -  853 : Created storage volume Name:'StorageVo⇒
l_smncm_19APRIL2019_0914',
Id:'ocid1.volume.oc1.iad.abuwcljrf2hcy3ff5mxhbumnldvftljsp5yz66n73wzsxllreleoh⇒
sqe2vcq'
2019-04-19 09:15:01 -     INFO -  598 : Cloud Manager Instance Backup Volume I⇒
d :ocid1.volume.oc1.iad.abuwcljr7k4bq4eqw3nfoyl7vxdsykzyrrthzgrco7jnwiyg5f6zga⇒
ghlmva
2019-04-19 09:15:01 -     INFO -  448 : Changing DB service state to 'Stop'
2019-04-19 09:15:22 -     INFO -  481 : DB service is in 'Stop' state
2019-04-19 09:15:22 -     INFO -  448 : Changing APPSERVER service state to 'S⇒
top'
2019-04-19 09:15:34 -     INFO -  481 : APPSERVER service is in 'Stop' state
2019-04-19 09:15:34 -     INFO -  448 : Changing PRCS service state to 'Stop'
2019-04-19 09:20:41 -     INFO -  481 : PRCS service is in 'Stop' state
2019-04-19 09:20:41 -     INFO -  448 : Changing PIA service state to 'Stop'
2019-04-19 09:20:57 -     INFO -  481 : PIA service is in 'Stop' state
2019-04-19 09:20:57 -     INFO -  497 : Kill some of the running 'psadm' proce⇒
sses
2019-04-19 09:21:02 -     INFO -  530 : Unmounted block volume '/opt/oracle/ps⇒
ft'
2019-04-19 09:21:02 -     INFO -  688 : Running ISCSI command to logout of sto⇒
rage volume iqn.2015-12.com.oracleiaas:22afb62d-a893-4ab4-a8fe-6dd14053c61b
2019-04-19 09:21:02 -     INFO -  698 : Logged out of storage volume iqn.2015-⇒
12.com.oracleiaas:22afb62d-a893-4ab4-a8fe-6dd14053c61b
2019-04-19 09:21:02 -     INFO -  700 : Running ISCSI command to delete storag⇒
e device iqn.2015-12.com.oracleiaas:22afb62d-a893-4ab4-a8fe-6dd14053c61b
2019-04-19 09:21:02 -     INFO -  709 : Deleted storage device iqn.2015-12.com⇒
.oracleiaas:22afb62d-a893-4ab4-a8fe-6dd14053c61b
2019-04-19 09:21:02 -     INFO -  793 : Initiated REST Call to Detach storage ⇒
volume ocid1.volumeattachment.oc1.iad.abuwcljrfnxyjammza3scounohq7qzawelzslmqi⇒
accvef7cm6w7m2wxjxuq
2019-04-19 09:21:23 -     INFO -  802 : Detached storage volume ocid1.volumeat⇒
tachment.oc1.iad.abuwcljrfnxyjammza3scounohq7qzawelzslmqiaccvef7cm6w7m2wxjxuq
2019-04-19 09:21:23 -     INFO -  915 : Attaching storage volume 'ocid1.volume⇒
.oc1.iad.abuwcljrf2hcy3ff5mxhbumnldvftljsp5yz66n73wzsxllreleohsqe2vcq'
2019-04-19 09:21:23 -     INFO -  918 : Creating input.json for attaching bloc⇒
k volume 'ocid1.volume.oc1.iad.abuwcljrf2hcy3ff5mxhbumnldvftljsp5yz66n73wzsxll⇒
```

```
releohsqe2vcq'
2019-04-19 09:21:23 -     INFO -  920 : Created input.json for attaching block⇒
 volume 'ocid1.volume.oc1.iad.abuwcljrf2hcy3ff5mxhbumnldvftljsp5yz66n73wzsxllr⇒
eleohsqe2vcq'
2019-04-19 09:21:23 -     INFO -  928 : Initiated REST Call to attach storage ⇒
volume ocid1.volume.oc1.iad.abuwcljrf2hcy3ff5mxhbumnldvftljsp5yz66n73wzsxllrel⇒
eohsqe2vcq
2019-04-19 09:22:04 -     INFO -  935 : Attached storage volume 'ocid1.volume.⇒
oc1.iad.abuwcljrf2hcy3ff5mxhbumnldvftljsp5yz66n73wzsxllreleohsqe2vcq'
2019-04-19 09:22:04 -     INFO -  598 : Cloud Manager Instance Backup Volume I⇒
d :ocid1.volume.oc1.iad.abuwcljrf2hcy3ff5mxhbumnldvftljsp5yz66n73wzsxllreleohs⇒
qe2vcq
2019-04-19 09:22:04 -     INFO -  718 : Running ISCSI Attach Commands
2019-04-19 09:22:04 -     INFO -  733 : Running ISCSI command to add new node ⇒
iqn.2015-12.com.oracleiaas:f6f08414-d96f-4fd2-a852-69c0208ca8b2
2019-04-19 09:22:04 -     INFO -  739 : Added new node iqn.2015-12.com.oraclei⇒
aas:f6f08414-d96f-4fd2-a852-69c0208ca8b2
2019-04-19 09:22:04 -     INFO -  741 : Running ISCSI command to start node on⇒
 boot iqn.2015-12.com.oracleiaas:f6f08414-d96f-4fd2-a852-69c0208ca8b2
2019-04-19 09:22:04 -     INFO -  747 : Updated node iqn.2015-12.com.oracleiaa⇒
s:f6f08414-d96f-4fd2-a852-69c0208ca8b2 settings to start on boot
2019-04-19 09:22:04 -     INFO -  749 : Running ISCSI command to login to node⇒
 iqn.2015-12.com.oracleiaas:f6f08414-d96f-4fd2-a852-69c0208ca8b2
2019-04-19 09:22:04 -     INFO -  755 : Logged in to node iqn.2015-12.com.orac⇒
leiaas:f6f08414-d96f-4fd2-a852-69c0208ca8b2
2019-04-19 09:22:04 -     INFO -  543 : Mounted block volume '/opt/oracle/psft⇒
'
2019-04-19 09:22:13 -     INFO -  448 : Changing DB service state to 'Start'
2019-04-19 09:22:25 -     INFO -  481 : DB service is in 'Start' state
2019-04-19 09:22:25 -     INFO -  448 : Changing APPSERVER service state to 'S⇒
tart'
2019-04-19 09:22:56 -     INFO -  481 : APPSERVER service is in 'Start' state
2019-04-19 09:22:56 -     INFO -  448 : Changing PRCS service state to 'Start'
2019-04-19 09:24:52 -     INFO -  481 : PRCS service is in 'Start' state
2019-04-19 09:24:52 -     INFO -  448 : Changing PIA service state to 'Start'
2019-04-19 09:24:52 -     INFO -  481 : PIA service is in 'Start' state
2019-04-19 09:24:52 -     INFO -  947 : Getting storage volume name for Id : '⇒
ocid1.volume.oc1.iad.abuwcljr7k4bq4eqw3nfoyl7vxdsykzyrrthzgrco7jnwiyg5f6zgaghl⇒
mva'
2019-04-19 09:24:52 -     INFO -  957 : Storage volume name for Id 'ocid1.volu⇒
me.oc1.iad.abuwcljr7k4bq4eqw3nfoyl7vxdsykzyrrthzgrco7jnwiyg5f6zgaghlmva' is 'S⇒
torageVol_smncm_18APR2019_1044'
2019-04-19 09:24:52 -     INFO - 1061 : Please remove detached volume 'Storage⇒
Vol_smncm_18APR2019_1044' from OCI manually
```

6. Manually restore boot volume files from the backup /opt/oracle/psft/dpks/cm_boot_vol_files.tar.gz

Next restore files on boot volume. To restore, execute following set of commands and set appropriate ownership on restored files.

1. SSH to Cloud Manager instance
2. Switch user to root.

```
$ sudo bash
```

3. Uncompress and extract boot volume files backup that were saved as /opt/oracle/psft/dpks/cm_boot_vol_files.tar.gz to /tmp/CMbkup

```
$ mkdir /tmp/CMbkup
$ cd /tmp/CMbkup
$ tar -xvf /opt/oracle/psft/dpks/cm_boot_vol_files.tar.gz
```


4. Restore PS_CFG_HOME files. The PS_CFG_HOME path varies if the PeopleTools version before backup was different. Ensure to use the right path.

```
$ cp -r  /tmp/CMbkup/home/psadm2/psft/pt/* /home/psadm2/psft/pt/
$ chown -R psadm2:oinstall /home/psadm2/psft/pt/
$ chmod 755 -R /home/psadm2/psft/pt/
```

5. Copy profile files for users psadm1, psadm2, psadm3, oracle2 and esadm1.

```
$ cp /tmp/CMbkup/etc/profile /etc/profile
$ cp /tmp/CMbkup/etc/bashrc /etc/bashrc
$ chown root:root /etc/profile /etc/bashrc
$ chmod 644 /etc/profile /etc/bashrc

$ cp /tmp/CMbkup/home/psadm1/.bashrc /home/psadm1/.bashrc
$ chown psadm1:oinstall /home/psadm1/.bashrc
$ chmod 644 /home/psadm1/.bashrc

$ cp /tmp/CMbkup/home/psadm2/.bashrc /home/psadm2/.bashrc
$ chown psadm2:oinstall /home/psadm2/.bashrc
$ chmod 644 /home/psadm2/.bashrc

$ cp /tmp/CMbkup/home/psadm3/.bashrc /home/psadm3/.bashrc
$ chown psadm3:appinst /home/psadm3/.bashrc
$ chmod 644 /home/psadm3/.bashrc

$ cp /tmp/CMbkup/home/oracle2/.bashrc /home/oracle2/.bashrc
$ chown oracle2:oinstall /home/oracle2/.bashrc
$ chmod 644 /home/oracle2/.bashrc

$ cp /tmp/CMbkup/home/esadm1/.bashrc /home/esadm1/.bashrc
$ chown esadm1:oinstall /home/esadm1/.bashrc
$ chmod 644 /home/esadm1/.bashrc
```

6. Copy init scripts.

```
$ cp /tmp/CMbkup/usr/lib/systemd/system/psft-db-<DB_NAME>.service /usr/lib/sys⇒
temd/system/
$ cp /tmp/CMbkup/usr/lib/systemd/system/psft-appserver-APPDOM.service /usr/lib⇒
/systemd/system/
$ cp /tmp/CMbkup/usr/lib/systemd/system/psft-prcs-PRCSDOM.service /usr/lib/sys⇒
temd/system/
$ cp /tmp/CMbkup/usr/lib/systemd/system/psft-pia-peoplesoft.service /usr/lib/s⇒
ystemd/system/
$ chown root:root /usr/lib/systemd/system/psft-db-<DB_NAME>.service /usr/lib/s⇒
ystemd/system/psft-appserver-APPDOM.service /usr/lib/systemd/system/psft-prcs-⇒
PRCSDOM.service /usr/lib/systemd/system/psft-pia-peoplesoft.service
$ chmod 755 /usr/lib/systemd/system/psft-db-<DB_NAME>.service /usr/lib/systemd⇒
/system/psft-appserver-APPDOM.service /usr/lib/systemd/system/psft-prcs-PRCSDO⇒
M.service /usr/lib/systemd/system/psft-pia-peoplesoft.service
```

7. Sync files to FS cloud directory.

```
$ mv /cm_psft_dpks/cloud /cm_psft_dpks/cloud_upgbkup
$ cp -r /opt/oracle/psft/pt/ps_app_home/cloud /cm_psft_dpks
$ chown -R root:root /cm_psft_dpks/cloud
$ chmod 755 -R /cm_psft_dpks/cloud
```

8. Verify the permission and ownership of files using below command.

```
$ ls -l /home/psadm1/.bashrc /home/psadm2/.bashrc /home/psadm3/.bashrc /home/o⇒
racle2/.bashrc /home/esadm1/.bashrc /etc/profile /usr/lib/systemd/system/psft-⇒
db-<DB_NAME>.service /usr/lib/systemd/system/psft-appserver-APPDOM.service /us⇒
r/lib/systemd/system/psft-prcs-PRCSDOM.service /usr/lib/systemd/system/psft-pi⇒
a-peoplesoft.service
-rw-r--r--. 1 root    root     3182 May  2 05:43 /etc/bashrc
-rwxr-xr-x. 1 root    root     1908 Apr 29 15:30 /usr/lib/systemd/system/psft-⇒
```



```
appserver-APPDOM.service
-rwxr-xr-x. 1 root    root     6891 Apr 29 15:24 /usr/lib/systemd/system/psft-⇒
db-<DB_NAME>.service
-rwxr-xr-x. 1 root    root     1773 Apr 29 15:36 /usr/lib/systemd/system/psft-⇒
pia-peoplesoft.service
-rwxr-xr-x. 1 root    root     1900 Apr 29 15:33 /usr/lib/systemd/system/psft-⇒
prcs-PRCSDOM.service
-rw-r--r--. 1 root    root     2354 May  2 05:43 /etc/profile
-rw-r--r--. 1 esadm1  oinstall  974 Apr 29 15:12 /home/esadm1/.bashrc
-rw-r--r--. 1 oracle2 oinstall  370 Apr 29 15:12 /home/oracle2/.bashrc
-rw-r--r--. 1 psadm1  oinstall  878 Apr 29 15:12 /home/psadm1/.bashrc
-rw-r--r--. 1 psadm2  oinstall 1097 Apr 29 15:12 /home/psadm2/.bashrc
-rw-r--r--. 1 psadm3  appinst   929 Apr 29 15:12 /home/psadm3/.bashrc
```

9. Start Cloud Manager using below commands or use the psadmin utility.

```
$ sudo systemctl start psft-db-<DBName>.service
$ sudo systemctl start psft-appserver-APPDOM.service
$ sudo systemctl start psft-prcs-PRCSDOM.service
$ sudo systemctl start psft-pia-peoplesoft.service
```

10. Restore the /cm_psft_dpks/cloud folder to all managed instances. This step is required if restoring from a latest Cloud Manager version to an older version. For example, restoring back to Cloud Manager Image 8 from Cloud Manager Image 9.

    Restoring to Linux instances

    a. SSH into Cloud Manager.

    b. Switch user to psadm2.

    ```
    $ sudo su - psadm2
    ```

    c. Securely copy the cloud directory from Cloud Manager to a managed node.

    ```
    $ scp -i /home/psadm2/psft/data/cloud/ocihome/keys/cm_adm_pvt_key -r /cm_⇒
    psft_dpks/cloud/  opc@< Instance1 IPADDRESS>:/home/opc/cloud
    ```

    Where <Instance1 IPADDRESS> is the first item in each row having unix as second field in backed up file /home/psadm2/managedenvironments.txt.

    d. Repeat the above copy step for all IP addresses tagged as unix in the file managedenvironments.txt.

    Restoring to Windows instances

    a. RDP into any Windows instance in the same VCN as the Cloud Manager.

    b. From the above Windows machine, RDP into each Windows instance listed in the backed up file managedenvironments.txt. The password is also captured in the same file.

    c. Access fileserver machine by opening the share \\<file_server_IP>\u01\app\oracle\product.

    d. Copy cloud folder from fileserver into D:\cloud.

Important! Please delete the managedenvironments.txt file after completing the cloud folder restores on all nodes.

Deleting Backup

To delete a block volume backup, the user must provide the backup name. User can list the existing backups then select the backup name to delete.

To delete a block (data) volume backup:

1. Run the utility with the restore option.

   ```
   sh cm_backup_restore.sh -o delete -n <backup_name>
   ```

2. User will be prompted to enter a passphrase for the private API signing key.

   Enter the passphrase if it exists or press enter.

3. The backup volume will be deleted.

Example:

```
[opc@smncm cm_backup_and_restore]$ sh cm_backup_restore.sh -o delete -n BLOCK_VOLBK⇒
P_SMNCM_20190410_110419
Please Enter Private Key Pass Phrase :
2019-04-19 10:16:02 -     INFO -  658 : Getting BLOCK volume backup 'BLOCK_VOLBKP_S⇒
MNCM_20190410_110419' details from OCI
2019-04-19 10:16:02 -     INFO -  666 : BLOCK volume backup 'BLOCK_VOLBKP_SMNCM_201⇒
90410_110419' Id : 'ocid1.volumebackup.oc1.iad.abuwcljre6zjpqrmk6ceqim3vu5jnmwt5zw4⇒
zb5vostgq55umw2bij5tt7cq'
2019-04-19 10:16:02 -     INFO - 1146 : Deleting volume backup : BLOCK_VOLBKP_SMNCM⇒
_20190410_110419
2019-04-19 10:16:02 -     INFO - 1157 : Deleted BLOCK volume backup 'BLOCK_VOLBKP_S⇒
MNCM_20190410_110419'
```

Manually Backing Up and Restoring Cloud Manager Using Block Volume Backups for OCI

Using block volume backup feature in OCI, the Cloud Manager data can be backed up and restored on demand.

Backing Up Cloud Manager

To backup Cloud Manager instance for OCI using block volumes, perform the following:

1. To create a consistent backup, shutdown the database, application, PIA and process scheduler domains.

   Note: Please make sure there are no provisioning or lifecycle jobs running. If there are, they will be abruptly ended and may result in environments in an unstable or unusable state.

2. SSH into the Cloud Manager instance and run following commands or use the psadmin utility.

   ```
   $ sudo systemctl stop psft-pia-peoplesoft.service
   $ sudo systemctl stop psft-prcs-PRCSDOM.service
   $ sudo systemctl stop psft-appserver-APPDOM.service
   $ sudo systemctl stop psft-db-<DBName>.service
   ```

3. Backup the set of files on boot volume that are listed below on to local file system on CM instance or any remote instance.

   Note: Use the environment variable PS_CFG_HOME to determine the exact path. Make a note of this in case the path gets modified during PeopleTools upgrade.

   - All files under PS_APP_HOME/cloud (/opt/oracle/psft/pt/ps_app_home/cloud)
   - All files under PS_CFG_HOME
   - /home/psadm1/.bashrc
   - /home/psadm2/.bashrc
   - /home/psadm3/.bashrc
   - /home/oracle2/.bashrc
   - /home/esadm1/.bashrc
   - /etc/profile
   - /etc/bashrc
   - /usr/lib/systemd/system/psft-db-<DB_NAME>.service
   - /usr/lib/systemd/system/psft-appserver-APPDOM.service
   - /usr/lib/systemd/system/psft-prcs-PRCSDOM.service
   - /usr/lib/systemd/system/psft-pia-peoplesoft.service

4. On the OCI console, navigate to Compute | Instances | Cloud Manager instance.
5. Navigate to Cloud Manager Instance Details page.
6. Scroll down to the Attached Block Volumes section. Click on the attached volume name which will have a name in the format StorageVol_<CMinstance>_<timestamp>. This volume is available as disk /dev/sdb in Cloud Manager instance. It is mounted on /u01/app/oracle/product, where Cloud Manager application is installed.
7. This will bring up the volume details. On this page, click on 'Create Backup'.
8. Optionally, create a backup of the boot volume in similar way.
9. Provide a name for the backup and click 'Create Backup'.
10. After few minutes a backup is created.
11. Start the database, pia, app and prcs domains. Use below commands or psadmin utility.

```
$ sudo systemctl start psft-db-<DBName>.service
$ sudo systemctl start psft-appserver-APPDOM.service
$ sudo systemctl start psft-prcs-PRCSDOM.service
$ sudo systemctl start psft-pia-peoplesoft.service
```


Restoring Cloud Manager

To restore a backup using block volumes, perform the following:

1. If restoring to an older version of Cloud Manager from a newer version, then generate the list of IP address of all managed instances that were provisioned by Cloud Manager. Follow step 1 in Restoring from a Backup.
2. On the OCI console, navigate to Storage | Backups.
3. Select the backup to restore and click 'Create Block Volume' using menu on the right.
4. Enter a name for the block volume and choose the Availability Domain in which the volume will be created. Ensure to choose the same Availability Domain where Cloud Manager instance is deployed.
5. A new volume is created in few seconds.
6. SSH to the Cloud Manager instance and shutdown database, pia, app and prcs domains using commands below or psadmin utility.

```
$ sudo systemctl stop psft-pia-peoplesoft.service
$ sudo systemctl stop psft-prcs-PRCSDOM.service
$ sudo systemctl stop psft-appserver-APPDOM.service
$ sudo systemctl stop psft-db-<DBName>.service
```

7. Clean up any running processes that might be using the data volume that needs to be restored.

```
$ ps -ef | grep psadm
psadm2 2969 1 0 Feb01 ? 00:00:19 rmiregistry 10100
psadm2 3495 1 0 Feb01 ? 00:00:20 rmiregistry 10200
$ sudo kill 2969 3495
```

8. Unmount /dev/sdb which is mounted on /opt/oracle/psft.

```
$ sudo umount /opt/oracle/psft
```

9. Navigate to OCI | Compute | Instances | Cloud Manager instance. Scroll down to the Attached Block Volumes. Select the volume to be restored and click Detach.
10. On the Detach Block Volume page, copy all DETACH COMMANDS.
11. Run the detach commands on the Cloud Manager instance.
12. Click 'Continue Detachment' (from step 9) and confirm detachment.
13. Verify in OCI UI for the instance that the volume is now removed.
14. Now restore the volume backup. Click Attach Block Volume. Select ISCSI attachment type. Select the block volume compartment where the backup volume was restored and select the restored volume. Select read-write access mode.
15. Click Attach to attach the restored volume to Cloud Manager instance.
16. After the status shows Attached. Retrieve the iSCSI commands that must be run on the instance to attach the volume in the OS. Click the Actions icon (Actions icon) next to the volume, and then click iSCSI Commands and Information. Copy all ATTACH COMMANDS.
17. SSH to the Cloud Manager instance and run the copied attach commands.

18. Verify the disk is attached using "sudo fdisk –l" command. There should now be an entry for /dev/sdb.

```
Disk /dev/sdb: 107.4 GB, 107374182400 bytes
255 heads, 63 sectors/track, 13054 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 4096 bytes
I/O size (minimum/optimal): 4096 bytes / 4096 bytes
Disk identifier: 0x00000000
```

19. Restore below set of files that were backed up from boot volume. Ensure to restore the PS_CFG_HOME files to the right path in case the backup contains files from an older PeopleTools release.

    - Restore /cm_psft_dpks/cloud/ from backup of PS_APP_HOME/cloud
    - All files under PS_CFG_HOME
    - /home/psadm1/.bashrc
    - /home/psadm2/.bashrc
    - /home/psadm3/.bashrc
    - /home/oracle2/.bashrc
    - /home/esadm1/.bashrc
    - /etc/profile
    - /etc/bashrc
    - /usr/lib/systemd/system/psft-db-<DB_NAME>.service
    - /usr/lib/systemd/system/psft-appserver-APPDOM.service
    - /usr/lib/systemd/system/psft-prcs-PRCSDOM.service
    - /usr/lib/systemd/system/psft-pia-peoplesoft.service

20. Run 'mount -a' command on the CM instance and reboot the instance. Check status of Cloud Manager domains using following commands.

```
$ sudo systemctl status psft-db-<DBName>.service
PeopleSoft Container Database CDBHCM Status is Up
PeopleSoft Pluggable Database PSPDB Status is Open
PeopleSoft Database Listener is Up
$ sudo systemctl status psft-prcs-PRCSDOM.service
PeopleSoft Process Scheduler Domain PRCSDOM is Up
$ sudo systemctl status psft-appserver-APPDOM.service
PeopleSoft Application Server Domain APPDOM is Up
$ sudo systemctl status psft-pia-peoplesoft.service
PeopleSoft PIA Domain peoplesoft is Up
```

    If database and domains do not come up automatically then start them using the following commands. Reboot only if necessary.

```
$ sudo systemctl start psft-db-<DBName>.service
$ sudo systemctl start psft-appserver-APPDOM.service
$ sudo systemctl start psft-prcs-PRCSDOM.service
$ sudo systemctl start psft-pia-peoplesoft.service
```


If the database or domains don't start successfully, then the restored backup may have issues, In such scenario, there are two options at this point:

a. Restore the original volume. Follow steps 5 to 18 described under 'How to restore a backup' section.

b. Troubleshoot the reason for failures and bring up the database or domains manually.

21. SSH into Cloud Manager and remove the directory /home/psadm2/psft/data/cloud/dm/cache/.

22. Before accessing the restored Cloud Manager PIA URL, you need to clear the application domain cache. To clear cache:

    a. SSH into Cloud Manager instance.

    b. Switch user to psadm2.

    ```
    sudo su - psadm2
    ```

    c. Start psadmin.

    d. Select 1) Application Server.

    e. Select 1) Administer a domain.

    f. Select 1) APPDOM.

    g. Select 8) Purge Cache.

23. If restoring to an older version from a newer version of Cloud Manager, copy the restored /cm_psft_dpks/cloud to all the managed instances. Follow step 10 in Restoring from a Backup.

Note: If you want specific downloads to begin, unsubscribe and then subscribe to the required download channels. Otherwise, the downloads will begin at the next scheduled time.
