INSTALLING PEOPLETOOLS 8.57 IN ORACLE CLOUD

Installing and configuring cloud manager:-

Process overview:

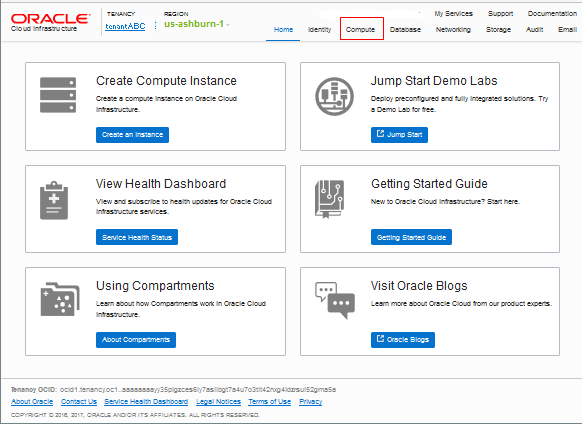
1. Verify Oracle Cloud account information used in installing Cloud Manager.
2. Download the Cloud Manager and Oracle Linux images to a local machine and upload them to Oracle Cloud Infrastructure Object Storage.
3. Import the Linux image from Oracle Cloud Object Storage to Compute.
4. Create a custom updated Microsoft Windows Server 2012 R2 image.
5. Generate an SSH key pair using an on-premises Linux or Microsoft Windows system.
6. In Compute Console, create a virtual cloud network (VCN).
7. Import the Cloud Manager image from Oracle Cloud Object Storage.
8. Provision a Compute instance using the Cloud Manager image.
9. Access the Cloud Manager instance and run a script to generate API keys.
10. Access the VM for the Cloud Manager instance and run the instance configuration wizard to set up Cloud Manager.
11. Sign in to the Cloud Manager instance in a browser and supply the Cloud Manager Settings and Infrastructure details.
12. In Cloud Manager, create a file server.
13. Set up security lists for PeopleSoft environments.
14. Review the delivered users and permission lists.

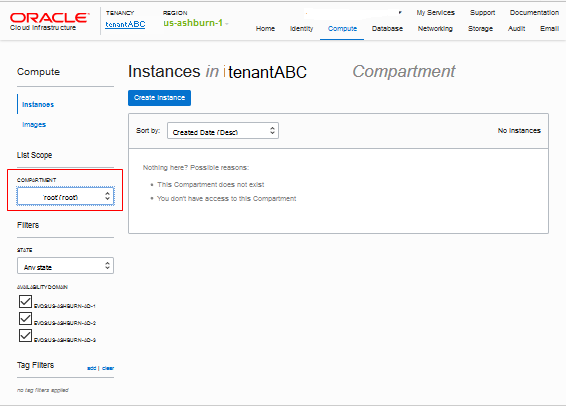
Verifying oracle cloud Account Information:

Verifying Access to Oracle Cloud Infrastructure Compute and Oracle Cloud Infrastructure Object Storage:

1. Sign in to Compute using the URL provided by your administrator, for example:

<https://console.us-ashburn-1.oraclecloud.com>.

1. Enter the name of your tenancy if necessary, and enter your user name and password.
2. Select Compute from the links at the top of the page.
3. 
4. On the Compute page, select your compartment from the drop-down list on the left.
5. If the Instances area does not display anything, as shown in this example, you may not have the appropriate permission to create instances. Contact your administrator.



7. Verify access to Oracle Cloud Infrastructure Object Storage by selecting Storage at the top of the page.

**Note**. For ease of use and faster transfers, it is a good idea to use the same Region to upload the image to Object Storage and to import to compute.

### Installing CLI for the Cloud Manager Image Upload:

### Due to the Cloud Manager Image size, you must use the CLI to upload the image to Oracle Cloud Infrastructure Object Storage, rather than uploading through the Oracle Cloud Infrastructure Console. Before you begin the process to upload the image, follow the instructions in the Oracle Cloud Infrastructure documentation to install and configure the CLI.

The CLI is a small footprint tool that you can use on its own or with the Console to complete Oracle Cloud Infrastructure tasks. The CLI provides the same core functionality as the Console, plus additional commands. Some of these, such as the ability to run scripts, extend the Console's functionality.

## **Requirements**

To install and use the CLI, you must have:

* An Oracle Cloud Infrastructure account
* A user created in that account, in a group with a policy that grants the desired permissions. This account user can be you, another person, or a system that calls the API. For an example of how to set up a new user, group, compartment, and policy, see [Adding Users](https://docs.cloud.oracle.com/iaas/Content/GSG/Tasks/addingusers.htm). For a list of other typical Oracle Cloud Infrastructure policies, see [Common Policies](https://docs.cloud.oracle.com/iaas/Content/Identity/Concepts/commonpolicies.htm).
* A keypair used for signing API requests, with the public key uploaded to Oracle. Only the user calling the API should possess the private key. See [Configuring the CLI](https://docs.cloud.oracle.com/iaas/Content/API/SDKDocs/cliconfigure.htm).
* Python version 2.7.5 or 3.5 or later, running on Mac, Windows, or Linux. Note that if you use the CLI Installer and do not have Python on your machine, the Installer offers to automatically install Python for you. If you already have Python installed on your machine, you can use the python --version command to find out which version is installed.
* If you require FIPS-compliance, see [Using FIPS-validated Libraries](https://docs.cloud.oracle.com/iaas/Content/API/SDKDocs/cliconfigure.htm#fips).

Windows

1. Open the PowerShell console using the **Run as Administrator** option.
2. The installer enables auto-complete by installing and running a script. To allow this script to run, you must enable the RemoteSigned execution policy.

To configure the remote execution policy for PowerShell, run the following command.

Set-ExecutionPolicy RemoteSigned

To run the installer script, run the following command

powershell -NoProfile -ExecutionPolicy Bypass -Command "iex ((New-Object System.Net.WebClient).DownloadString('https://raw.githubusercontent.com/oracle/oci-cli/master/scripts/install/install.ps1'))"

Installation Script Prompts

The installation script prompts you for the following information.

* If you do not have a compatible version of Python installed:
  + Windows and Linux: You are prompted to provide a location for installing the binaries and executables. The script will install Python for you.
* When prompted to upgrade the CLI to the newest version, respond with **Y** to overwrite an existing installation.
* When prompted to update your PATH, respond with **Y** to be able to invoke the CLI without providing the full path to the executable. This will add oci.exe to your PATH.

## **Setting up the Config File**

Before using the CLI, you must create a config file that contains the required credentials for working with Oracle Cloud Infrastructure. You can create this file using a setup dialog or manually using a text editor.

Type below command

oci setup config

Then it will ask your tenancy ocid and user ocid, and where to create oci config fie, private key pum file , public key pum file enter default location or choose one.

These public key pum file are used to store in user API key file location later.

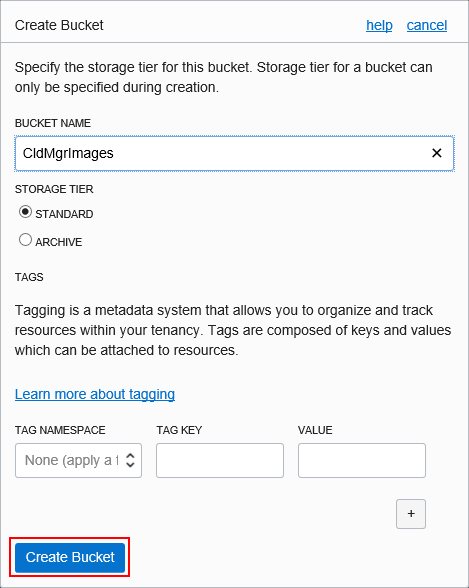
### Creating an Object Storage Bucket

In the next section you upload the Cloud Manager image to a bucket in Oracle Cloud Infrastructure Object Storage. If there is an existing bucket in Object Storage, note the name and skip this section.

See Object Storage, [Managing Buckets](https://docs.us-phoenix-1.oraclecloud.com/Content/Object/Tasks/managingbuckets.htm).

If you need to create a bucket in Object Storage for the CLI process:

1. Sign in to the Oracle Cloud Infrastructure Console and select the Storage tab.
2. Select your compartment from the drop-down list on the left, and then select the Object Storage link on the left.
3. Click **Create Bucket**.
4. On the Create Bucket dialog box, select the Storage Tier option, provide a name for the bucket, and click **Create Bucket**. Note the bucket name, which is CldMgrImages in this example, for the next section.



### Downloading the Cloud Manager Image and Uploading to Object Storage

Download and extract the Cloud Manager image, and import it to Oracle Cloud Infrastructure Object Storage as follows:

1. Sign in to the Oracle Cloud Marketplace at <http://cloud.oracle.com/marketplace>.
2. In the Applications area, enter PeopleSoft or Cloud Manager in the search text box, and click the **Go** button.
3. In the search results, locate the listing for PeopleSoft Cloud Manager 7 for Oracle Cloud Infrastructure.

**Note**. Be sure to select the listing for Cloud Manager Image for Oracle Cloud Infrastructure. There is a different listing for Cloud Manager Image for Oracle Cloud Infrastructure Classic.

1. On the details page for the application, click the **Get App** button at the top right.
2. Read and accept the Oracle terms. When you click Next, you are redirected to My Oracle Support.
3. Sign in to My Oracle Support, and select the link to the Cloud Manager image listing in My Oracle Support.
4. From the Patches & Updates area, download the image file to your local system.

The image file is in qcow2 format and is available for download as a compressed file. The file name has the format OCI\_X86\_64\_PSFTCM\_PXX\_OL\_6.9\_01.zip, where PXX is the image number, such as P07.

1. Extract the compressed image file to obtain the file in qcow2 format.
2. On the computer where you downloaded and extracted the image, open a command prompt and use the CLI to upload the image file to a bucket in Object Storage.

See the Oracle Cloud Infrastructure documentation, Object Storage, Managing Objects, [Using the Command Line Interface (CLI)](https://docs.us-phoenix-1.oraclecloud.com/Content/Object/Tasks/managingobjects.htm#CLI).

For example, use this CLI command:

C:\users\opc\bin> ./oci.exe os object put -ns tenancyABC -bn bucket\_name --file C:\Users\opc\Documents\OCI\_X86\_64\_PSFTCM\_P06\_OL\_6.9\_01.qcow2 --name OCI\_X86\_64\_PSFTCM\_P06\_OL\_6.9\_01 --no-multipart

1. The command uses the following options:
   * -ns — Specify the namespace that you want to use. To determine your namespace, click the Tenancy link at the top of the Oracle Cloud Infrastructure Console window. On the Tenancy Information page, note the name for Object Storage Namespace.
   * -bn — Specify the name of the Object Storage bucket that you created or noted in Creating an Object Storage Bucket.
   * --file — Specify the full path and filename for the Cloud Manager image file that you downloaded and extracted.
   * --name — Specify the name to be applied to the object in the Object Storage bucket.
   * --no-multipart — Specify that the files will not be split when uploading to Object Storage.

**Note**. The –ns and –bn options require a single dash, and the other options use a double dash. See the [OCI CLI Command Reference](https://docs.us-phoenix-1.oraclecloud.com/tools/oci-cli/latest/oci_cli_docs/cmdref/os.html) for more information.

1. Sign in to the Oracle Cloud Infrastructure Console and select the Storage tab.
2. Select your compartment from the drop-down list on the left, and then select the Object Storage link.
3. Select the bucket that you used to upload the Cloud Manager image, and the image in the Objects list.
4. Select **Details** from the Action menu for the object, and copy the URL path. Make a note of the path to use in the section Importing the Cloud Manager Image.

### Choosing an Oracle Linux Image for the File Server

Cloud Manager requires an Oracle Linux 6 image for the file server. Obtain an image using one of the methods outlined here. After completing the Cloud Manager setup, you will configure the file server in the Cloud Manager Infrastructure Settings area.

Choose one of these methods to obtain an Oracle Linux image for the file server:

* You can download an Oracle Linux image, called PeopleSoft Linux Image for Cloud Manager, that is configured for use with Cloud Manager, from My Oracle Support, and upload it to Oracle Cloud Infrastructure Object Storage. The next section describes how to locate, download, and upload the image.

This is a reference image that you can use for a quick start to evaluate Cloud Manager. If the image suits your organizational requirements, you can continue to use the same image for production.

* If your organization has requirements for custom packages and security settings, you can create a custom image based on the PeopleSoft Linux Image for Cloud Manager reference image. Use the information in the tutorial [Creating a Custom Linux Image for PeopleSoft Cloud Manager in Oracle Cloud Infrastructure](http://www.oracle.com/webfolder/technetwork/tutorials/obe/cloud/compute-iaas/create_custom_linux_image_psft_cm_oci/cloud-manager-linux-image-oracle-cloud-infrastructure.html) to customize the reference image.
* You also have the option to create a custom image using a base Oracle Linux image. In this case, you must carry out additional steps to configure the image to work with Cloud Manager. In addition, you are responsible for determining and obtaining any operating system requirements.

For information, see the tutorial [Creating a Custom Linux Image for PeopleSoft Cloud Manager in Oracle Cloud Infrastructure](http://www.oracle.com/webfolder/technetwork/tutorials/obe/cloud/compute-iaas/create_custom_linux_image_psft_cm_oci/cloud-manager-linux-image-oracle-cloud-infrastructure.html).

### Downloading the PeopleSoft Linux Image for Cloud Manager and Uploading to Object Storage

If you want to use the PeopleSoft Linux Image for Cloud Manager, download, extract, and combine the image, and import it to Oracle Cloud Infrastructure Object Storage as follows:

1. Sign in to the Oracle Cloud Marketplace at <http://cloud.oracle.com/marketplace>.
2. In the Applications area, enter PeopleSoft or Cloud Manager in the search text box, and click the **Go** button.
3. In the search results, locate the listing for PeopleSoft Cloud Manager 7 for Oracle Cloud Infrastructure.

**Note**. Be sure to select the listing for Cloud Manager Image for Oracle Cloud Infrastructure. There is a different listing for Cloud Manager Image for Oracle Cloud Infrastructure Classic.

1. On the details page for the application, click the Get App button at the top right.
2. Read and accept the terms. When you click Next, you are redirected to My Oracle Support.
3. Sign in to My Oracle Support, and select the link to the PeopleSoft Linux Image for Cloud Manager listing in My Oracle Support.
4. From the Patches & Updates area, download the image file to your local system.

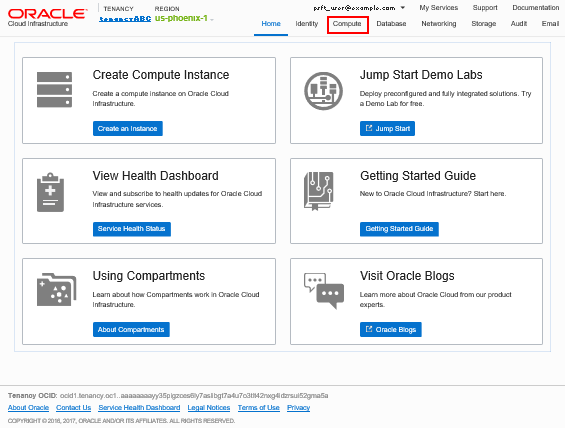
The image file is in qcow2 format and is available for download as a compressed file. The file name has the format OCI\_X86\_64\_PSFTBASE\_OL\_6.9\_01.zip.

1. Extract the compressed image file to obtain the file in qcow2 format.
2. Sign in to the Oracle Cloud Infrastructure Console and select the Storage tab.
3. Select your compartment from the drop-down list on the left, and then select the Object Storage links on the left.
4. Select the Bucket you created in the previous section.
5. Select **View Bucket** from the Action menu for the bucket.
6. On the Bucket Details page, click **Upload Object** and browse to the location where you saved the Linux image.
7. Select Details from the Action menu for the object, and copy the URL path. Make a note of the path to use in the section Importing PeopleSoft Linux Image for Cloud Manager.

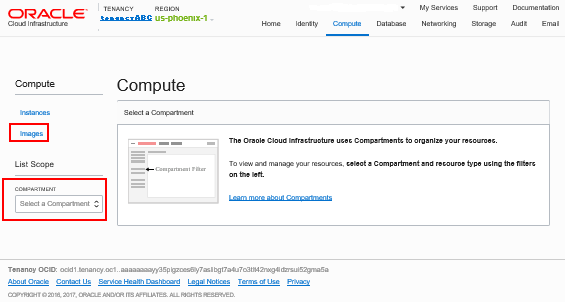
## **Importing the PeopleSoft Linux Image for Cloud Manager**

Import the PeopleSoft Oracle Linux image for Cloud Manager as follows:

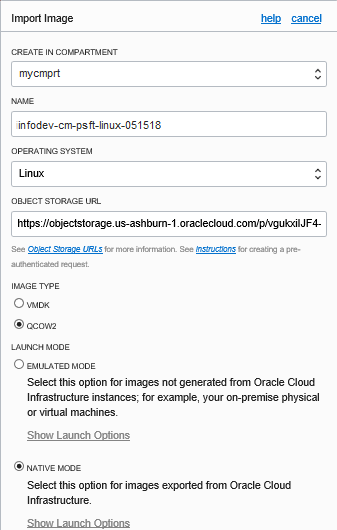
1. Sign in to the Compute Console and select **Compute**.



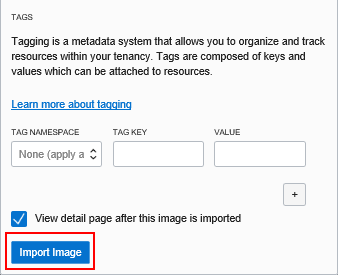
From the panel on the left, select the compartment that you want to work in, and select Images.



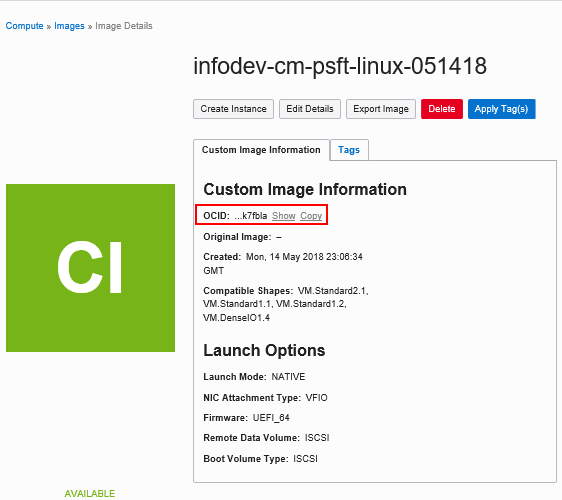
1. Click the **Import Image** button.
2. On the Import Image dialog box, select the compartment where you want to create the image from the Create in Compartment drop-down list, mycmprt in this example.



1. Enter a name for the image, psft-linux1 in this example.
2. Select Linux from the Operating System drop-down list.
3. Enter the URL to the image in the Object Storage URL field.
4. Select the QCOW2 Image Type.
5. Under Launch Mode, select Native Mode.
6. Click **Import Image**.



When the status for the image displays Available, select Show or Copy for the OCID. Make a note of the OCID, as you will need this when running the Cloud Manager instance configuration wizard.



## **Obtaining an Updated Microsoft Windows Image for Cloud Manager**

Cloud Manager requires a Microsoft Windows image to host PeopleSoft client tools such as Change Assistant and Application Designer. Follow the instructions in the tutorial [Creating a Custom Windows Image for PeopleSoft Cloud Manager in Oracle Cloud Infrastructure](http://www.oracle.com/webfolder/technetwork/tutorials/obe/cloud/compute-iaas/create_custom_windows_image_psft_cm_oci/cloud-manager-windows-image-oracle-cloud-infrastructure.html) to obtain a Microsoft Windows Server 2012 R2 image, apply the latest Microsoft updates, and create a custom image. You will enter the OCID and Windows administrator password for the custom image when completing the section Specifying the Cloud Manager Settings in this tutorial.

Note that the Windows administrator password must meet the password complexity requirements set by the Microsoft Windows operating system. See the section Reviewing the Windows Password Policy in the tutorial [Creating a Custom Windows Image for PeopleSoft Cloud Manager in Oracle Cloud Infrastructure](http://www.oracle.com/webfolder/technetwork/tutorials/obe/cloud/compute-iaas/create_custom_windows_image_psft_cm_oci/cloud-manager-windows-image-oracle-cloud-infrastructure.html).

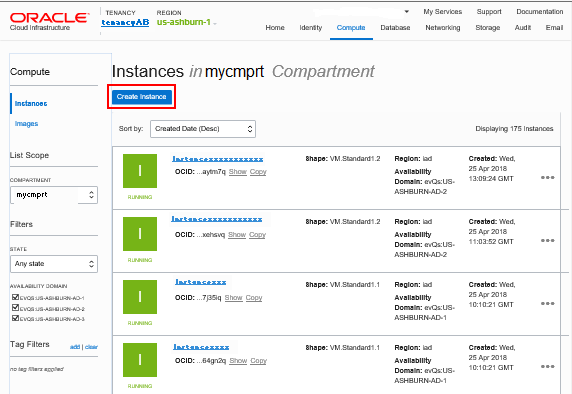
## **Provisioning the Microsoft Windows Instance**

Use the Compute Console to configure a VM instance from a Microsoft Windows 2012 R2 Oracle-provided image.

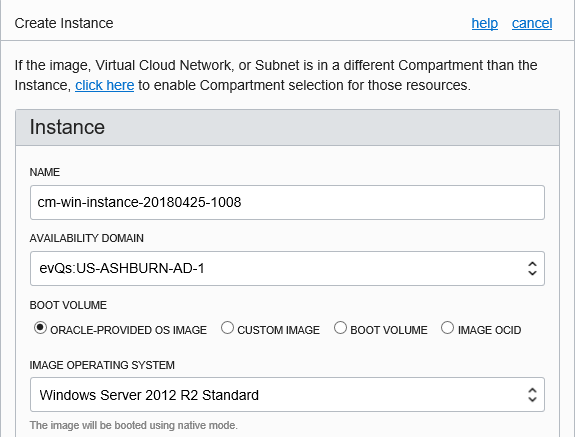
1. Sign in to Compute using the URL provided by your administrator, for example:

<https://console.us-ashburn-1.oraclecloud.com>.

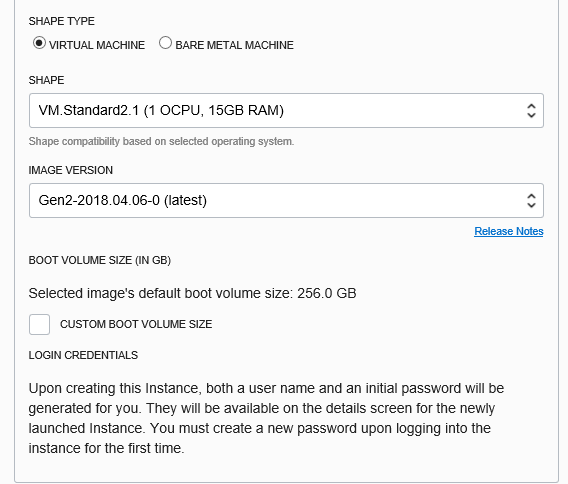
1. Enter the name of your tenancy if necessary, and enter your user name and password.
2. Select **Compute** from the links at the top of the page.
3. If necessary, select **Instances** from the left-hand frame.
4. Click **Create Instance**.



Enter a name for the Windows instance on the Create Instance dialog box.



1. Select the Availability Domain where you want the instance to reside.
2. Select the option **ORACLE-PROVIDED OS IMAGE**, and select Windows Server 2012 R2 Standard from the IMAGE OPERATING SYSTEM drop-down list.
3. Select the option **VIRTUAL MACHINE**.



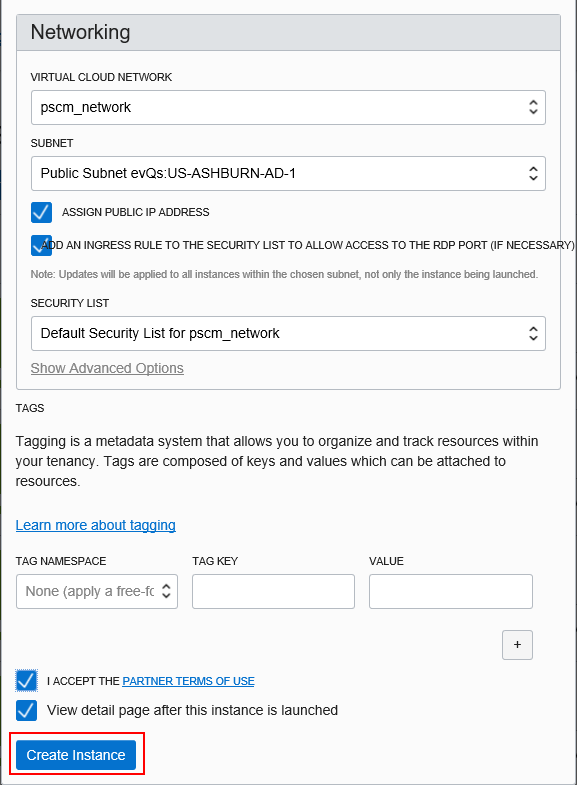
1. Select a shape from the drop-down list, such as VM.Standard2.1 (1 OCPU, 15GB RAM). The shapes listed depend upon the selected OS image and the availability for your tenancy.

Note that the shapes associated with the Windows image will also be available for nodes created in Cloud Manager on Microsoft Windows.

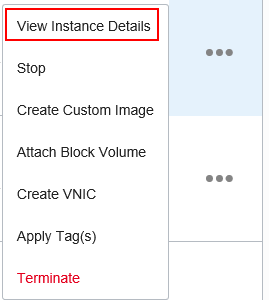
1. Accept the latest image version.
2. Select the VCN that you created from the VIRTUAL CLOUD NETWORK drop-down list, and select a subnet.

You can choose either a private subnet or a public subnet. If you choose a private subnet, then the Microsoft Windows instance will be accessible from another Microsoft Windows instance on

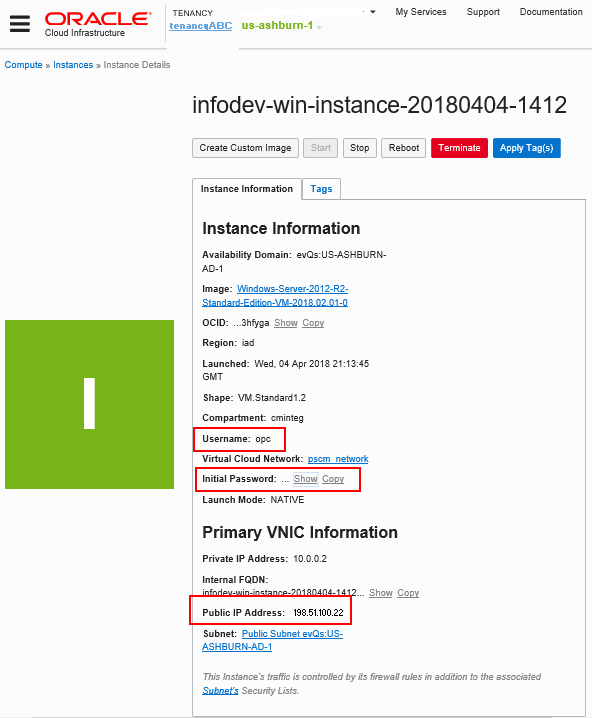
the same subnet. If you choose a public subnet, then the Microsoft Windows instance is easily accessible over the Internet.



1. Accept the option **ASSIGN PUBLIC IP ADDRESS**.
2. Select the option **ADD AN INGRESS RULE TO THE SECURITY LIST TO ALLOW ACCESS TO THE RDP PORT (IF NECESSARY)**, and select a security list.
3. Select the option **I ACCEPT THE PARTNER TERMS OF USE**, and accept the option **View detail page after the instance is launched**.
4. Click **Create Instance**.
5. On the Compute Console Instances page, locate the instance.
6. Click the Actions icon (Action icon), and select **View Instance Details**.



On the Details page, make a note of the Public IP Address, 198.51.100.22 in this example, and the username, opc.



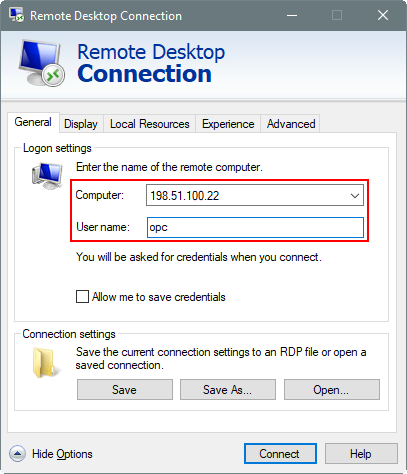
Click the link to Copy the Initial Password to the clipboard.

## **Accessing the Windows Instance with Remote Desktop Connection**

After you create the Windows instance, use Remote Desktop Connection to access it.

See Oracle Cloud Infrastructure online documentation, Compute, [Connecting to an Instance](https://docs.us-phoenix-1.oraclecloud.com/Content/Compute/Tasks/accessinginstance.htm).

1. Launch Remote Desktop Connection, for example from the Start menu of a local Microsoft Windows host.
2. In the Computer field, enter the Public IP address, which is 198.51.100.22 in this example, of the Microsoft Windows VM that you noted in the previous section. Enter opc in the User name field.



1. Click **Connect**.
2. Enter the default password you noted from the instance details page.
3. Click **Yes** on the security message, which mentions that the identity of the remote computer cannot be verified.
4. Change the password to a complex password. You will change it again in a later section.

## **Updating the Windows Instance for Cloud Manager**

### Configuring WinRM and Opening Ports

For a list of the ports used by Cloud Manager, see the section section Reviewing Cloud Manager Ports in the tutorial [Installing PeopleSoft Cloud Manager in Oracle Cloud Infrastructure](http://www.oracle.com/webfolder/technetwork/tutorials/obe/cloud/compute-iaas/install_peoplesoft_cloud_manager_oci/cloud-manager-install-oracle-cloud-infrastructure.html)

1. Select Start, Windows PowerShell. Right-click and select Run as Administrator.
2. In the PowerShell window, run the following command to prepare WinRM, and answer **y** to the prompt.

WinRM is a Windows administration protocol that Cloud Manager uses to connect remotely to the Windows VMs.

PS> winrm quickconfig  
  
WinRM service is already running on this machine.

WinRM is not set up to allow remote access to this machine for management.

The following changes must be made:

Configure LocalAccountTokenFilterPolicy to grant administrative rights remotely to local users.

Make these changes [y/n]? **y**

WinRM has been updated for remote management.

Configured LocalAccountTokenFilterPolicy to grant administrative rights remotely to local users.

1. Run the following three commands to allow login through basic authentication; wait for the status messages to complete for each.
   * winrm set winrm/config/service/Auth '@{Basic="true"}'
   * winrm set winrm/config/service '@{AllowUnencrypted="true"}'
   * winrm set winrm/config/winrs '@{MaxMemoryPerShellMB="1024"}'
2. Run the following commands to open ports 5985 and 5986 for WinRM:
   * netsh advfirewall firewall add rule name="Open Port 5985" dir=in action=allow protocol=TCP localport=5985
   * netsh advfirewall firewall add rule name="Open Port 5986" dir=in action=allow protocol=TCP localport=5986
3. Determine whether ports 137, 138, 139, and 445 are open in the Windows firewall, using a command such as netstat -an.

These ports are needed for Common Internet File System (CIFS), which is used for transferring files from Windows VMs to the Cloud Manager VM.

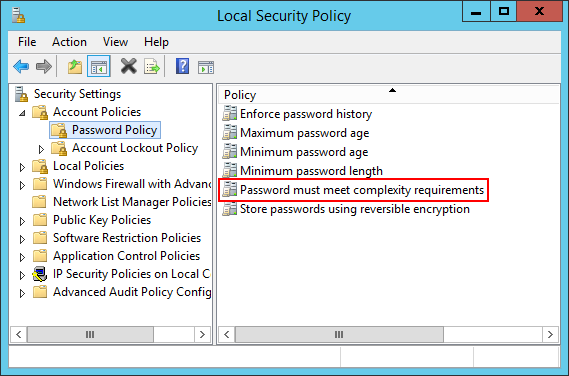
If the ports are not open, run the following commands to open the ports for CIFS:

* + netsh advfirewall firewall add rule name="Open Port 137" dir=in action=allow protocol=TCP localport=137
  + netsh advfirewall firewall add rule name="Open Port 138" dir=in action=allow protocol=TCP localport=138
  + netsh advfirewall firewall add rule name="Open Port 139" dir=in action=allow protocol=TCP localport=139
  + netsh advfirewall firewall add rule name="Open Port 445" dir=in action=allow protocol=TCP localport=445

### Reviewing the Windows Password Policy

The Windows administrator password that you supply when creating the custom Windows image must satisfy the password policy set by the Microsoft Windows operating system. When you provision an environment with a Windows node, for example a PUM environment with a PeopleSoft Client, Cloud Manager uses this custom Windows image. If you modify the attributes for the Windows node, and enter a new password, be sure that you specify a password that meets these password requirements. To view the Windows password policy:

1. Select Start, Administrative Tools, Local Security Policy.
2. On the Local Security Policy dialog box, expand Account Policies, and then expand Password Policy.
3. In the frame on the right, right-click Password must meet complexity requirements, and select Properties.



1. Note the Enabled or Disabled setting on the Local Security Setting tab.
2. Select the Explain tab to view the password complexity requirements. Make a note of the requirements to use if necessary when provisioning an environment that requires a Windows node.

### Configuring the Windows Administrator Password

1. Open Notepad with Run as Administrator, and open C:\Program Files\bmcs\imageType.json.
2. Change the image type from general to custom, and then save the file.

This is to prohibit a new Microsoft Windows instance from generating a random login password, when it is launched using this newly-created custom image. See [Creating Windows Custom Images](https://docs.us-phoenix-1.oraclecloud.com/Content/Compute/References/windowsimages.htm) for details.

Before:

{

"imageType": "general"

}

After:

{

"imageType": "custom"

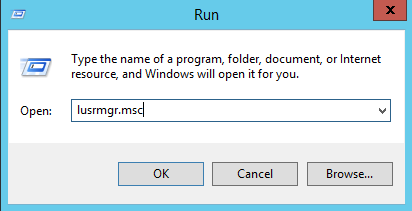
}

1. Run this command to reset the opc user (Windows administrator) password. Specify a password that meets the complexity requirements for Oracle Cloud Infrastructure, for example, "CloudManager@2017".

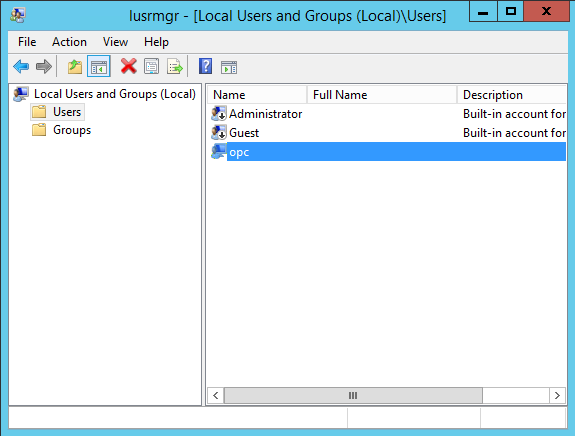
Make a note of the password you choose, because you must enter it on the Cloud Manager Infrastructure Settings page, in the field Windows Default Password.

net user opc "CloudManager@2017"

1. Run this command to install the NFS client, and wait until the process is complete.
2. >Install-WindowsFeature NFS-Client  
     
   Success Restart Needed Exit Code Feature Result
3. ------- -------------- --------- --------------
4. True Yes SuccessRest... {Client for NFS}
5. WARNING: You must restart this server to finish the installation process.
6. WARNING: Windows automatic updating is not enabled. To ensure that your newly-installed role or feature is
7. automatically updated, turn on Windows Update.
8. Restart the VM, by selecting Start, Shut down or sign out, Restart. Wait a few minutes for it to come back up.
9. Use Remote Desktop Connection to sign in as user opc with the password that you specified in step 3, CloudManager@2017.
10. Select Start, Run, and enter lusrmgr.msc to access the Windows Local Users and Groups utility.

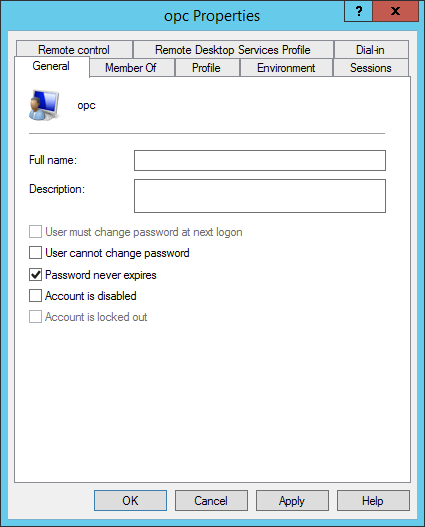


Double-click the Users folder and select the opc user.



1. Select Action, Properties.
2. On the opc Properties dialog box, select the General tab. Select the option **Password never expires**.

**Important!** This is required to prevent the password on the image from expiring after some time. If the password were to expire, the image would have to be recreated.



1. Click **OK** to close the opc Properties dialog box, and File, Exit to close the Local Users and Groups dialog box.

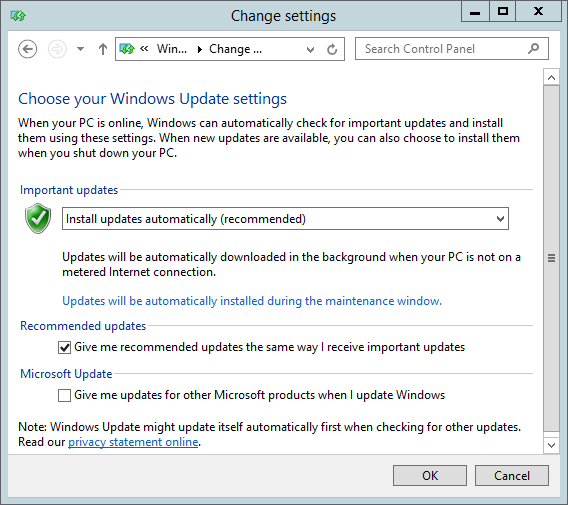
**Important**: Before proceeding, verify that you have completed all of the steps in this section in order to use the image successfully with Cloud Manager.

## **Applying Windows Updates**

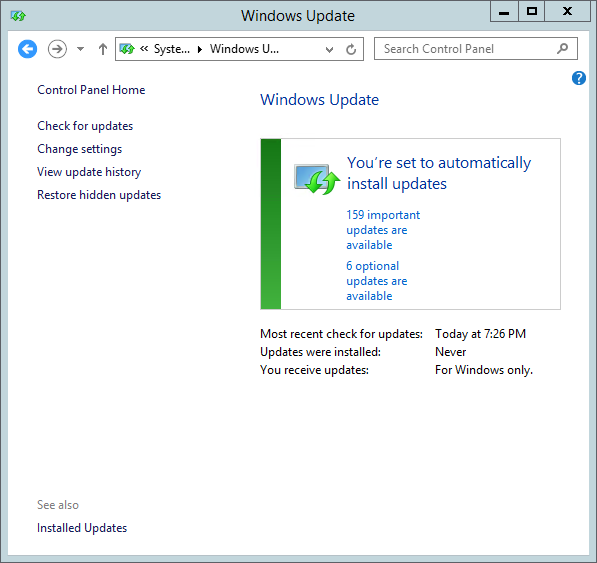
Install the latest version of Universal C Runtime on the Microsoft Windows instance. If you use the Windows Update procedure, as described here, review the updates to ensure that that latest Universal C Runtime was included.

Alternatively, go to the Microsoft site and follow the instructions there. See https://support.microsoft.com/en-in/help/2999226/update-for-universal-c-runtime-in-windows.

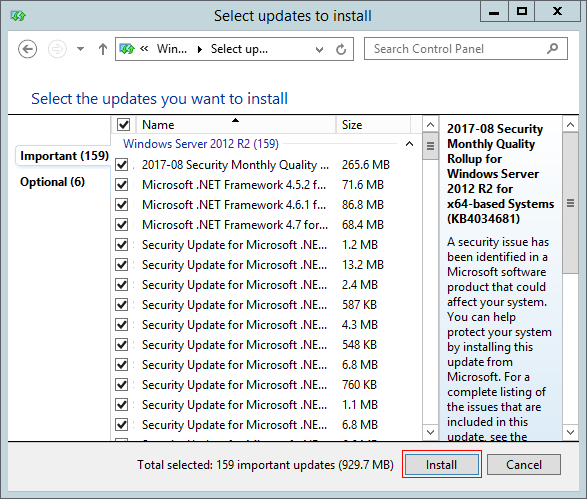
1. In the Windows VM, select Control Panel, Systems and Security, Windows Update.
2. Select **Change Settings**.
3. On the Choose your Windows Update settings window, select Install updates automatically (recommended) from the **Important updates** drop-down list. The other options include:
   * Download updates but let me choose whether to install them
   * Check for updates, but let me choose whether to download and install them
   * Never check for updates (not recommended)



1. Choose how to receive recommended options. The example shows that the option **Give me recommended updates the same way I receive important updates**is selected.
2. Click **OK** to begin checking for updates.
3. On the Windows Update window, click the link for the important updates.

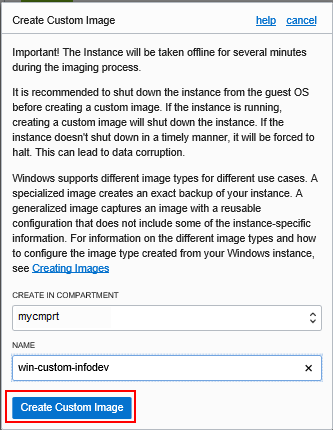


On the Select updates to install window, select all updates, and click **Install**.



## **Creating a Custom Image**

1. In Compute Console, select Compute, Instances.
2. Locate the updated Windows instance.
3. Click the Actions icon (Actions icon), and select **Create Custom Image**.
4. Select the compartment where you want the custom image to reside.
5. Enter a name, such as win-custom-infodev.



1. Click **Create Custom Image**.
2. Monitor the progress on the Compute, Images page.
3. When the status of the custom image changes to Available, copy the OCID for the image. You use it in the next section.
4. After you create the custom image, you can safely remove the instance used to create the image.

See [Creating Windows Custom Images](https://docs.us-phoenix-1.oraclecloud.com/Content/Compute/References/windowsimages.htm) in the Oracle Cloud Infrastructure online documentation.

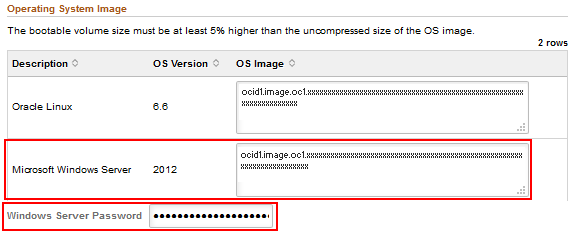
## **Using the Windows Image in Cloud Manager**

### Updating the Cloud Manager Settings

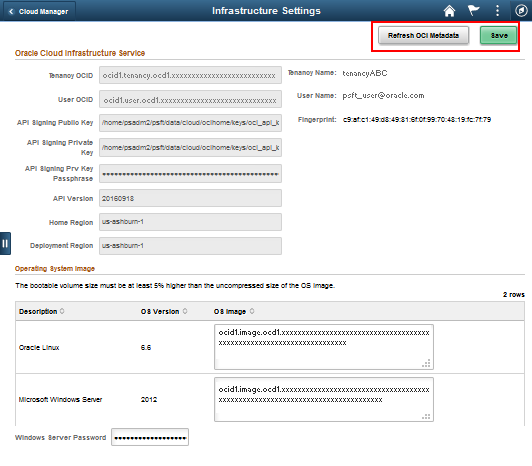
1. Complete the Cloud Manager installation.

See the tutorial Installing PeopleSoft Cloud Manager in Oracle Cloud Infrastructure.

1. Sign in to the Cloud Manager instance as the Cloud Administrator, click the Cloud Manager Settings card, and select the Infrastructure Settings page.
2. Enter the OCID for the Microsoft Windows custom image in the Operating System Image section for Microsoft Windows.



1. On the same page, update the value for the password in the Windows Server Password field with the password you entered in the section Updating the Windows Instance for Cloud Manager.
2. Click **Save** and then **Refresh OCI Metadata** at the top of the page. This ensures that the shapes that are associated with this image are reflected in Cloud Manager.



### Troubleshooting

When you provision an environment that uses the Windows image, for example the PeopleTools client, you may see the following error message:

http response error: 401 - invalid content type

This error occurs when the wrong values are entered for the Windows image OCID or Windows Server Password in the Cloud Manager Infrastructure Settings page. If you see this error, correct the values on the Infrastructure Settings page and save the page.

Generating an SSH Key Pair on UNIX or UNIX-Like Systems Using ssh-keygen

1. Run the ssh-keygen command.

ssh-keygen -b 2048 -t rsa

1. The command prompts you to enter the path to the file in which you want to save the key. A default path and file name are suggested in parentheses. For example: /home/user\_name/.ssh/id\_rsa. To accept the default path and file name, press **Enter.** Otherwise, enter the required path and file name, and then press **Enter**.
2. The command prompts you for a passphrase. Enter a passphrase.

Note that the passphrase isn't displayed when you type it in. Remember the passphrase. If you forget the passphrase, you can't recover it.

1. When prompted, enter the passphrase again to confirm it.

The command generates an SSH key pair consisting of a public key and a private key, and saves them in the specified path. The file name of the public key is created automatically by appending .pub to the name of the private key file. For example, if the file name of the SSH private key is id\_rsa, then the file name of the public key would be id\_rsa.pub.

1. Make a note of the path where you've saved the SSH key pair.

When you create instances, you must provide the SSH public key. When you log in to an instance, you must specify the corresponding SSH private key and enter the passphrase when prompted.

Generating an SSH Key Pair on Microsoft Windows

Generate a secure SSH key pair using an application such as PuTTY.

Make a note of the public and private key names and where they are saved. When you create instances, you must specify the SSH public key. When you log in to an instance, you must provide the path to the corresponding SSH private key and enter the passphrase when prompted.

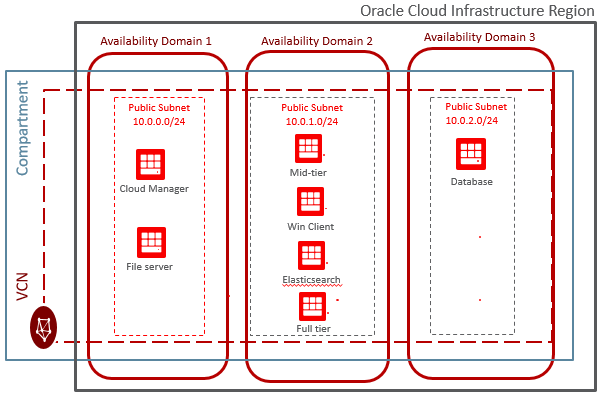
## **Creating a Virtual Cloud Network for Cloud Manager**

### Planning the Cloud Manager VCN

The PeopleSoft Cloud Manager image contains a web server installation configured to listen for requests on port 8000 (HTTP) and 8443 (HTTPS). Your security protocols may require you to use other port values. If you use other ports, configure them here and supply the same values in the section Running the Cloud Manager Instance Configuration Wizard.

See the [Oracle Cloud Infrastructure Networking](https://docs.us-phoenix-1.oraclecloud.com/Content/Network/Concepts/overview.htm) documentation for information on VCNs.

**Note**. Oracle highly recommends that you use the HTTPS protocol in all deployments. Follow the instructions found in the [*PeopleTools System and Server Administration*](http://docs.oracle.com/cd/E17566_01/epm91pbr0/eng/psbooks/psft_homepage.htm) product documentation to implement the encryption keys and certificates required for Secure Sockets Layer (SSL) encryption.



### Defining Subnets

The subnets that you define in your VCN must take into account the requirements for communication between the PeopleSoft environment and Cloud Manager components. It is important to note that all subnets must allow traffic from the Cloud Manager instance. To achieve this, you must add rules to each security list allowing NFS ports from the source subnet (which is the subnet on which Cloud Manager resides).

For successful deployments of PeopleSoft environments, you must define security lists for subnets based on what type of PeopleSoft instances will be deployed in that subnet.

For example, if you create separate subnets for mid-tier, database tier and PeopleSoft Windows Client, then you must create security lists for the subnet that hosts the mid-tier instance such that it allows all the required ports that a user plans to use when deploying PeopleSoft environments.

If you plan to use more than one subnet for your PeopleSoft deployments, then those subnets must allow communications from the subnet where Cloud Manager is set up. Create security lists for subnets that allow Cloud Manager and the file server to communicate with instances that will be deployed on other subnets.

When you create a VCN for Cloud Manager, you choose from options to create a VCN with related resources or create only a VCN. In this tutorial, a later section creates a VCN using the option to create related resources. This creates a VCN with default components, including three public subnets with open access, an Internet gateway, a route table, and a security list.  In this case, you must update the default security list with a rule to allow all Cloud Manager NFS ports either with the VCN CIDR as source or Cloud Manager's subnet CIDR as source.

If instead you choose to create only a VCN, you would define the subnets separately. In this case, there would be one security list per subnet, and you must update each security list to allow traffic from the subnet where Cloud Manager resides.

The following table shows the required security rules needed based on the PeopleSoft node types:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Destinations** | **Source: Cloud Manager and File Server** | **Source: Mid-tier** | **Source: Database** | **Source: PeopleSoft Windows Client** | **Source: Full-tier** | **Source: Elasticsearch** |
| **Cloud Manager and File Server** | * NFS (ports 2049, 111, 892, and 32803) * SSH (port 22) | NFS (ports 2049, 111, 892, and 32803) | NFS (ports 2049, 111, 892, and 32803) | * NFS (ports 2049, 111, 892, and 32803) * PIA HTTP (port 8000) * PIA HTTPS (port 8443) | NFS (ports 2049, 111, 892, and 32803) | NFS (ports 2049, 111, 892, and 32803) |
| **Mid-tier** | SSH (port 22) | * Jolt (port 9033) * PIA HTTP (port 8000) * PIA HTTPS (port 8443) | NA | * PIA HTTP (port 8000) * PIA HTTPS (port 8443) | NA | NA |
| **Database** | SSH (port 22) | Database ports (1521) | NA | NA | NA | NA |
| **PeopleSoft Windows client** | * Winrm (ports 5985 and 5986) * CIFS (ports 137, 138, 139, and 445) | NA | NA | NA | NA | NA |
| **Full-tier** | SSH (port 22) | NA | NA | * NFS (ports 2049, 111, 892, and 32803) * PIA HTTP (port 8000) * PIA HTTPS (port 8443) | NA | * PIA HTTP (port 8000) * PIA HTTPS (port 8443) |
| **Elasticsearch** | SSH (port 22) | Elasticsearch HTTP (port 9200) | NA | NA | Elasticsearch (port 9200) | NA |

Updating Security Lists for Necessary Ports

Here are sample security lists for the three default subnets that are created for a VCN with related resources. This assumes the following setup:

* The Cloud Manager and file server instances are hosted on Public Subnet evQs: US-ASHBURN-AD-1 (10.0.0.0/24).
* Mid-tier components (application server, Process Scheduler, and web server), Windows Client, Full-tier and Elasticsearch instances are hosted on  Public Subnet evQs: US-ASHBURN-AD-2 (10.0.1.0/24).
* Database instances are hosted on Public Subnet evQs: US-ASHBURN-AD-3 (10.0.2.0/24).

The following table lists the rules required for the security list for the first public subnet, hosting the Cloud Manager and file server instances.

The following table lists the rules required for the security list for the first public subnet, hosting the Cloud Manager and file server instances.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| # | **Source CIDR** | **IP Protocol** | **Source Port Range** | **Destination Port Ranges** |
| 1 | 10.0.0.0/24 | TCP | All | 2049 (NFS) |
| 2 | 10.0.0.0/24 | TCP | All | 111 (NFS) |
| 3 | 10.0.0.0/24 | TCP | All | 892 (NFS) |
| 4 | 10.0.0.0/24 | TCP | All | 32803 (NFS) |
| 5 | 10.0.1.0/24 | TCP | All | 2049 (NFS) |
| 6 | 10.0.1.0/24 | TCP | All | 111 (NFS) |
| 7 | 10.0.1.0/24 | TCP | All | 892 (NFS) |
| 8 | 10.0.1.0/24 | TCP | All | 32803 (NFS) |
| 9 | 10.0.2.0/24 | TCP | All | 2049 (NFS) |
| 10 | 10.0.2.0/24 | TCP | All | 111 (NFS) |
| 11 | 10.0.2.0/24 | TCP | All | 892 (NFS) |
| 12 | 10.0.2.0/24 | TCP | All | 32803 (NFS) |
| 13 | 0.0.0.0/0 | TCP | All | 22 (SSH) |

The following table lists the rules required for the security list for the second subnet, hosting the mid-tier, PeopleSoft Windows client, full-tier, and Elasticsearch.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| # | **Source CIDR** | **IP Protocol** | **Source Port Range** | **Destination Port Ranges** |
| 1 | 10.0.0.0/24 | TCP | All | 22 (SSH) |
| 2 | 10.0.0.0/24 | TCP | All | 5985 and 5986 (Winrm) 137, 138, 139, and 445 (CIFS) |
| 3 | 10.0.1.0/24 | TCP | All | * 8000 (default PIA HTTP port) * 8443 (default PIA HTTPS port) * 9033 (default Jolt Port) * 3389 (RDP port) * 9200 (default Elasticsearch port) |
| 4 | 0.0.0.0/0 | TCP | All | 3389 (RDP) |

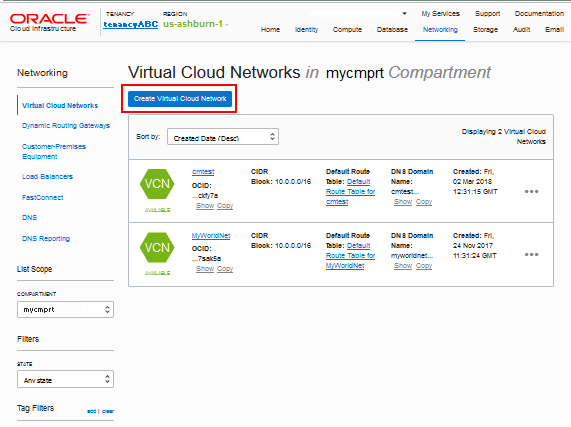
The following table lists the rules required for the security list for the third subnet, hosting the database.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| # | **Source CIDR** | **IP Protocol** | **Source Port Range** | **Destination Port Ranges** |
| 1 | 10.0.0.0/24 | TCP | All | 22 (SSH) |
| 2 | 10.0.0.0/24 | TCP | All | 1521 (database port) |

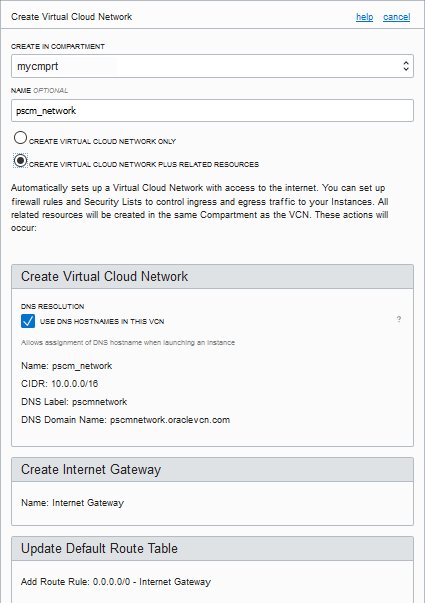
### Creating a VCN with Related Resources

To create a VCN with related (default) resources:

1. In the Compute Console, select Networking, Virtual Cloud Networks.
2. Click **Create Virtual Cloud Network**.



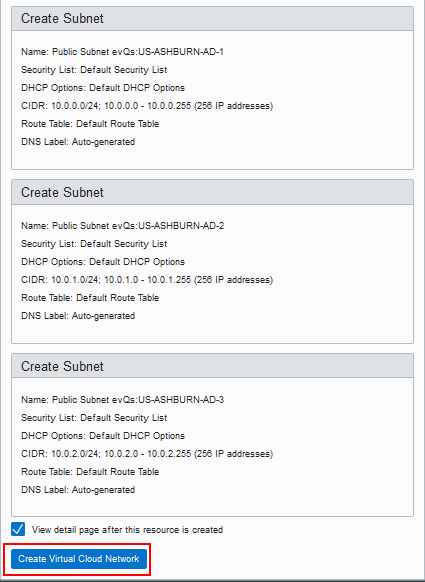
On the Create Virtual Cloud Network dialog box, select the compartment you want to work in from the drop-down list, which is mycmprt in this example.



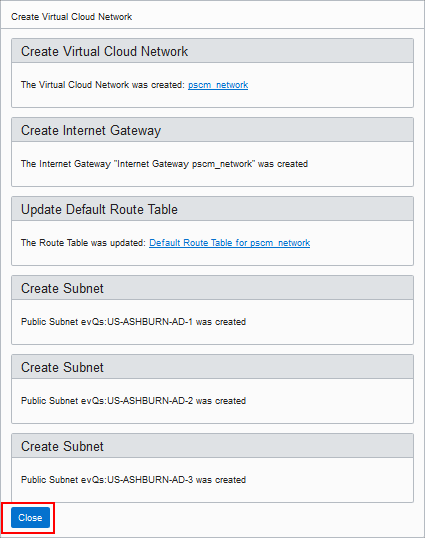
1. Enter a name for the VCN, such as pscm\_network. Make a note of the name, as you will need it when creating the Cloud Manager instance.
2. Select the option **CREATE VIRTUAL CLOUD NETWORK PLUS RELATED RESOURCES**, as shown in this example, to create a VCN with default components, including three public subnets, an Internet gateway, a route table, and a security list.

If you prefer to define the resources for the VCN, select the option **CREATE VIRTUAL CLOUD NETWORK ONLY**. After you create the VCN, create the necessary components to fit your requirements.

1. Select the option **USE DNS HOSTNAMES IN THIS VCN**. The Create VCN process assigns a DNS label based on the VCN name.
2. Click **Create Virtual Cloud Network**.



When the network is ready, click **Close**.

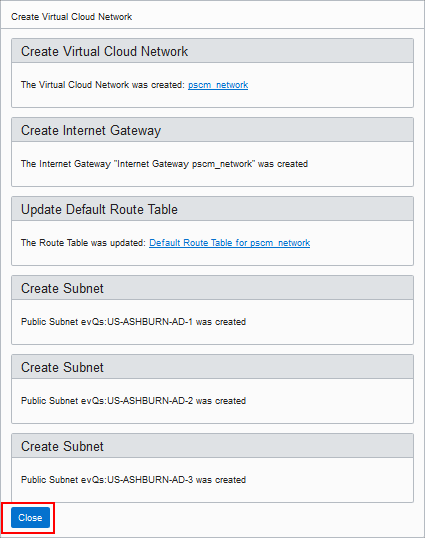


1. On the Virtual Cloud Networks page, select the VCN name to review the details.
2. Update the security lists to allow all necessary ports.

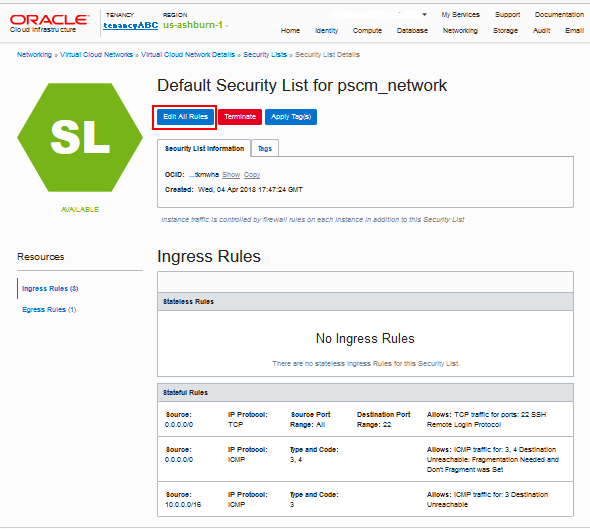
Creating Subnets and Editing Security Lists

This section gives an example of creating a subnet with a security list that allows access between the Cloud Manager instance and file server instance. The subnet where Cloud Manager is created (and where NFS also gets provisioned) needs to allow the ingress of four NFS-related TCP ports (2049, 111, 892, 32803). This will ensure that NFS mounts will work across Linux and Windows in all the subnets within the VCN. For simplicity, the source in the stateful ingress rules can be the whole VCN’s CIDR.

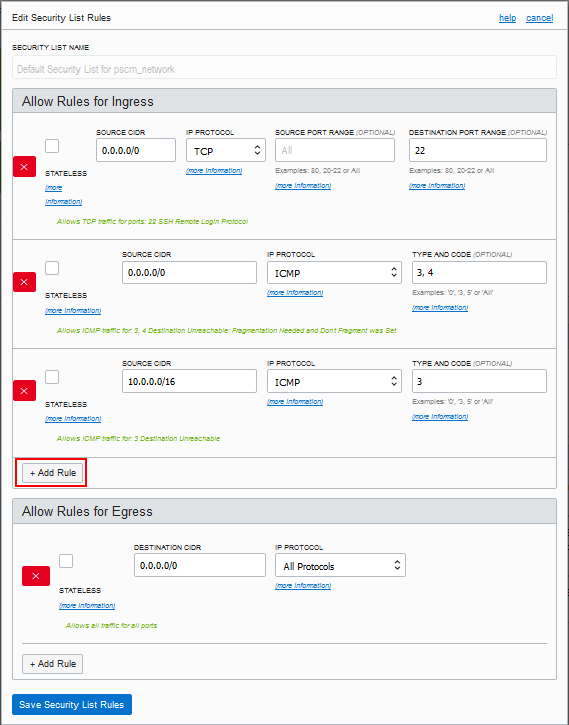
1. If you want to add more public or private subnets, go to the details page for the VCN and click **Create Subnet**.



If you want to modify or add a security list to one of the subnets, select the subnet. On the details page, click **Edit All Rules**



On the Edit Security List Rules dialog box, under Allow Rules for Ingress, click **Add Rule**

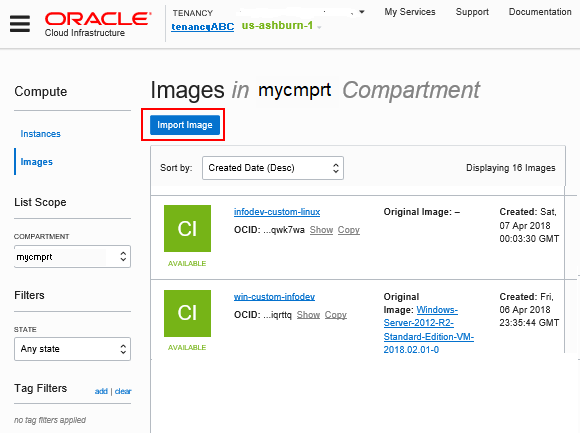


1. Enter 10.0.0.0/16 for the Source CIDR. This is the same as the CIDR for the VCN.
2. Accept TCP as the protocol.
3. Enter 2049 for the Destination Port Range.
4. Repeat steps 3 through 6 for NFS-related ports 111, 892, 32803. Also add a rule for the HTTP port, default 8000, and any other ports you need.
5. When you have added all the security rules, click **Save Security List Rules**.
6. Specify this subset when you create the Cloud Manager and file server instances.

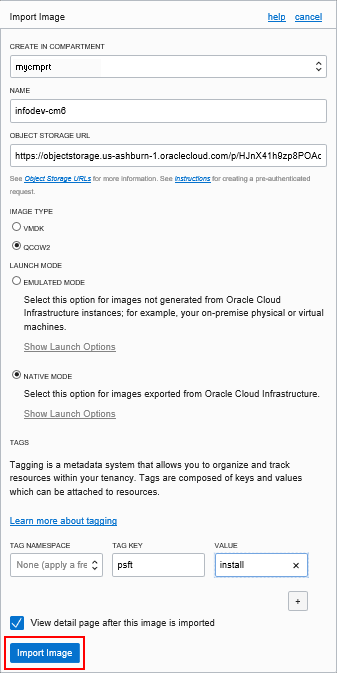
## **Importing the Cloud Manager Image**

In the Compute Console, import the image from Object Storage as follows:

1. Click the **Import Image** button at the top of the page.



On the Import Image dialog box, select the compartment where you want to create the image from the Create in Compartment drop-down list, mycmprt in this example.

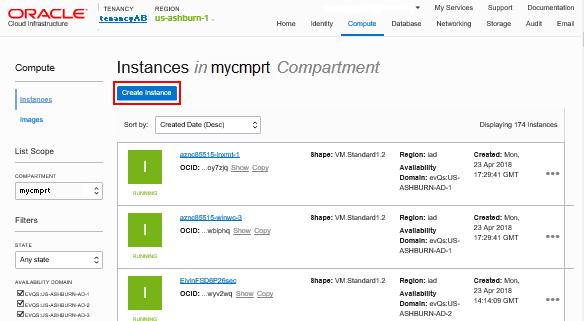


1. Enter a name for the image, infodev-cm6 in this example.
2. Select Linux from the Operating System drop-down list.
3. Enter the URL to the image in the Object Storage URL field.
4. Select the QCOW2 Image Type.
5. Under Launch Mode, select Native Mode.
6. Click **Import Image**.
7. When the status for the image displays Available, select Show or Copy for the OCID. Make a note of the OCID, as you will need this when creating the Cloud Manager instance.

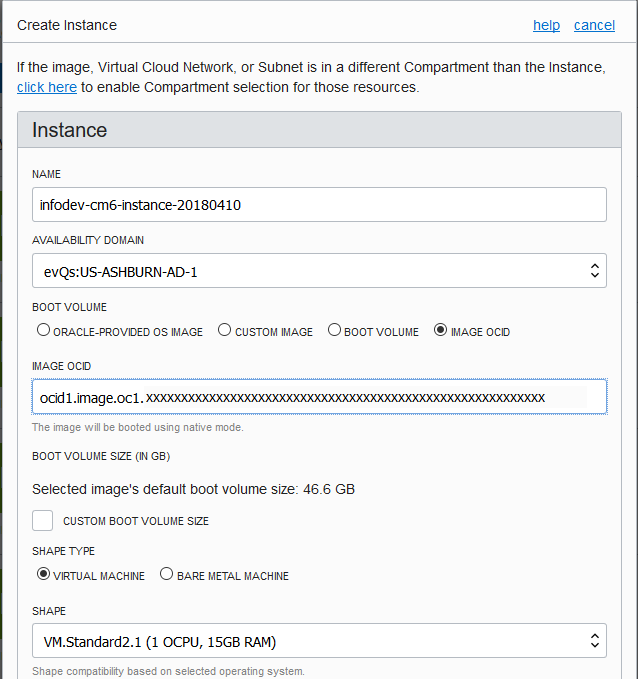
## **Provisioning the Cloud Manager Instance**

Use the Compute Console to configure the VM instance from the Cloud Manager image.

1. In the Compute Console, select **Instances**, and select your compartment.
2. Click **Create Instance**.



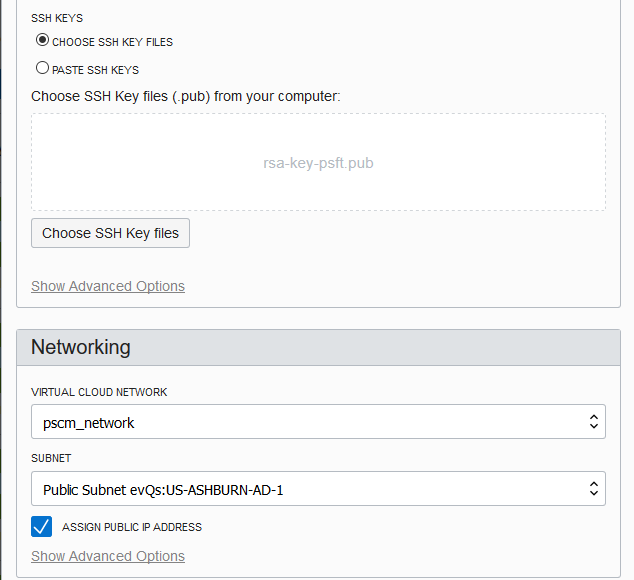
On the Create Instance dialog box, enter a name for the instance, infodev-cm6-instance in this example.



1. Select an Availability Domain from the drop-down list.
2. Select **Image OCID** in the Boot Volume area.
3. Enter the OCID that you saved for the Cloud Manager image.
4. Select **Virtual Machine** as the Shape Type, and select a shape.

The minimum shape required for the Cloud Manager image is VM.Standard2.1 (1 OCPU, 15GB RAM).

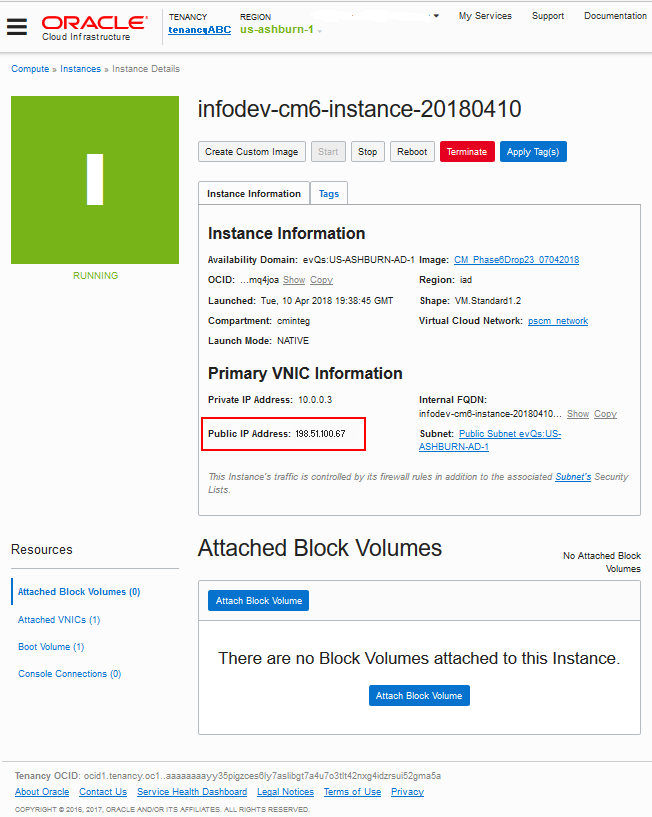
1. In the SSH Keys area, select the option Choose SSH Key Files, and browse to the location where you saved the public SSH key.



1. From the Virtual Cloud Network drop-down list, select the VCN you created.
2. From the Subnet drop-down list, select the public subnet you want to use for the Cloud Manager instance.

Ensure that Cloud Manager is deployed on a public subnet to allow access from the Internet.

1. Verify that the **Assign Public IP Address** option is selected.
2. Click **Create Instance**.
3. Monitor the instance creation on the Compute Console Instances page. When the instance creation is complete, as indicated by status Running, make a note of the Public IP address for the instance.



## **Logging in to the Linux VM**

The Cloud Manager image includes a setup script that you run in the Linux VM instance created in the previous section. The instance can be accessed from a Microsoft Windows machine using an SSH client such as PuTTY, or directly from a Linux machine. The setup script prompts you for several user IDs and passwords, as mentioned in the section [What Do You Need](https://www.oracle.com/webfolder/technetwork/tutorials/obe/cloud/compute-iaas/install_peoplesoft_cloud_manager_oci/cloud-manager-install-oracle-cloud-infrastructure.html#overview). Make a note of your input for later reference.

### Logging in to the Linux VM from a Linux or UNIX System

1. Enter the following command:

ssh -i <path\_to\_private\_key\_file>/<private\_key\_name> -o ServerAliveInterval=5 -o ServerAliveCountMax=1 opc@<public\_ip\_address\_of\_instance>

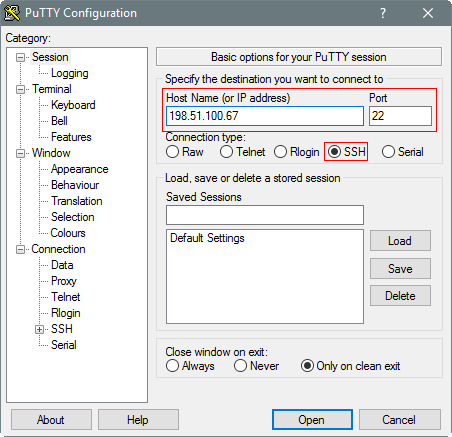
1. If you don't know the public IP address of your instance, you can find it by going to the Compute console and selecting the Instances tab. Select your compartment, and view the instance details page. The Primary VNIC information section includes the Public IP Address.
2. If you entered a passphrase when creating your SSH key pair, enter the passphrase when prompted.
3. The first time you connect to your instance, the SSH utility prompts you to confirm the public key. In response to the prompt, enter **yes.**

### Logging in to the Linux VM from a Microsoft Windows System

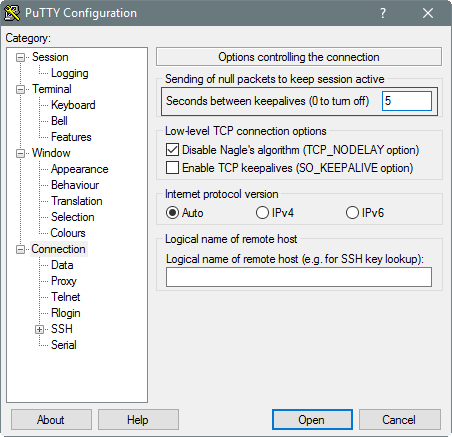
1. Start PuTTY. The PuTTY Configuration window is displayed, showing the Session panel.
2. In the **Host Name (or IP address)** field, enter the public IP address of your instance.

**Note.** If you don't know the public IP address of your instance, you can find it by going to the Compute console and selecting the Instances tab. Select your compartment, and view the instance details page. The Primary VNIC information section includes the Public IP Address.

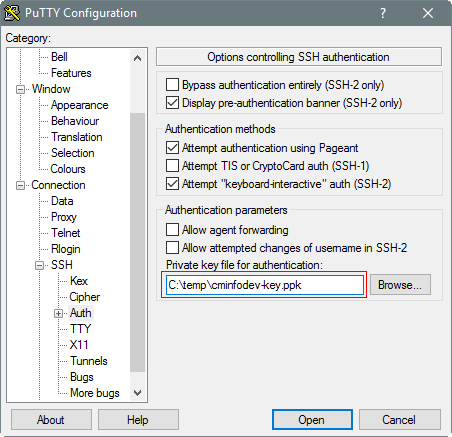
1. In the **Connection type** field, select **SSH** if it is not already selected.



In the **Category** pane, click **Connection**. Enter **5** in the **Seconds between keepalives (0 to turn off)** text box.



1. In the **Category** pane, expand **SSH,** and then click **Auth.** The Auth panel is displayed.
2. In the **Private key file for authentication** field, click **Browse** and select the private key file that you saved earlier, **cminfodev-key.ppk** in this example.



1. In the Category tree, click **Session.**

The Session panel is displayed.

1. In the **Saved Sessions** field, enter a name for this connection configuration, and then click **Save.**
2. Click **Open**to open the connection.

The PuTTY Configuration window is closed and the PuTTY window is displayed.

1. When prompted for a user name, enter **opc**.
2. Enter the passphrase you had provided for your SSH key pair.
3. The first time you connect to your instance, the PuTTY Security Alert window is displayed, prompting you to confirm the public key. Click **Yes** to continue.

## **Generating API keys**

Access the Cloud Manager image and use the script provided for generating API keys.

1. Access the Linux VM for the Cloud Manager instance and sign in as user opc.
2. Change directory to /home/opc/bootstrap.
3. Run the create\_keys script.

sh create\_keys.sh

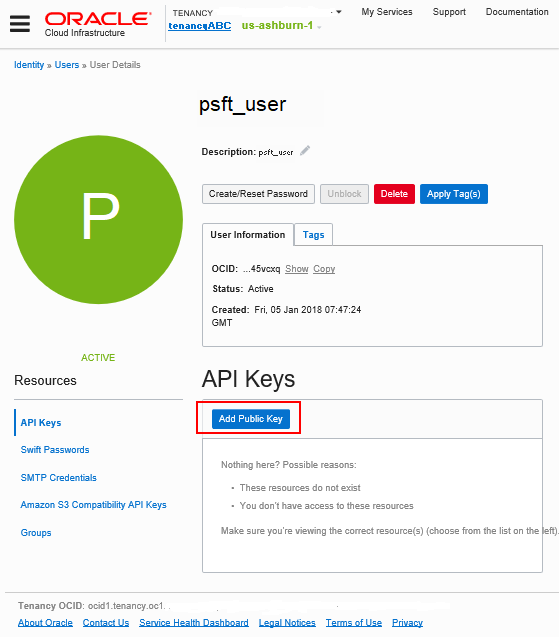
1. Enter a directory to store the public and private keys, such as /home/opc/apikeys.
2. \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*
3. \*                 API Signing Key Generation                     \*
4. \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Enter the absolute path to save API Signing key pair (e.g /home/opc/.oci):**/home/opc/apikeys**

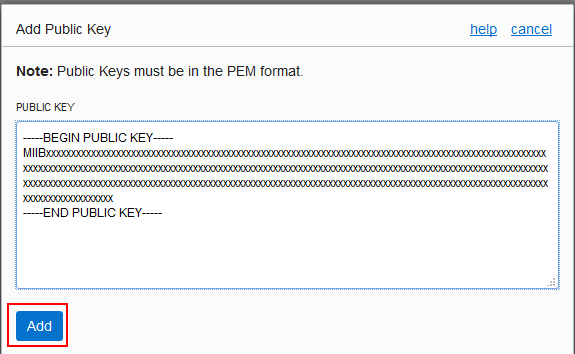
1. Enter a passphrase twice for the keys. The passphrase must not include any spaces. Be sure to remember the passphrase, as you will need to supply it when running the script in the next section.
2. Enter a pass phrase for /home/opc/apikeys/oci\_api\_key.pem (empty for no passphrase):  
   Re-enter pass phrase for /home/opc/apikeys/oci\_api\_key.pem:  
   Generating RSA private key, 2048 bit long modulus
3. .....................................+++
4. ................................................................+++
5. e is 65537 (0x10001)
6. Success: API Signing private key generated successfully
7. writing RSA key

Success: API Signing key pair generated successfully.

1. When the key generation is complete, go to the directory where the script saved the keys. Open the public key in a text editor, and copy it.
2. In Compute Console, select Identity, Users, and then your user name.
3. Under API Keys, click **Add Public Key**.



Paste the key contents into the field and click **Add**. The key appears on the user details page.



Save the full path, names, and passphrase for the public and private API keys. You will use them in the section Running the Cloud Manager Instance Configuration Wizard.

## **Setting Up Cloud Manager on the Linux VM**

### Gathering Information for the Cloud Manager Instance Configuration Wizard

The Cloud Manager Instance Configuration Wizard prompts you for account and instance information. This section describes how to gather the information before you run the script. Alternatively, you may prefer to have a Compute Console window open as you run the script, and copy the necessary OCIDs as needed.

1. On the Compute Console user page, copy the user OCID.
2. Click on the TENANCY name on top of the Compute window to get the list of regions. Look for the region with (Home Region) next to it.
3. On the same page, copy the Tenancy OCID.
4. To obtain the API version, see the Oracle Cloud Infrastructure API documentation. For example, the API version is listed on this page:

https://docs.us-phoenix-1.oraclecloud.com/api/#/en/iaas/20160918/

Running the Cloud Manager Instance Configuration Wizard

Before beginning this procedure, ensure that you have the account information and OCIDs mentioned in the previous section.

1. Connect to the Cloud Manager instance with SSH if necessary.

If you are using PuTTY to connect on Microsoft Windows, select **Session**, enter the IP address for the Cloud Manager instance in the Host Name field, and then click **Open**.

1. Change directory to /home/opc/bootstrap and run this command as a root user:

sudo sh psft\_cm\_bootstrap.sh

1. Enter the number for your home region to create the Compute instance, which is Phoenix in this example.
2. \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*
3. \* Welcome to Cloud Manager Instance Configuration Wizard \*
4. \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*
5. Reading configuration file... [ OK ]
6. Retrieving fqdn for the instance [ OK ]
7. Select your Home Region
8. 1. ASHBURN (IAD)
9. 2. PHOENIX (PHX)
10. 3. FRANKFURT (FRA)
11. 4. Other region

Enter region [1-4]: 2

1. Enter the OCIDs for your tenancy and your user account.
2. Enter your Tenancy OCID: ocid1.tenancy.oc1.xxxxxxxxxxxxxxxxxxxxxxxxx

Enter your User OCID: ocid1.user.oc1.xxxxxxxxxxxxxxxxxxxxxxxxxxxxx

1. Enter the full path and name for your API Signing private key:

Enter the path to your API Signing Private Key: /home/opc/oci\_api\_key.pem

1. Enter the passphrase twice for your API Signing private key:
2. Enter the passphrase of your API Signing Private Key (empty for no passphrase):

Re-Enter the passphrase of your API Signing Private Key:

1. Enter the password twice for the Cloud Manager administrator, CLADM.
2. Enter the new Domain Boot user password for user CLADM.
3. Ensure that the password contains only alphanumeric characters
4. and is no more than 32 characters in length :

Re-Enter the new Domain Boot user password for user CLADM:

1. Enter the password twice for the PeopleSoft connect ID, people, following the requirements in the prompt.
2. Enter the new PeopleSoft Connect ID password for user people. Ensure that
3. the password contains only alphanumeric characters   
   and is at least 6 and no more than 30 characters in length:

Re-Enter the new PeopleSoft Connect ID password for user people:

1. Enter the PeopleSoft access ID, SYSADM, and enter the password twice, following the requirements in the prompt.

SYSADM is the only valid access ID for Cloud Manager.

Enter the PeopleSoft Access ID [SYSADM]: **SYSADM**

Enter the new PeopleSoft Access password for user SYSADM:  
Ensure that the password contains only alphanumeric characters and  
is between 6 and 30 characters in length:

Re-Enter the new PeopleSoft Access password for user SYSADM:

1. Enter the password twice for the SYS or SYSTEM database users, following the requirements in the prompt.

Enter a new PeopleSoft database admin users [SYS/SYSTEM] password.  
Ensure that the password is between 8 and 30 characters in length  
with at least one lowercase letter, one uppercase letter, one number  
and one special character (\_,-,#):  
Re-Enter the new Database Admin Password:

1. Enter the password twice for the Oracle WebLogic administrator user, system, following the requirements in the prompt.

Enter a new WebLogic Server Admin user [system] password. Ensure that  
the password is between 8 and 30 characters in length with at least  
one lowercase letter, one uppercase letter, one number or one  
one special character (!@#$%^&):  
Re-Enter a new WebLogic Server Admin user [system] password:

1. Enter the password twice for the PeopleSoft Web Profile user, PTWEBSERVER:

Enter the new password for Web Profile user PTWEBSERVER.  
Ensure that the password contains only alphanumeric characters and  
is between 8 and 30 characters in length:  
Re-Enter the password for Web Profile user PTWEBSERVER:

1. Enter the password twice for the Integration Gateway user, administrator, following the requirements in the prompt:

Enter the new password for Integration Gateway user administrator.  
Ensure the password contains only alphanumeric characters and  
is between 8 and 30 characters in length:  
Re-Enter the new password for Integration Gateway user administrator:

1. If you want to configure advanced options answer *y* (yes) to the following prompt, and then use the next prompts to change the default database name and port numbers.

If you want to accept the default options, answer *n* (no) and continue with step 15.

Do you want to configure advanced options [y|N]: y

Enter your API Version [20160918]:

Enter a new PeopleSoft database name. Please ensure that the database

name start with a letter and contains only uppercase letters

and numbers and is no more than 8 characters in length [CMPSDB]:

Enter the HTTP port. Please ensure that port value is between 1024 and 65535 [8000]:

Enter the HTTPS port. Please ensure that port value is between 1024 and 65535 [8443]:

Enter the JOLT port. Please ensure that port value is between 1024 and 65535 [9033]:

Enter the WSL port. Please ensure that port value is between 1024 and 65535 [7000]:

1. Review the summary information. Answer *y* to continue, or *n* to change your responses.

If you did not configure the advanced options, the summary shows the default values for the database name and port numbers. Be sure to verify these values before continuing.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Cloud Manager Instance Configuration Summary

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Home Region : us-phoenix-1

Deployment Region : us-ashburn-1

Tenancy OCID : ocid1.tenancy.oc1.xxxxxxxxxxxxxxxxxxxxxxxxx

Tenancy name : tenancyABC

User OCID : ocid1.user.oc1.xxxxxxxxxxxxxxxxxxxxxxxxxxx

Username : psft\_user@example.com

API Signing Private Key path : /home/opc/oci\_api\_key.pem

API Signing Public Key fingerprint : c0:a0:38:17:8d:11:03:57:a3:4f:6f:07:e1:70:9d:90

API Version : 20160918

Name of the database : CMPSDB

HTTP port : 8000

HTTPS port : 8443

JOLT port : 9033

WSL port : 7000

Cloud Manager hostname : infodev-cm6-instance-20180410

PIA Authorisation token : .subnet1.pscmnetwork.oraclevcn.com

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Cloud Manager Bootstrap Input Validation Summary

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

User data retrieval from OCI : SUCCESS

Tenancy data retrieval from OCI : SUCCESS

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Are you happy with your answers? [y|n|q]:y  
  
\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\* \*

\* Cloud Manager provisioning started. \*

\* Please check /home/opc/bootstrap/CloudManagerStatus.log file for status \*

\* \*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. Monitor the configuration process status by reviewing the log file /home/opc/bootstrap/CloudManagerStatus.log.

The configuration process takes several minutes. When the process completes successfully, the same log file includes the Cloud Manager URL to sign in to the PeopleSoft Pure Internet Architecture (PIA) in a browser.

**Note**. The term bootstrap is sometimes used to refer to the Cloud Manager Instance Configuration wizard.

The Cloud Manager instance configuration log files are found in these locations:

* /home/opc/bootstrap/CloudManagerStatus.log — Input logs for the Cloud Manager Instance Configuration wizard
* /home/opc/bootstrap/psft\_opc\_setup.log — Cloud Manager provisioning log
* /home/psadm2/psft/data/cloud/cmlogs/BOOTSTRAP\_LOGS/\* — PeopleSoft Cloud Administrator logs related to processes such as file server creation
* /opt/oracle/psft/dpks/setup/psft\_dpk\_setup.log — Detailed Puppet log for the Cloud Manager installation.

### Reviewing the Cloud Manager Input Validation Details

The table in this section lists input validation messages you may see and their meaning.

|  |  |  |  |
| --- | --- | --- | --- |
| # | **Message Value** | **Reason** | **Comment** |
| 1 | SUCCESS | The values supplied for the Compute user OCID and tenancy OCID are correct. | NA |
| 2 | FAILURE | One or more of the following inputs is wrong:   * Home region * User OCID * Tenancy OCID * API Signing Private Key path * Passphrase of API Signing Private Key * API version | * If the validation summaries for both User data retrieval from OCI and Tenancy data retrieval from OCI show FAILURE, verify the correct values for all of the inputs. * If the validation summary shows FAILURE for one while the other shows SUCCESS, the failure is probably due only to the one showing failure:   + If User data retrieval from OCI has status FAILURE while Tenancy data retrieval from OCI has status SUCCESS, then the User OCID provided is likely the reason for the failure.   + If Tenancy data retrieval from OCI has status FAILURE while User data retrieval from OCI has status SUCCESS, then the Tenancy OCID provided is likely the reason for the failure. |

## **Accessing the Cloud Manager Instance in a Browser**

1. To locate the URL for Cloud Manager, review the /home/opc/bootstrap/CloudManagerStatus.log file created after the successful completion of the Cloud Manager Instance Configuration Wizard.

The URLs for Cloud Manager Pure Internet Architecture (PIA) are included at the end of the file. For example:

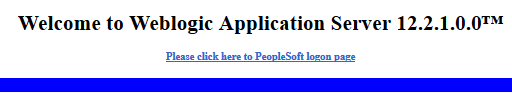
CM installed successfully  
Cloud Manager PIA URL: http://infodev-cm6-instance-20180410.subnet1.pscmnetwork.oraclevcn.com:8000  
Cloud Manager PIA SSL URL: https://infodev-cm6-instance-20180410.subnet1.pscmnetwork.oraclevcn.com:8443

1. To access the URL over the Internet, the DNS for the instance must be successfully resolved.

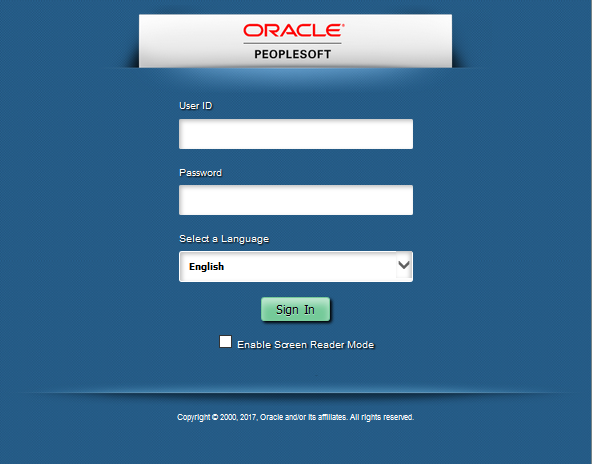
If you do not have a public DNS, edit the etc\hosts file (for example, C:\Windows\System32\drivers\etc\hosts on Microsoft Windows 10) on the machine from which you want to access the Cloud Manager URL. To modify the file, add a line with the Public IP address and fully-qualified domain name for the Cloud Manager instance, such as:

198.51.100.67 infodev-cm6-instance-20180410.subnet1.pscmnetwork.oraclevcn.com

1. Enter the Cloud Manager URL in a browser. You see a window for Weblogic Application Server 12.2.1.0.0.



Click the link **Please click here to PeopleSoft logon page** to display the Cloud Manger sign in window.



**Note.** Oracle strongly recommends that you change the default PeopleSoft Pure Internet Architecture (PIA) user passwords, because the Cloud Manager instances are on the public Internet.

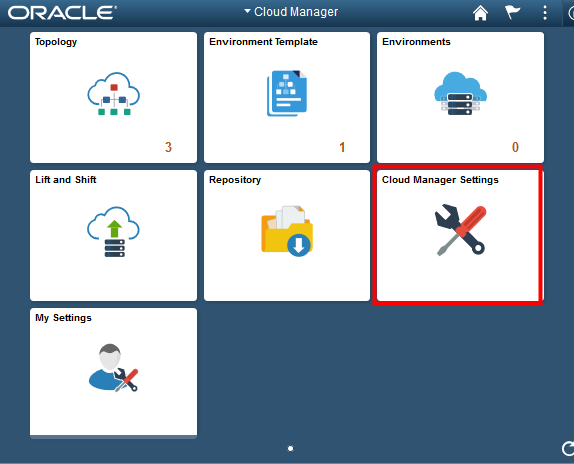
## **Specifying the Cloud Manager Settings**

### Using the Cloud Manager Settings Page

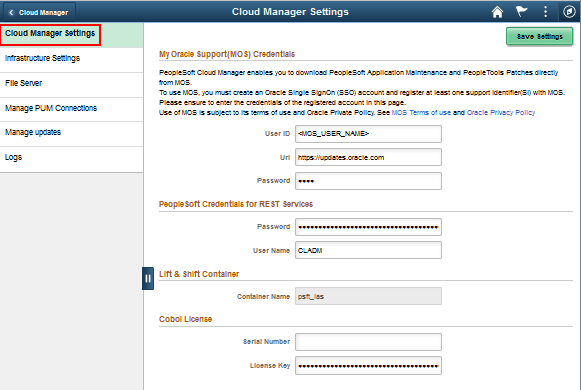
Use the Cloud Manager Setting page to specify user IDs and other information before using Cloud Manager to create topologies and templates.

1. Sign in to Cloud Manager in a browser using the Cloud Administrator user ID and password.
2. On the home page, select the **Cloud Manager Settings** tile.

Note that the Cloud Manager Settings tile appears only for users who sign in with the Cloud Administrator user ID

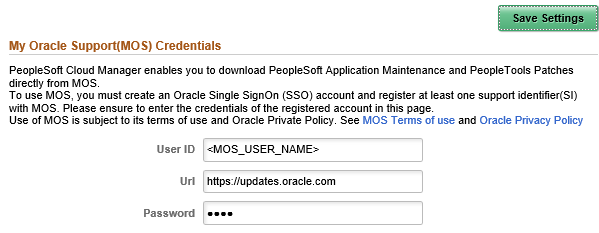


Select **Cloud Manager Settings** from the left-hand panel.



In the My Oracle Support (MOS) Credentials section, verify that the user ID and password for your My Oracle Support account are correct.

* **User ID**: This field displays the Compute account ID. Do not change this value.
* **Url**: This field displays the URL https://updates.oracle.com for access to My Oracle Support. Do not change this value.
* **Password**: Enter the password for your My Oracle Support account.



In the PeopleSoft Credentials for REST Services section, verify the delivered Cloud Manager Administrator user name, CLADM, and password. This information is based on the input to the Cloud Manager Instance Configuration wizard.

This refers to the standard Integration Broker REST services that are available in the Cloud Manager instance. These REST services are used internally by Cloud Manager modules to send and receive the results of long-running, asynchronous activities.



In the Lift & Shift Container section, the container name is included for information.



If you have a license for a COBOL compiler, enter your COBOL serial number and license key in the Cobol License section (optional).

**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.

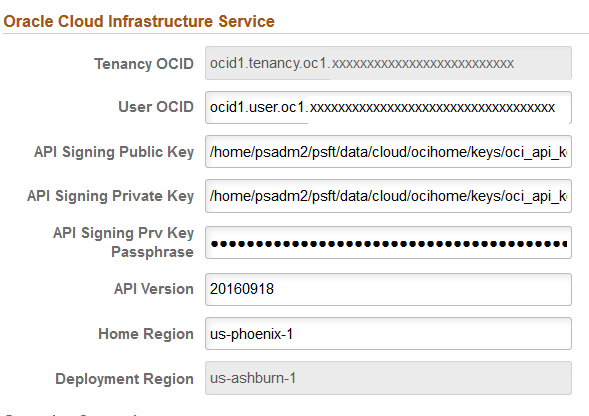


1. Click **Save Settings** at the top of the page if you make any changes.

Using the Infrastructure Settings Page

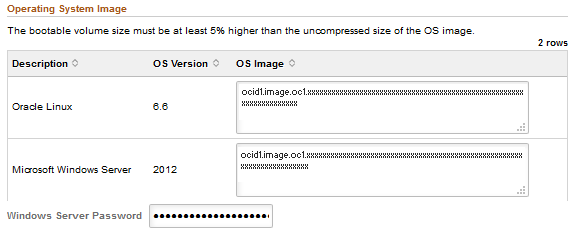
Use the Infrastructure Settings page to verify account, instance, and operating system information.

1. Select **Infrastructure Settings** from the left-hand panel.
2. In the Oracle Cloud Infrastructure Service section, the tenancy OCID and Deployment Region that you supplied when provisioning the instance are given for information.



1. Verify the following information that you supplied when running Cloud Manager Instance Configuration wizard:
   * User OCID
   * Full path and name for the API Signing Public Key
   * Full path and name for the API Signing Private Key
   * API Signing Private Key passphrase
   * API Version
   * Home Region
2. Enter the OCIDs for the Oracle Linux and Microsoft Windows operating system images that Cloud Manager will access.

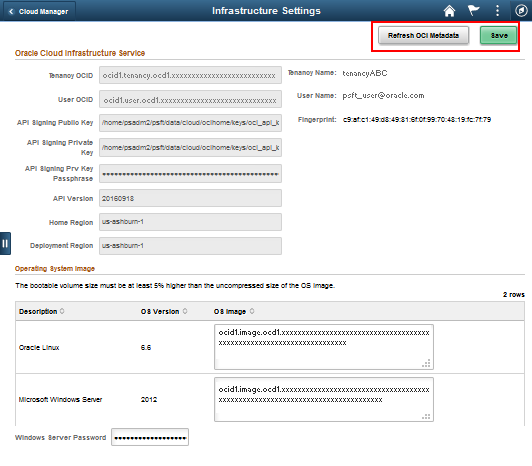
The following example shows the Operating System Image section after specifying two images, for Oracle Linux 6.6 and Microsoft Windows Server 2012. The Microsoft Windows image is used for Windows client components with PUM environments.



1. In the Windows Server Password field, update the value with the password that you specified when creating the Windows custom image.

See the section Obtaining an Updated Microsoft Windows Image for Cloud Manager.

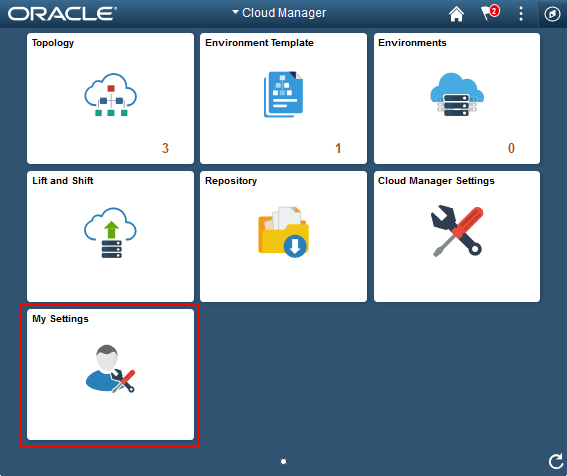
1. Click **Save** and then **Refresh OCI Metadata** at the top of the page if you make any changes, to refresh the metadata related to the operating system images. Wait a few minutes for the data to be refreshed before creating a file server.



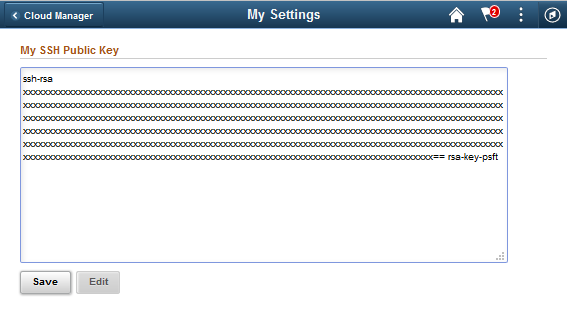
### Using the My Settings Page

End users can enter or edit their public SSH key on the My Settings page. After adding this SSH key, Cloud Manager will inject the key into the Linux VM of any PeopleSoft environment that you provision.

1. From the Cloud Manager home page, click the My Settings tile.



To enter a new SSH Public key, enter the text in the My SSH Publish Key field and click **Save**.



1. To edit or replace an existing key, enter the text for the key, and then click **Save**.
2. Click **Edit**, and change or replace the text.
3. Click **Save** again.

## **Creating a File Server**

### Creating a New File Server

Use the Cloud Manager Settings tile to create a file server, which is used with the Cloud Manager Repository feature to automatically download updates. This section describes how to create a new file server for a Cloud Manager instance. This section assumes that an Oracle Linux image is available and specified under Operating System Image in the Settings page described previously.

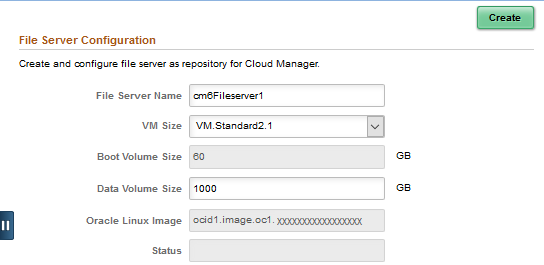
**Note**. If you modified or created non-default VCN resources, be sure that the security list for the subnet on which Cloud Manager is installed includes rules to allow access for NFS-related ports before file server creation. Without this file server creation will fail. The required NFS ports are 2049, 111, 892, and 32803.

See the information on Cloud Manager Settings - File Server page in the PeopleSoft Cloud Manager product documentation, [PeopleSoft Hosted Online Help](http://docs.oracle.com/cd/E17566_01/epm91pbr0/eng/psbooks/psft_homepage.htm).

1. Sign in to Cloud Manager in a browser using the Cloud Administrator user ID and password.
2. On the home page, select the **Cloud Manager Settings** tile.

Note that the Cloud Manager Settings tile appears only for users who sign in with the Cloud Administrator user ID.

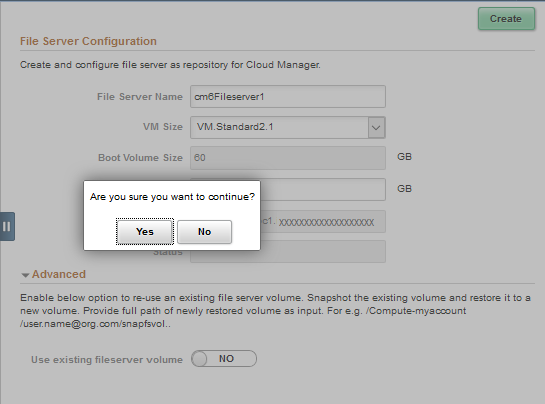
1. Select File Server from the panel on the left.
2. On the File Server Configuration page, enter a name, such as cm6Fileserver1. Enter a name with alphanumeric characters, and no special characters.



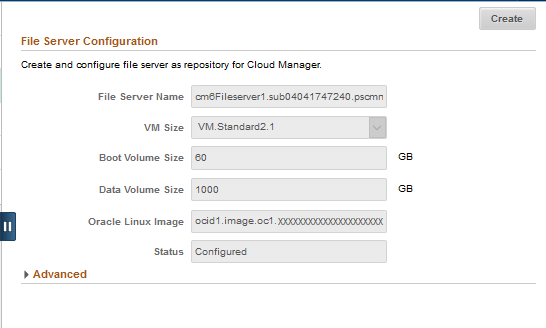
1. Select a **VM Size** from the drop-down list, such as VM.Standard2.1.
2. The **Boot Volume Size** is specified when setting up the image.
3. Enter a value in GB for the **Data Volume Size**. Enter a value large enough to accommodate images you plan to download, such as 1000 GB.
4. The **Oracle Linux Image** OCID is specified when setting up the image.
5. In the Advanced section, select NO for **Use existing fileserver volume**.

See the next section for information on reusing an existing file server volume

1. Click **Create**.
2. Click **Yes** on the dialog box with **Are you sure you want to continue?**



The file server is ready when the Status changes to Configured.



### Ensuring File Server Access

You can access the Cloud Manager VM in an SSH session using your personal public and private SSH key pair, as previously mentioned. To log in to the file server VM, you access the Cloud Manager VM with SSH, then initiate another session using the Cloud Manager private SSH key, which is added by the Cloud Manager deployment process. Use the following steps to access the file server VM from the Cloud Manager VM:

1. Log in to the Cloud Manager instance as the opc user, and supply the passphrase for your SSH public key.
2. Change to root user:

sudo su - psadm2

1. Change directory to /home/psadm2/psft/data/cloud/ocihome/keys.
2. Locate the file cm\_adm\_pvt\_key.pub, which contains the SSH public key of the Cloud Manager instance.

Note that cm\_adm\_pvt\_key.pub is the SSH key that Cloud Manager uses to connect to instances that it provisions, and is not the same as your personal public SSH key. The corresponding private SSH key is cm\_adm\_pvt\_key.

1. To access the existing file server VM, start an SSH session with this command:

ssh -i cm\_adm\_pvt\_key opc@<file\_server\_name>

If you wish to retain and access all downloaded packages on the file server VM independently, you must manually add your personal public SSH key to the file server after you create it in Cloud Manager. This applies to both new file servers and file servers you create from existing file server storage volumes. Add the personal public SSH key text to a new line in the /home/opc/.ssh/authorized\_keys file on the file server VM. After adding the personal public SSH key, use the matching private SSH key to access the file server VM.

For more information on working with file servers, see the PeopleSoft Cloud Manager online documentation on [PeopleSoft Hosted Online Help](http://docs.oracle.com/cd/E17566_01/epm91pbr0/eng/psbooks/psft_homepage.htm).

### Removing the File Server in Case of Failure

If the file server creation fails due to any issues, perform the following steps to clean up and recreate the file server. This section assumes that the Cloud Manager VM is up and running.

1. Sign in to Cloud Manager in a browser using the Administrator user ID and password, and select the Cloud Manager Settings tile.
2. Select File Server from the panel on the left. If the file server creation has failed, a **Delete** button will be enabled at the top right of the File Server Configuration page, and the Status will be Failed.
3. For information about the failure, select the link beside **Status**Click here for more info to see the error description.

Alternatively, select Logs from the panel on the left, and search for the term "fileserver" for example:

1. Click **Delete** to clean up the failed file server instance, and click **Yes** on the message box with "Are you sure you want to continue?"

Verify that the file server was deleted from the instances on the Instances tab of the Compute console.

1. If the delete action failed, as indicated by status Deletion Failed, click the **Delete** button again.
2. You see a message explaining that subsequent attempts to delete the file server will only delete the file server configuration details that are saved in Cloud Manager. You must also delete the file server instance and storage volumes manually before continuing. Click **Yes** to continue.

To delete the instance manually, sign in to the Compute console, and locate the file server instance on the Instances tab. Select Delete from the options menu.

1. When you have deleted the file server, you can crate a new file server. Enter and save the correct information for the Linux OS image on the Settings page in the Operating System image section, and then return to the File Server Configuration page, which will have the **Create** button enabled. Enter the required input and try to create the file server again.

## **Reviewing Cloud Manager Ports**

The following table lists the ports used by the Cloud Manager configuration.

|  |  |  |  |
| --- | --- | --- | --- |
| # | **Port Name** | **Value** | **Comment** |
| 1 | RDP | 3389 | Required for Remote Desktop access to Windows VM. |
| 2 | NFS processes | 2049, 111, 892, 32803 | Required\* |
| 3 | Winrm | 5985 and 5986 | Winrm is a Windows administration protocol used by Cloud Manager to connect remotely to the Windows VMs. See the tutorial Creating a Windows Custom Image for PeopleSoft Cloud Manager in Oracle Cloud Infrastructure. |
| 4 | CIFS process | 137, 138, 139, and 445 | Common Internet File System (CIFS) is a protocol used for transferring files from the Windows VMs to the Cloud Manager VM. |
| 5 | HTTP | 8000 (default) | For security reasons Oracle recommends that you do not use the default HTTP port number. Change it in Cloud Manager Instance Configuration Wizard. |
| 6 | HTTPS | 8443 (default) | For security reasons Oracle recommends that you do not use the default HTTPS port number. Change in Cloud Manager Instance Configuration Wizard. |
| 7 | WSL | 7000 (default) | Change in Cloud Manager Instance Configuration Wizard if desired. |
| 8 | JOLT | 9033 (default) | Change in Cloud Manager Instance Configuration Wizard if desired. |
| 9 | Database port | 1522 (default) | None |
| 10 | webserver\_admin\_port | 7700 (default) | None |
| 11 | webserver\_http\_port | 7740 (default) | None |
| 12 | webserver\_https\_port | 7743 (default) | None |
| 13 | OHS domain node manager port | 7500 (default) | None |
| 14 | Elasticsearch HTTP port | 9200 (default) | None |

.

\*The subnet where Cloud Manager is created (and where NFS also gets provisioned) needs to allow the ingress of four NFS-related TCP ports (2049, 111, 892, 32803). This will ensure that NFS mounts will work across Linux and Windows in all the subnets within the VCN. For simplicity, the source in the stateful ingress rules can be the whole VCN’s CIDR.

## **Reviewing Cloud Manager User, Roles, and Permission Lists**

### Understanding Cloud Manager Roles, Permission Lists, and User

Cloud Manager is delivered with these roles, permission lists, and user account:

* Delivered roles  
  + Cloud Administrator (PACL\_CAD)
  + Cloud PeopleSoft Administrator (PACL\_PAD)
  + Self-Service User (PACL\_SSC)
* Delivered permission lists  
  + Cloud Administrator Permissions (PACL\_001)
  + PeopleSoft Admin for Cloud (PACL\_002)
  + Cloud Self Service (PACL\_003)
* Delivered user account  
  The CLADM user account is associated with the Cloud Administrator role and other PeopleSoft administrative roles.

Here is a brief summary of the tasks associated with each delivered role.

The Cloud Administrator:

* Downloads and initiates the Cloud Manager image from Oracle Cloud Marketplace.
* Provisions the Cloud Manager instance in Oracle Cloud Infrastructure Compute.
* Configures the Cloud Manager Repository to auto-download required PeopleSoft Update Images (PIs) from My Oracle Support.
* Has access to all Cloud Manager tiles.
* Has the ability to add Cloud PeopleSoft Administrator and Self-Service Users.
* Can manage all environments.

The Cloud PeopleSoft Administrator:

* Creates deployment templates based on downloaded PIs or customer environments that have been cloned to template in Oracle Cloud Infrastructure Compute.
* Has access to the Topology, Environment Template, Environments, and My Settings tiles.
* Can manage all environments.

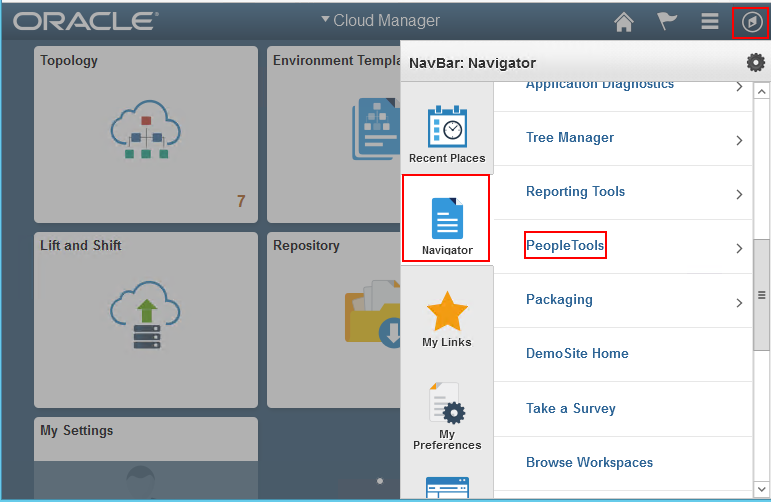
The Self-Service User:

* Creates Oracle Cloud Infrastructure Compute instances from available templates.
* Starts, stops, and deletes instances.
* Has access to the Environments and My Settings tiles.
* Can manage only his own environments.

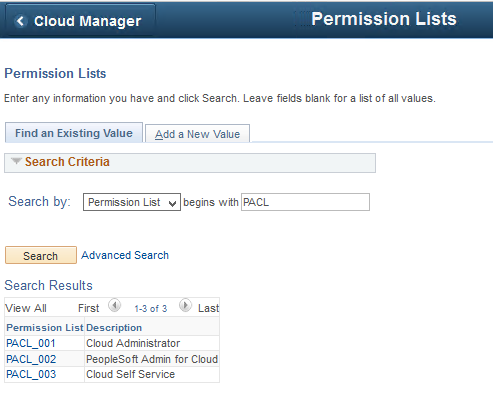
### Viewing Cloud Manager Permission Lists and Roles

To view the delivered Cloud Manager Permission Lists:

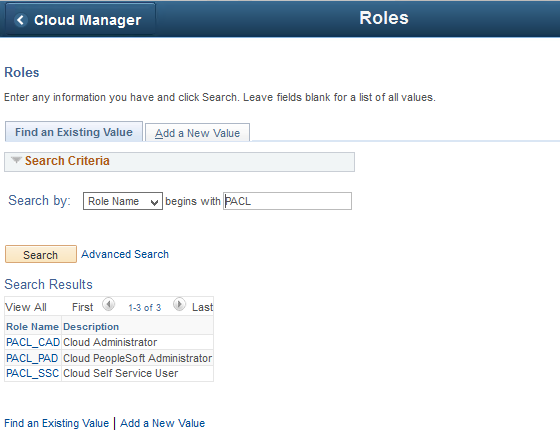
1. On the Cloud Manager home page, click the NavBar button at the top right, click the **Navigator** button, and select PeopleTools, Security, Permissions & Roles, Permission Lists from the menu.



Enter PACL in the Search By field, and click **Search** on the Permission Lists page to see the three delivered Cloud Manager Permission Lists, PACL\_001, PACL\_002, PACL\_003.

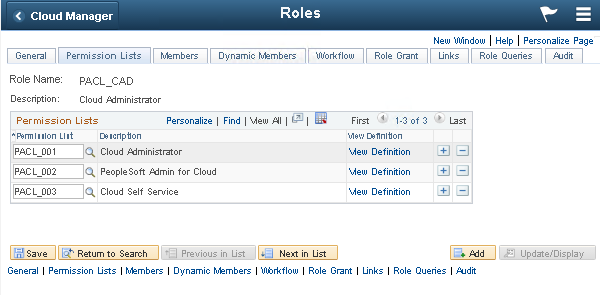


Navigate to PeopleTools, Security, Permissions & Roles, Roles, enter PACL and click **Search** to view the delivered Cloud Manager Roles, PACL\_CAD, PACL\_PAD and PACL\_SSC.



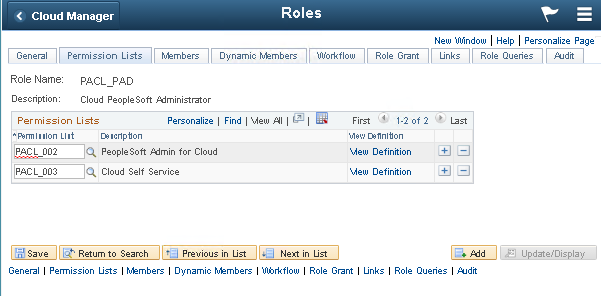
Select PACL\_CAD from the Search Results and select the **Permission Lists** tab.

The permission lists that are associated with Cloud Administrator include PACL\_001, PACL\_002, and PACL\_003.



Click **Next in List** to view the three permission lists associated with PACL\_PAD, the Cloud PeopleSoft Administrator.

The associated permission lists include the Cloud Manager permission lists PACL\_002 and PACL\_003.



Click **Next in List** to view the two permission lists associated with PACL\_SSC, the Cloud Self Service User.

The associated permission list is the Cloud Manager permission list PACL\_003.

