ORACLE

PEOPLESOFT

Understanding PeopleSoft Deployment Packages for Update Images (PeopleSoft PeopleTools 8.55)

March 2016

ORACLE

Understanding PeopleSoft Deployment Packages for Update Images (PeopleSoft PeopleTools 8.55)
SKU

Trademark Notice

License Restrictions Warranty/Consequential Damages Disclaimer

Warranty Disclaimer

Restricted Rights Notice

Hazardous Applications Notice

Third Party Content, Products, and Services Disclaimer

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

About this Documentation

This preface discusses:

- Understanding this Documentation
- Audience
- Typographical Conventions
- Products
- Related Information
- Comments and Suggestions

Understanding this Documentation

This documentation is designed to guide you through the deployment of the Oracle's PeopleSoft Deployment Packages. It is not a substitute for the documentation provided for PeopleSoft PeopleTools, PeopleSoft applications, or Oracle® VM VirtualBox.

Audience

This documentation is intended for individuals responsible for deploying the PeopleSoft Deployment Packages for Oracle's PeopleSoft application Update Images. You should have a basic understanding of virtual machines. You should have a basic understanding of the PeopleSoft system.

Typographical Conventions

To help you locate and understand information easily, the following conventions are used in this documentation:

Convention	Description
`Monospace`	Indicates a PeopleCode program or other code, such as scripts that you run during the install. Monospace is also used for messages that you may receive during the install process.

Convention	Description
Italics	Indicates field values, emphasis, and book-length publication titles. Italics is also used to refer to words as words or letters as letters, as in the following example: Enter the letter *O*. Italics are also used to indicate user-supplied information. For example, the term *domain* is used as a placeholder for the actual domain name in the user's environment. When two such placeholders are used together, they may be set apart with angle brackets. For example, the path <*PS_CFG_HOME*>/appserv/<*domain*> includes two placeholders that require user-supplied information.
Initial Caps	Field names, commands, and processes are represented as they appear on the window, menu, or page.
lower case	File or directory names are represented in lower case, unless they appear otherwise on the interface.
Menu, Page	A comma (,) between menu and page references indicates that the page exists on the menu. For example, "Select Use, Process Definitions" indicates that you can select the Process Definitions page from the Use menu.
Cross-references	Cross-references that begin with *See* refer you to additional documentation that will help you implement the task at hand. We highly recommend that you reference this documentation. Cross-references under the heading *See Also* refer you to additional documentation that has more information regarding the subject.
⇒ (line-continuation arrow)	A line-continuation arrow inserted at the end of a line of code indicates that the line of code has been wrapped at the page margin. The code should be viewed or entered as a continuous line of code, without the line-continuation arrow.
" " (quotation marks)	Indicate chapter titles in cross-references and words that are used differently from their intended meaning.
Note. Note text.	Text that begins with *Note.* indicates information that you should pay particular attention to as you work with your PeopleSoft system.
Important! Important note text.	A note that begins with *Important!* is crucial and includes information about what you need to do for the system to function properly.

Convention	Description
Warning! Warning text.	A note that begins with *Warning!* contains critical configuration information or implementation considerations; for example, if there is a chance of losing or corrupting data. Pay close attention to warning messages.

Products

This documentation may refer to these products and product families:

- Oracle® Database
- Oracle® Enterprise Manager
- Oracle® Tuxedo
- Oracle VM VirtualBox®
- Oracle® WebLogic Server
- Oracle's PeopleSoft Application Designer
- Oracle's PeopleSoft Customer Relationship Management (CRM)
- Oracle's PeopleSoft Enterprise Learning Management (ELM)
- Oracle's PeopleSoft Financial Management (part of FSCM)
- Oracle's PeopleSoft Human Capital Management (HCM)
- Oracle's PeopleSoft Interaction Hub
- Oracle's PeopleSoft PeopleTools
- Oracle's PeopleSoft Process Scheduler
- Oracle's PeopleSoft Supply Chain Management (part of FSCM)
- Oracle® Secure Enterprise Search

See http://www.oracle.com/applications/peoplesoft-enterprise.html for a list of Oracle's PeopleSoft products.

Related Information

You can find several sources of reference information about PeopleSoft PeopleTools and your particular PeopleSoft application. You can access the current release of online help for PeopleSoft PeopleTools and PeopleSoft applications at the PeopleSoft Online Help site (formerly Hosted PeopleBooks). You can also find installation guides and other information by searching for the product name and release number on My Oracle Support.

- PeopleSoft Deployment Packages for Update Images Installation (PeopleSoft PeopleTools 8.55).

  See PeopleSoft Update Images Home Page, My Oracle Support, Doc ID 1641843.2.
- PeopleSoft PeopleTools 8.55 Deployment Packages Installation. This document includes advanced information for using the PeopleSoft deployment packages.

  See PeopleSoft PeopleTools Patches Home Page, My Oracle Support, Doc ID 2062712.2.
- Oracle PeopleSoft Online Help. This page includes links to the most recent documentation for PeopleSoft

PeopleTools and PeopleSoft applications.

See Oracle PeopleSoft Online Help, http://www.peoplesoftonlinehelp.com.

- PeopleTools: Getting Started with PeopleTools for your release. This documentation provides a high-level introduction to PeopleTools technology and usage.

  See Oracle PeopleSoft Online Help, http://www.peoplesoftonlinehelp.com.

- My Oracle Support. This support platform requires a user account to log in. Contact your PeopleSoft representative for information.

  To locate documentation on My Oracle Support, search for the title and select PeopleSoft Enterprise to refine the search results.

  See My Oracle Support, https://support.oracle.com.

- PeopleTools Installation for your database platform for the current release. This documentation provides instructions for installing PeopleSoft PeopleTools using the traditional method.

  See My Oracle Support, (search for title).

- Installation guide for your PeopleSoft application. Search My Oracle Support for the application-specific installation instructions.

- PeopleSoft Application Fundamentals for your PeopleSoft application and release. This documentation provides essential information about the setup, design, and implementation of your PeopleSoft application.

  See Oracle PeopleSoft Online Help, http://www.peoplesoftonlinehelp.com.

- PeopleTools Mid-Tier Deployment Best Practices. This white paper explains the PeopleSoft Homes (for example *PS_APP_HOME*) introduced since the PeopleSoft PeopleTools 8.50 release.

  See PeopleTools Mid-Tier Deployment Best Practices, My Oracle Support, Doc ID 1448479.1.

For information on Oracle Secure Enterprise Search (SES), see the following documentation:

See Oracle Secure Enterprise Search Documentation 11g Release 2 (11.2.2.2), http://docs.oracle.com/cd/E35215_01/index.htm.

- Oracle Secure Enterprise Search Administrator's Guide
- Oracle Secure Enterprise Search Installation and Upgrade Guide for Linux x86 (64-Bit)

Comments and Suggestions

Your comments are important to us. We encourage you to tell us what you like, or what you would like changed about our documentation, PeopleSoft Online Help, and other Oracle reference and training materials. Please send your suggestions to:

PSOFT-Infodev_US@oracle.com

While we cannot guarantee to answer every email message, we will pay careful attention to your comments and suggestions. We are always improving our product communications for you.

Chapter 1

Preparing to Deploy

This chapter discusses:

- Understanding the PeopleSoft Deployment Framework
- Understanding PeopleSoft Components
- Understanding Oracle VM VirtualBox
- Understanding Puppet and the PeopleSoft Puppet Modules
- Reviewing the Deployment Packages
- Setting the Network Configuration for a VirtualBox Deployment
- Completing the PeopleSoft Application-Specific Installation

Understanding the PeopleSoft Deployment Framework

In PeopleSoft PeopleTools 8.55, the installation of the PeopleSoft Update Images takes advantage of PeopleSoft Deployment Packages (DPKs). The DPKs can be installed on Oracle VirtualBox, as in previous releases. In addition, the PeopleSoft DPKs include an interactive setup script that allows for fast deployment on physical or virtual Oracle Linux, Red Hat Enterprise Linux, and Microsoft Windows operating system platforms.

Understanding PeopleSoft Components

Here are brief descriptions of some of the terms referenced in this documentation for components included in a PeopleSoft environment. The components included for each deployment depend upon the types of DPKs downloaded and method used to deploy them. PeopleSoft components, including PeopleSoft Pure Internet Architecture (PIA), application server and Process Scheduler, are described in the PeopleSoft PeopleTools product documentation.

See the PeopleTools System and Server Administration product documentation for an explanation of PeopleSoft architecture fundamentals.

- PeopleSoft Pure Internet Architecture (PIA)

  This is the Web Server component of the PeopleSoft system.

- Application server and Process Scheduler

  The application server acts as the business logic engine of the PeopleSoft system. 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.

- PeopleSoft application database

  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.

- Db-tier components

  This documentation uses the term "db-tier" to refer to Oracle database server, Oracle database client, and PeopleSoft application database.

- Mid-tier components

  This documentation uses the term "mid-tier" to refer to PeopleSoft Application Server, Process Scheduler, and PIA, and the software required to deploy them, including Oracle Tuxedo and Oracle WebLogic.

- Full tier components

  This document uses the term "full tier" to refer to a complete PeopleSoft environment. This includes the Oracle database server and PeopleSoft application database along with the application server, Process Scheduler, and PIA.

- AppBatch components

  This documentation uses the term "AppBatch" to refer to the Application Server and Process Scheduler server.

Understanding Oracle VM VirtualBox

When deploying the PeopleSoft application DPKs, you have the option of using Oracle VM VirtualBox. Oracle VM VirtualBox is a virtualization product from Oracle that allows one or more guest operating systems (OSs) to be run on and in a single host OS.

VirtualBox is intended to host applications with only a very small number of users. VirtualBox is a machine-bound solution—it runs on a single host. Therefore, PeopleSoft VirtualBox appliances as delivered are intended for demonstration or evaluation purposes. They are not intended to be used for a large number of users or for remote access. A typical PeopleSoft application will be secured by the administrator before being made available to the user population. Furthermore, a PeopleSoft deployment typically makes considerations for scalability and fault tolerance. The PeopleSoft VirtualBox appliances, as delivered, have not been constructed to meet these requirements. If the decision is made to make the virtual appliance available to a larger user population, the administrator should take steps to implement the necessary security requirements.

See Oracle VM VirtualBox Web site, https://www.virtualbox.org.

See *Oracle VM VirtualBox® User Manual,* Oracle Technology Network, http://www.oracle.com/technetwork/server-storage/virtualbox/documentation/index.html.

Understanding Puppet and the PeopleSoft Puppet Modules

The DPKs are delivered with the PeopleSoft Puppet modules, which are initialization and management scripts based upon the open-source Puppet software. The PeopleSoft Puppet modules can be used to customize and control the PeopleSoft environments deployed from the DPKs. For detailed information, see the documentation on the Puppet Labs Web site.

See Puppet Labs Documentation, http://docs.puppetlabs.com.

The PeopleSoft DPKs use Puppet to automate the process of deploying and configuring a PeopleSoft environment. Oracle has created custom modules and types to deploy and configure a PeopleSoft environment, which can be used to customize the DPK deployment. Customization examples and instructions are described in the PeopleSoft PeopleTools product documentation.

See *PeopleSoft PeopleTools 8.55 Deployment Packages Installation,* PeopleSoft PeopleTools Patches Home Page, My Oracle Support, Doc ID 2062712.2.

Task 1-1: Reviewing the Deployment Packages

This section discusses:

- Understanding the Downloaded Zip Files
- Using the DPK Manifests
- Reviewing the DPK Setup Zip File
- Reviewing the VirtualBox Shell File
- Reviewing the PeopleSoft PeopleTools Deployment Package
- Reviewing the PeopleSoft PeopleTools Client Deployment Package
- Reviewing the PeopleSoft Application Deployment Package
- Reviewing the Oracle Database Server Deployment Package
- Reviewing the Oracle Secure Enterprise Search Deployment

Understanding the Downloaded Zip Files

The DPK zip files that you download for either PeopleSoft PeopleTools or PeopleSoft applications include a variety of DPKs. This section describes the various DPKs you obtain. The downloaded DPK zip files contain all of the DPKs that are required for each specific type of deployment.

See PeopleSoft Deployment Packages for Update Images Installation (PeopleSoft PeopleTools 8.55) for the instructions for obtaining and using the zip files.

Task 1-1-1: Using the DPK Manifests

Each PeopleSoft DPK includes a manifest that lists the software versions included in the DPK. Review the manifests and compare the software with your current environment. Use this comparison to decide which of the zip files to download to set up a PeopleSoft environment.

Task 1-1-2: Reviewing the DPK Setup Zip File

The first zip file that you download will include scripts that you can use to automate the deployment process.

See the sections on using the PeopleSoft DPK setup script in PeopleSoft Deployment Packages for Update Images Installation (PeopleSoft PeopleTools 8.55).

In addition to the files that are described in this documentation for deployment, the DPK setup zip file also includes several files and folders that are used for deployment of PeopleSoft systems to Oracle Compute Cloud Service.

See Oracle Help Center, http://docs.oracle.com/cloud/latest/.

Task 1-1-3: Reviewing the VirtualBox Shell File

The VirtualBox shell file is an OVA file that you import into Oracle VM VirtualBox to create a virtual machine (VM) with an Oracle Linux operating system. The VirtualBox shell file is included with the Virtual Box DPKs.

Task 1-1-4: Reviewing the PeopleSoft PeopleTools Deployment Package

The PeopleSoft PeopleTools DPKs include the following features:

- PeopleSoft PeopleTools installation directory *(PS_HOME)*
- Oracle WebLogic Web server
- Oracle Tuxedo
- Oracle RDBMS client software
- Puppet modules for PeopleSoft PeopleTools and Hiera data
- Python initialization scripts
- Readme file
- Manifest

Task 1-1-5: Reviewing the PeopleSoft PeopleTools Client Deployment Package

The PeopleSoft PeopleTools Client DPKs include instances of each of the following features for the currently available releases:

- PeopleSoft Application Designer
- PeopleSoft Change Assistant
- PeopleSoft Configuration Manager
- PeopleSoft Test Framework
- Python initialization scripts
- Readme file
- Manifest

Task 1-1-6: Reviewing the PeopleSoft Application Deployment Package

The PeopleSoft application DPKs include the following features:

- PeopleSoft application installation directory *(PS_APP_HOME)*
- PeopleSoft Update Manager data files *(PI_HOME)*
- Application database (Oracle pluggable database)
- Puppet modules for PeopleSoft application and Hiera data
- Python initialization scripts
- Readme file
- Manifest

Task 1-1-7: Reviewing the Oracle Database Server Deployment Package

The Oracle Database Server (ODS) DPK includes the following features:

- Oracle database server
- Readme file
- Manifest

Task 1-1-8: Reviewing the Oracle Secure Enterprise Search Deployment

The Oracle Secure Enterprise Search (SES) includes multiple files that are combined to create a single VMDK. The VMDK can be used with VirtualBox to set up Oracle SES for the PeopleSoft Search Framework.

Note. The Oracle SES VMDK can only be used with VirtualBox.

See *PeopleSoft Deployment Packages for Update Images Installation (PeopleSoft PeopleTools 8.55)*.

Task 1-2: Setting the Network Configuration for a VirtualBox Deployment

This section discusses:

- Understanding Network Configuration Settings
- Setting a Host-Only Network Configuration
- Using Alternative Network Configurations

Understanding Network Configuration Settings

This section briefly describes the network configuration settings that you can use with the VirtualBox DPK. When you deploy the VirtualBox DPK, you have the option to select either host-only or bridged adapter configuration.

See Oracle VM VirtualBox Users Manual for more information about the VirtualBox network configuration, http://virtualbox.oracle.com.

A host-only adapter network configuration means:

- The virtual machine will be used in a machine-bound deployment.

  Select the host-only configuration if your environment will not need access to networked resources outside the host. This means that the virtual machine will only be used for single user or demonstration purposes and will be accessed only by users logged on to the host OS.
- Everything required of the runtime environment is contained within the virtual appliance.
- During the deployment process, a dynamic IP address is assigned to the virtual machine.

A bridged adapter network adapter means:

- The virtual machine will be able to operate in a wider network.
- If you choose to use a bridged adapter network configuration, you must provide a static IP address, DNS server IP address, gateway, and netmask during the deployment process.

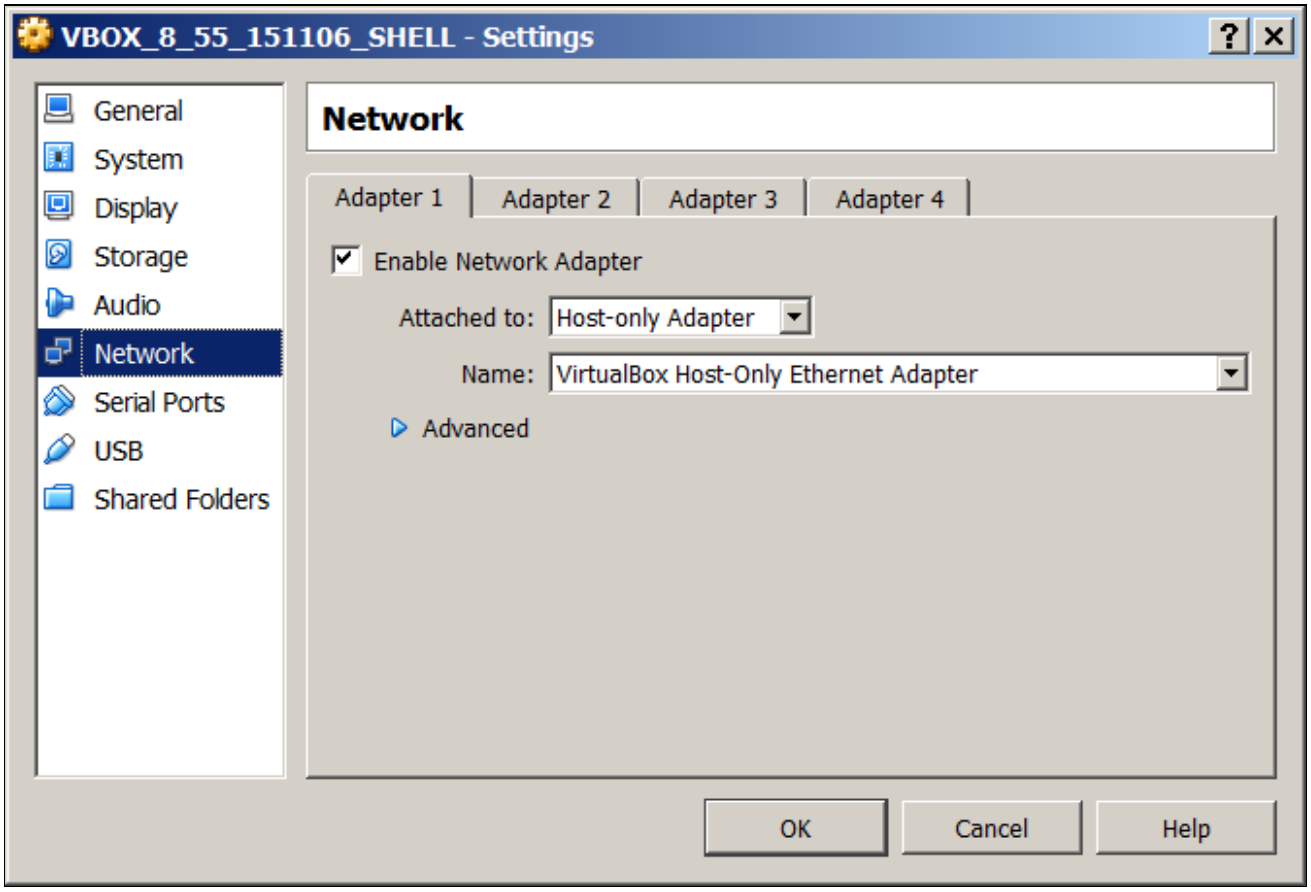
Oracle strongly recommends that the IP address of the VirtualBox host and the IP address of the guest be within the same subnet. Otherwise, customers will need to have their own networking experts verify that everything is set up properly, such that all virtual machines can see other machines as needed. Oracle Support will not assist customers directly with the actual network configuration of machines on different subnets.

Task 1-2-1: Setting a Host-Only Network Configuration

This procedure assumes that you have installed Oracle VM VirtualBox and imported the VirtualBox shell.

To set the network configuration for a host-only configuration:

1. In the Oracle VM VirtualBox Manager, highlight the virtual appliance and click Settings in the menu bar.
2. On the Settings window, select Network in the left-hand frame.
3. Select *Host-only Adapter* from the Attached to drop-down list, as shown in this example.



VirtualBox Manager Settings window: Network page with Host-only Adapter selected

---

Note. Setting the adapter to being Host-only means that the virtual machine will be unable to access the network outside the host on which it will run. The IP and hostname of the virtual machine will be known only within the host and virtual machine OS. During the time that the virtual machine is connected to the Host-only network consider performing any security configuration you need.

Task 1-2-2: Using Alternative Network Configurations

This section discusses:

- Understanding Alternative Network Configurations
- Allowing Your VM to Access the External Network
- Accessing VirtualBox and Your VM from Another Host
- Using the Virtual Machine with VPN
- Using the Virtual Machine Hostname from the Host OS

Understanding Alternative Network Configurations

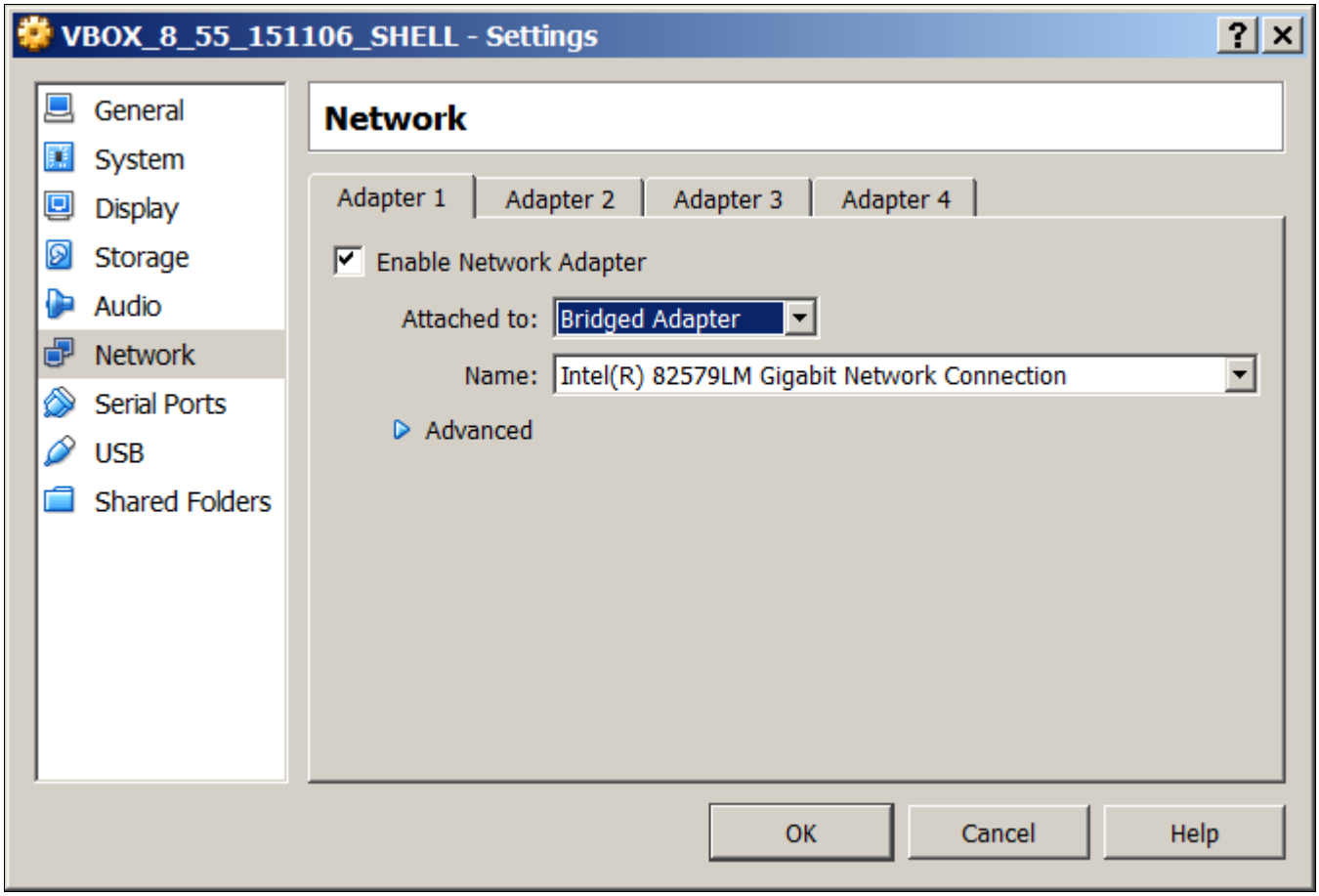
Oracle VM VirtualBox provides a rich set of network configuration options for your virtual machines (VMs). This will allow the virtual machine to function within your network in the same way as any other physical or virtual host. This topic is described in detail in the Oracle VM VirtualBox User Manual. Topics such as bridging, virtual LANs, dynamic and static IP address assignment are not described in this document. These concepts correlate to general network administrator activities and therefore are not discussed here.

Some of the scenarios with which you may wish to extend your virtual appliance are described here.

Allowing Your VM to Access the External Network

This is possible if your virtual machine has a network configuration that allows it to participate in the wider network. The default instructions in the previous section, Setting a Host-Only Network Configuration, permit the virtual machine to only run within the host machine. In order for the VM to operate in the wider network it is necessary to use one of the other network configuration options offered by VirtualBox. The most common choice is to use a bridged network adapter.

To use a bridged adapter rather than a host-only adapter, access the Network page in the Settings dialog box, as described in Setting a Host-Only Network Configuration, and select Bridged Adapter from the Attached to drop-down list, as shown in this example.



VirtualBox Manager Settings window: Network page with Bridged Adapter selected

After you choose the Bridged Adapter option, you will select the correct adapter with which to connect to the network. On a single user system such as a laptop this will typically correspond to the wireless network card. If multiple adapters are listed you should consult the Microsoft Windows Control Panel to identify which network adapter to use.

Accessing VirtualBox and Your VM from Another Host

VirtualBox is not intended for use as a server product, or for multi-user access. However, it is in fact possible to access the virtual machine from outside the host on which it runs. In such a case the network configuration of the virtual machine will need to be initialized with settings that are understood by the network in which it will run. The virtual machine will be subject to any rules imposed upon conventional hosts residing on the network. This means that a valid hostname, and IP address if using static IP, will be required.

To allow multiple users to access the VM, you must change the network adapter from Host-Only to Bridged Adapter. The procedure that you follow depends upon where you are in the deployment process.

If you have just imported the VirtualBox appliance, carry out these steps:

1. In the Oracle VM Virtual Box Manager, highlight the virtual appliance and click Settings in the menu bar.
2. On the Settings window, select Network in the left-hand frame.

The Network page includes four tabs in the right-hand frame, one for each of the network adapters.

3. On the Adapter 1 tab, select *Bridged Adapter* in the Attached to drop-down list.
4. Verify that the Name drop-down list is populated with the correct network adapter.

   This will typically be the wireless or wired network adapter that is on the host computer. This can be found, for example, by examining the network configuration in the Microsoft Windows Control Panel.
5. Click OK and start the VM.

If you have already started the VM with the setting Host-Only Adapter, carry out these steps:

1. Open the VM console window and select the following command to stop the VM:

   ```
   Machine, ACPI Shutdown
   ```
2. In the Oracle VM Virtual Box Manager, highlight the virtual appliance and click Settings in the menu bar.
3. On the Settings window, select Network in the left-hand frame.

   The Network page includes four tabs in the right-hand frame, one for each of the network adapters.
4. On the Adapter 1 tab, select *Bridged Adapter* in the Attached to drop-down list.
5. Verify that the Name drop-down list is populated with the correct network adapter.

   This will typically be the wireless or wired network adapter that is on the host computer. This can be found, for example, by examining the network configuration in Microsoft Windows Control Panel.
6. Click OK and start the VM.
7. Update the hosts file on the host Microsoft Windows machine to reflect the new IP address of the VM.

Using the Virtual Machine with VPN

Your virtual machine may not work as expected if your host OS is connected to a private network using a Virtual Private Network (VPN). In particular, Application Designer, PuTTY or browser connections to PIA may fail. This is because communication to and from the virtual machine takes place through the VirtualBox Network Adapter. When a VPN connection is active, the host OS will route all network communication through the VPN network adapter. The reason that communications to and from the virtual machine will not work is that the VPN adapter does not recognize the private network that VirtualBox is using. Therefore communications from the browser, Application Designer and so forth, get stopped at the VPN adapter and do not get propagated to the virtual machine.

If you want to use VPN, you can investigate the following configurations. Set up the VPN on the host OS, and use NAT for the network adapter for the virtual machine. Alternatively, if you choose to set up the virtual machine with a bridged adapter, you need to locate a VPN client that is compatible with the Oracle Linux server.

For more information on working with VPN, consult the VirtualBox documentation.

See VirtualBox, https://www.virtualbox.org.

Using the Virtual Machine Hostname from the Host OS

If the hostname of your virtual machine is not known to the network on which your host OS is running, you will not be able to use it to access the virtual machine. Client connections such as those made by the browser to PIA will not be able to resolve the hostname.

To overcome this issue it is necessary to update the hosts file on the host OS. This file will be located in %SystemRoot%\System32\drivers\etc. The %SystemRoot% value by default maps to C:\Windows. The hosts file must be updated to contain a mapping from the virtual machine IP address to the hostname that it has been assigned. This will allow the network adapter on the host OS to route any network traffic directly to the virtual appliance.

Add an entry such as the following in order to use the virtual machine hostname rather than the IP address to establish connections:

```
192.168.1.103   hostname.example.com
```

Task 1-3: Completing the PeopleSoft Application-Specific Installation

It is possible to use the PeopleSoft application DPKs to set up a full PeopleSoft demo environment. In that case, after you complete the installation tasks for the PeopleSoft DPKs covered in this documentation, there may be additional installation and configuration steps that are specific to the PeopleSoft application you are installing. Be sure to obtain the installation documentation for your PeopleSoft application and complete any necessary tasks covered there. You can find the PeopleSoft application-specific installation guides by searching on My Oracle Support.

Note. This task is not necessary if you are deploying the PeopleSoft Update Image DPKs as a PUM source.

Chapter 2

Planning Security Administration

This chapter discusses:

- Understanding Virtual Machine Security Administration
- Considering Network Security
- Considering User Security
- Considering the Virtual Machine Guest Operating System Security
- Considering PeopleSoft Application Security and Client Access
- Summarizing Security Considerations

Understanding Virtual Machine Security Administration

This chapter presents topics for you to consider when planning to secure your PeopleSoft virtual machine (VM). This chapter is not intended to replace or supersede any of the concepts covered in the PeopleSoft PeopleTools Security Red Papers or other sources of corporate infrastructure hardening.

The extent to which your VM must be secured is decided by the way in which it will be used and by whom. The more exposure the VM receives, the more secure it must be.

This chapter does not discuss details concerning the physical security of the servers on which your virtual machines will run. This is because the physical and operational obligations will be unique to your situation and will be based on standards defined at your organization. By the time you are deploying virtual machines you will have implemented a security infrastructure within your data center. You will have secured your network and firewalls and other security infrastructure components at appropriate points.

This chapter therefore discusses the aspects that are specific to the PeopleSoft DPKs and the VM deployed from them. This section applies especially to the use of the VirtualBox DPKs or the Native OS for Linux DPKs when using a virtual operating system. The chapter sometimes uses the term "guest OS" to mean the VM OS (Oracle Linux in this case) installed on the host OS for the VirtualBox deployment, such as Microsoft Windows. Communication with the virtual machine and network-based access are subjects that are not included here; decisions concerning these subjects derive from standards and procedures defined at your organization.

See Also

Oracle VM User's Guide for Release 3.1.1

Oracle VM Security Guide for Release 3

PeopleTools: Security Administration

Securing Your PeopleSoft Application Environment, Oracle Technology Network, http://download.oracle.com/peopletools/documents/Securing_PSFT_App_Environment_May2010%20v4.pdf

Considering Network Security

The approach that you take towards network security will mirror existing guidelines you have in place for traditional non-virtual ("bare-metal") systems. The main distinction between network security for your virtual artifacts and bare-metal systems is that the OVM PeopleSoft templates do not contain a network configuration when shipped. The network configuration is assigned to the VMs when they are initialized from the OVM PeopleSoft templates. This means that prior to this initialization you should plan your network configuration and provide necessary access to the users of this system. The PeopleSoft Security Red Paper provides detailed information about how to plan your network configurations for a multi-tiered PeopleSoft deployment involving load balancers, proxy servers and the logical tiers of a PeopleSoft application including PeopleSoft Pure Internet Architecture (PIA), Application Server, Process Scheduler and Database.

See Securing Your PeopleSoft Application Environment, My Oracle Support, (search for the title).

Network services used for reaching the VM services such as Samba, NFS, SSH and so on are configured and sometimes enabled in the VM by default. You must inspect the default configuration of your VM. Use Linux utilities such as netstat and ps to report the services and ports that are open on the VM. Use this information to reconfigure the system services and other network security utilities such as iptables.

Considering User Security

A number of distinct and separate user accounts are used when interacting with the VM. These user accounts are as follows:

- Network users — Network users that access the virtual machine after it is started by using PIA, Application Designer, and so on.
- Application user accounts — User accounts contained in the PeopleSoft application database that are used to sign on to the PeopleSoft application.
- Guest OS user accounts — User accounts for signing on to the guest virtual machine. There are a number of default users in the virtual machine.

  See *PeopleSoft Deployment Packages for Update Images Installation (PeopleSoft PeopleTools 8.55)*, "Using and Maintaining the PeopleSoft Environment."

  It is important to understand the implications of the local user accounts. The availability of these accounts means that there is no domain authentication of user log in. Audit facilities that you employ for tracking user activity and access will not be available for the VM by default. You may wish to disable these accounts and replace them with network users. This will require consideration of the later section that describes the default users. The default configuration for PeopleSoft runtime components and installed software is reliant on these default users. Replacing these users with domain users will require you to map these user roles and responsibilities to the new users.

  For example, Oracle Tuxedo domains are tightly bound to the users with whom they were created. You must recreate the Oracle Tuxedo domains if they must be run as a different user account.
- Samba user accounts — User accounts for accessing a limited part of the file system of the VM from outside the virtual machine.

  See *PeopleSoft Deployment Packages for Update Images Installation (PeopleSoft PeopleTools 8.55)*, "Using and Maintaining the PeopleSoft Environment."

Each of these accounts has different activities or roles that can be associated with them. This partitioning of roles with different authentication mechanisms provides scope for a more secure deployment of the VM similar to a typical environment management strategy used in your data center.

For example, it is possible to manage the environment such that the owner of the VM is unable to log in to the virtual machine. This allows the system and database administrators of the virtual machine to be divided into separate groups.

The following table lists administrators and likely sample activities:

Administrator	Sample Activities and Permissions
Network administrator	• Administers network addresses and names • (Sys Admin) Manages the host on which the VM runs and creates the VM. • After initial configuration, cannot log in to guest OS
System administrator	• Applies security to the guest OS and PeopleSoft runtime environment • Shuts down non-essential services and configures firewall • Cannot log in to Oracle VM Manager and cannot control starting up and shutting down of the VM.
PeopleSoft runtime administrator	• Manages the PeopleSoft runtime components and local installed software. • This is a non-root user and cannot stop or start OS services, install system software, change kernel parameters, and so on. • Manages the three user accounts psadm1 and psadm3, which are installation administrators, and psadm2 which is the runtime administrator. See *PeopleSoft Deployment Packages for Update Images Installation (PeopleSoft PeopleTools 8.55)*, "Using and Maintaining the PeopleSoft Environment." **Note.** This role may in fact be broken into a number of users along the lines of the three separate user accounts. This separation has been skipped for the sake of simplicity in this example.
Database administrator (DBA)	• Manages the PeopleSoft application databases, availability and performance • Participates in creating new databases during upgrade
PeopleSoft administrator	Signs on to PeopleSoft Application (PIA and Application Designer) and manages users, groups and authorization.

Here is a possible scenario for the security administration provided by these four administrators:

1. The network administrator downloads the latest OVM PeopleSoft template to the physical machine on which the VM will run.

2. The network administrator verifies that the checksum for each template part matches the digest information available on the download page.
3. The network administrator imports the OVM PeopleSoft template using Oracle VM Manager.
4. The network administrator creates a VM from the imported OVM PeopleSoft template.

   In doing so she assigns resources such as RAM and vCPUs to the VM in addition to assigning virtual network configuration including the IP address allocation method—static or dynamic.
5. The network administrator starts the VM, notifies the System Administrator that the VM has been started, and provides the connectivity details.
6. The system administrator logs in to the VM and applies security to the guest OS; for example:
   - Firewall configuration
   - Disabling unnecessary services
   - Installing software packages with Yum

     See Applying Operating System Patches and Updates.
7. The system administrator provides temporary root access (or uses lroot or sudo) to PeopleSoft runtime administrator.

   Note. For information on using lroot or sudo, see Linux user documentation.
8. The database administrator provides connectivity information for the PeopleSoft database to which the VM will connect.
9. The PeopleSoft runtime administrator logs in to the VM and invokes the PeopleSoft configuration script.

   The startup procedure includes prompts for the user for which PeopleSoft components should be run on the VM, and the location of the PeopleSoft Application Home *(PS_APP_HOME).*
10. The PeopleSoft runtime administrator changes the passwords for each of the ordinary (non-root) user accounts in the VM.
11. After the PeopleSoft runtime administrator has completed setup of the on-host PeopleSoft components, the system administrator withdraws super-user access from the PeopleSoft runtime administrator.

    This may involve changing the root password or perhaps editing the sudoers file to withdraw privileges from the PeopleSoft runtime administrator.

    Note. The sudoers file is a Linux or UNIX file that defines execution privileges for users. For more information, see Linux user documentation.
12. If necessary, the PeopleSoft runtime administrator announces the availability of the VM to the broader end-user population.

    This may be unnecessary if the VM is joining an already running PeopleSoft application, for example where the VM has been added to support increased load or high availability.
13. The end users access the PeopleSoft application through the normal mechanisms of using PIA or Application Designer.

Considering the Virtual Machine Guest Operating System Security

This section discusses:

- Understanding the Virtual Machine Guest Operating System Security

- Applying Operating System Patches and Updates
- Checking for Critical Patch Updates
- Disabling Unnecessary Services

Understanding the Virtual Machine Guest Operating System Security

The OS packaged with the VirtualBox is delivered with limited security. The PeopleSoft installation is secure in terms of file system permissions. The OS users that are used to administer the PeopleSoft system are consistent with available recommended guidelines. As noted elsewhere, those users are local to the virtual machine and must have their passwords immediately changed upon initial deployment.

See PeopleTools Mid-Tier Deployment Best Practices, Oracle Technology Network, http://docs.oracle.com/cd/E29604_01/psft/html/docset.html.

Applying Operating System Patches and Updates

The PeopleSoft DPKs that are downloaded from My Oracle Support contain the most recent versions of PeopleSoft PeopleTools and additional component (third-party) products (for example, Oracle Tuxedo) required by the PeopleSoft application. You may need to apply updates to the VM operating system, Oracle Linux, to ensure that it has all the required patches and fixes to function correctly and securely.

It is highly recommended that you use the fixes and updates for Oracle Linux that are available from the Oracle Yum Public Repository (http://public-yum.oracle.com). These fixes can be accessed directly from your VM by configuring yum on your VM to connect directly to the repository. You will connect to the yum repository through a secure channel. If traffic to the public yum repository is required to flow through a corporate proxy, the yum process can be configured to honor those settings. An alternative to using the remote public repository is to create your own yum repository. The approach you take will derive from pre-existing security processes in place within your organization for patching operating systems.

Note. The Yum repository is not configured on the delivered PeopleSoft DPKs.

See the information on Yum in the Oracle Linux documentation.

See *Oracle Linux Administrator's Solutions Guide for Release 6,* Oracle Technology Network, http://www.oracle.com/technetwork/indexes/documentation/ol-1-1861776.html.

Your organization will have pre-existing guidelines and standards set forth for hardening the operating system prior to making any host accessible on your network. You should apply these same security guidelines for the guest OS of any virtual artifacts delivered by Oracle for PeopleSoft environments. Your security personnel should be familiar with published hardening and threat mitigation documentation, including the following from Oracle:

- Tips for Hardening an Oracle Linux Server

  Suggestions and techniques for hardening an Oracle Linux server.

  See Oracle Technology Network, http://www.oracle.com/technetwork/articles/servers-storage-admin/tips-harden-oracle-linux-1695888.html.

- Tips for Securing an Oracle Linux Environment

  An overview of the software, network, and system monitoring recommendations for maintaining a secure Oracle Linux environment, plus an overview of the tools to help you do it.

  See Oracle Technology Network, http://www.oracle.com/technetwork/articles/servers-storage-admin/secure-linux-env-1841089.html.

In addition, review the following Oracle resources for information on securing the machines running the PeopleSoft database:

- Oracle Database Security Guide 11g Release 1 (11.1)

  This guide describes how you can configure security for Oracle Database by using the default database features.

  See Oracle Database Documentation Library, http://docs.oracle.com/cd/B28359_01/network.111/b28531/toc.htm.

- Oracle Database 2 Day + Security Guide 11g Release 1 (11.1), "Securing the Network."

  This chapter explains how you can encrypt data as it travels through the network, and also provides guidelines that you can follow to secure the network connections for Oracle Database

  See Oracle Database Documentation Library, http://docs.oracle.com/cd/B28359_01/server.111/b28337/tdpsg_network_secure.htm.

- Series: Project Lockdown. A phased approach to securing your database infrastructure.

  This project is divided into four distinct phases, each of which are achievable and provide measurable improvements within a specific period of time: one day, one week, one month, and one quarter.

  See Oracle Technology Network, http://www.oracle.com/technetwork/articles/index-087388.html.

Checking for Critical Patch Updates

Critical Patch Updates (CPUs) are made available according to a published schedule. If CPUs have been released subsequent to the availability of the PeopleSoft DPKs, you may want to install these CPUs if your VM is available to an untrusted user population.

See Critical Patch Updates, Security Alerts and Third Party Bulletin, Oracle Technology Networks, http://www.oracle.com/technetwork/topics/security/alerts-086861.html.

You can also search for critical patches in My Oracle Support, Patches & Updates.

See My Oracle Support Patches and Updates for PeopleSoft Products, My Oracle Support, Document 1465172.1.

Disabling Unnecessary Services

At initialization the VM starts a number of services. These frequently run as background or daemon processes, and they may be owned by either root or regular users. These services are responsible for runtime management of the system. Some of these services may be deemed non-essential for the running of your VM.

You may wish to review the services that are running, for example with the following Linux command:

```
service --status-all
```

Decide from those running services which ones are non-essential and whether the essential ones are properly configured. Consult your organization security authorities to determine which services are either mandatory or prohibited.

Considering PeopleSoft Application Security and Client Access

This section discusses:

- Understanding PeopleSoft Application Security and Client Access
- Considering PeopleSoft Pure Internet Architecture Security
- Considering Security for Client Tools

- Considering SQL*Plus Security
- Considering Security for Samba and the VM File System
- Considering the VM Operating System and Secure Shell Access

Understanding PeopleSoft Application Security and Client Access

To effectively use the virtual machine you will need to make it available to users. This access may be direct where the users can communicate directly with the machine from their own machine. For example, this might be in a demo environment where a small and known population of functional users have the host name or IP address of the system to perform tasks such as logging in to PIA. More frequently however, the access will be indirect, where the user is not aware, and should not be aware, that the machine is accessing the VM. In such cases proxy servers and load balancers will be part of a larger system configuration that is employed to make the system opaque to the client with the exception of the specific channels, such as HTTPS, through which the communication is directed.

In the most secure deployment the only user that needs to access the VM is the logged-in user on the host OS. This is not expected to be sufficient in most cases and therefore access to the VM will need to be made available to the user population. The VM should be made only as accessible as it needs to be for the users to perform the required tasks. Each of the VM access channels is discussed below.

Considering PeopleSoft Pure Internet Architecture Security

By default, any user that can reach the VM over TCP/IP can access the PIA login page. The URL for accessing PIA is well-known and can be constructed if the host name of the VM is known. There are no security certificates with the delivered VM and all traffic is HTTP by default. Because these default characteristics mean that access to the virtual appliance is quite open by default, and because unencrypted HTTP can be observed on the network by anyone that is reading the network path between the user and PIA machine, unless there is a security infrastructure including the use of SSL on front of the PIA domains, HTTP should be disabled and only HTTPS should be used.

For information on setting up SSL for PeopleSoft PeopleTools, see the *PeopleTools: Security Administration* product documentation.

For an example of steps that can be taken to lock down PIA and other components, see Reviewing a Sample Scenario later in this chapter.

Considering Security for Client Tools

Understanding Client Tools

PeopleSoft PeopleTools, including Application Designer (PSIDE) and PeopleSoft Change Assistant, are client tools that can run on only a Microsoft Windows machine, which can be the host OS or a remote workstation that has network access to the virtual machine. Alternatively the PeopleTools client installation can be placed on a shared (or mapped) drive that multiple users can access in read-execute mode. The installer for these Microsoft Windows-based client tools is contained within the VM and is exposed through a Samba share. Note that the Samba service is delivered disabled by default.

The administrator should access the installation program for the client tools from the VM to a shared location in order to make it available to users. See the documentation on Samba shares for more information about how to manage access to the shared folders. After the client installation has been deployed from the VM it is no longer necessary to expose the VM file system to clients.

See *PeopleSoft Deployment Packages for Update Images Installation (PeopleSoft PeopleTools 8.55),* "Deploying the PeopleSoft Application Deployment Packages."

Considering Application Designer Security

Application Designer is not needed for feature demonstration or evaluation purposes; it is used for development or debugging purposes. The Workstation Listener (WSL) port (7000) on the Application Server domain for Application Designer connectivity is disabled in the delivered PeopleSoft DPK. This port should be enabled if Application Designer is needed.

Note. If you choose to set up your environment without an Application Home *(PS_APP_HOME),* the WSL port is enabled by default.

See the information on Workstation Listener options in the *PeopleTools: System and Server Administration* product documentation.

Considering SQL*Plus Security

Oracle SQL*Plus is a client tool that allows direct access to the database tables. It can be used by a super-user to manipulate application data, and a database administrator can use it manipulate the database itself. Obviously, this level of access should only be afforded to the most trusted users and DBAs.

The connectivity information for the PeopleSoft application database is available in the VM file system when the Samba service is enabled and the file system is accessed. This connectivity information is available in the form of a tnsnames.ora file that provides the service name and listening port for the database. This can be seen by any user that can log in to the virtual machine over SSH or remotely access the file system of the VM. With this information it is necessary to supply the required credentials to connect to the database with SQL*Plus.

Your environment will include a database created separately from the VM. Nevertheless, as a general rule for database security, access to the database should be disabled for user accounts that do not require direct database access. Passwords for legitimate users should be changed from the default values that are contained in the delivered virtual appliance. Most importantly the administrator must change the password for the SYSADM user immediately after VM startup. The DBA will be familiar with which parts of the PeopleSoft database tablespace must be secured including user accounts and passwords.

Network security can also be employed to turn off remote access in the database service. As noted earlier in this section, the firewall can be configured to only allow connections to the database service listener port from specific clients.

See Also

*SQL*Plus User's Guide and Reference,* Oracle Technology Network, Oracle Database Documentation Library

Considering Security for Samba and the VM File System

The Samba configuration allows users outside the guest OS to access the file system that is internal to the VM. Only a limited part of the file system is exposed, mostly for access to the client installation programs required for PeopleSoft application development and customization. The client installations programs can be copied and relocated.

The Samba service is delivered disabled, and Samba is not required for ongoing use of the virtual machine after initial setup. After the required file systems are used, the Samba service should be disabled. This will further prevent unauthorized users accessing the VM file system. Use this command to disable the Samba service:


```
chkconfig smb off
```

See *PeopleSoft Deployment Packages for Update Images Installation (PeopleSoft PeopleTools 8.55),* "Deploying the PeopleSoft Application Deployment Packages."

Considering the VM Operating System and Secure Shell Access

Remote users (that is, users outside the host OS) can only sign on to the virtual machine using Secure Shell (SSH). All of the default users in the virtual machine must therefore have their passwords changed or invalidated immediately after initial startup.

SSH uses public-private key pairs to authenticate users and restrict access to the machine. The approaches provided in the virtual machine are the same as those used for conventional Linux systems.

See the documentation for your SSH client for more information.

Summarizing Security Considerations

This section discusses:

- Deciding on Security Plans
- Reviewing a Sample Scenario

Deciding on Security Plans

This section includes samples of questions related to security considerations. Use these questions to help you decide the level of security to be applied to your virtual machine:

1. *Question:* Do you have the required hardware available to run the virtual machine?

   Implication: You may have to procure new hardware that is an exception to the current hardware in place.

2. *Question:* Does the hardware on which you will run the virtual machine require an exception to the existing organizational standards?

   Implication: You will have to work with your security and network administration team.

3. *Question:* Do you have organizational processes and standards in place for assessment or auditing of new hosts on the network?

   Implication: You will have to work with your security and network administration team to verify that the VM is permitted to join the corporate network. In addition, consider the use of security scan and analysis tools to help you determine compliance with organizational standards.

4. *Question:* Will multiple users require access to the VM without connection through a proxy or firewall?

   Implication: If multiple users require access to the VM it will be necessary to apply network, VM and application security, as discussed earlier in this chapter.

5. *Question:* Will the VM be hosted in a LAN sub-domain that can only be accessed by the authorized domain users?

   Implication: If not, and if the unauthorized users have a network path to the VM, additional on-host security will need to be applied to prevent access to the VM.

6. *Question:* What is your time line for retaining the VM?

   Implication: If you download new templates from My Oracle Support frequently, you can take advantage of updated patches and so on. For long-term use, you must consider activities associated with ongoing

maintenance of the VM such as OS and PeopleSoft application software patching, password expiration, and so on.

Reviewing a Sample Scenario

Here is a suggested list of steps that an administrator might carry out to secure the system:

1. Review the existing operational guidelines for your organization for adding machines, web servers, AppBatch domains and so on to the network.
2. Update account and authentication settings, by changing default passwords; for example:
   - Change the OS passwords for the non-root users.

     If any of the users are not required they can be disabled completely.

     See *PeopleSoft Deployment Packages for Update Images Installation (PeopleSoft PeopleTools 8.55),* "Using and Maintaining the PeopleSoft Environment."
   - Change the default Oracle WebLogic password of PSKEY.

     See *PeopleTools: System and Server Administration,* "Implementing WebLogic SSL Keys and Certificates."
   - Change the domain connection password, used in the PIA to Application Server communication.

     See *PeopleTools: System and Server Administration,* "Configuring Domain Connection Password."
   - Disable unneeded user accounts in the PeopleSoft database.

     PeopleSoft databases contain a number of default users, such as VP1 or PS, with well-known passwords. These users are only needed as templates for creating users with specific roles, and after that is done, they should be removed or disabled. The needed accounts should have their passwords changed on first signon.

     See *PeopleTools: Security Administration,* "Purging Inactive User Profiles."
3. Configure iptables to restrict access to well-known ports, such as those listed here, to a restricted set of client IP addresses:

   See Considering Network Security.
   - Secure shell, SSH, Port 22
   - TNS listener, port 1521
   - Jolt listeners, ports 9000–9003
   - Workstation listeners, ports 7000–7003 (normally disabled by default but needed if Application Designer access is required)
4. Disable HTTP access in PIA.

   As noted earlier, HTTP is enabled by default in the virtual machine. Secure HTTP (HTTPS) should be used if the virtual machine is network accessible. This is to prevent eavesdropping on the network between the authorized user and the VM

   See *PeopleTools: Portal Technology,* "Configuring Web Profiles."
5. Obtain and install a valid security certificate from an approved certificate authority (CA).

   See *PeopleTools: Security Administration,* "Understanding SSL/TLS and Digital Certificates."

   See *PeopleTools: Integration Broker,* "Understanding Digital Certificates."
6. Enable encryption between PIA and Application Server domain.

   This is achieved by using the Custom Configuration menu for the Application Server domain. In the section for Workstation Listener options, set the value for Encryption to 128 bit.

See *PeopleTools: System and Server Administration*, "Workstation Listener Options."

7. Configure a forward proxy server if your VM allows communications with an untrusted network, such as communications over the internet.

Note. This is relevant for the next step for access to the yum repository on the internet.

---

8. Configure the yum repository to use the latest label from Oracle Linux.

   See Considering the Virtual Machine Guest Operating System Security.

9. Update all packages on the virtual appliance using yum update.
10. Disable any network services that are not needed.

    In particular the Samba service should be disabled as soon as it is no longer needed.

    See *PeopleSoft Deployment Packages for Update Images Installation (PeopleSoft PeopleTools 8.55)*, "Deploying the PeopleSoft Application Deployment Packages."

Appendix A

Reviewing Deployment Use Cases

This appendix discusses:

- Reviewing the PeopleSoft Update Image DPK Use Cases
- Reviewing the PeopleTools Client DPK Use Case
- Reviewing the Customization Use Cases

Task A-1: Reviewing the PeopleSoft Update Image DPK Use Cases

This section discusses:

- Understanding the PeopleSoft Update Image DPKs
- Reviewing the Native OS DPK Use Cases
- Reviewing the VirtualBox DPK Use Cases
- Setting the Network Configuration for a VirtualBox Deployment

Understanding the PeopleSoft Update Image DPKs

In previous releases, the PeopleSoft Update Images (PIs) were deployed on a Microsoft Windows host machine with Oracle VM VirtualBox. The current release of the PIs can also be deployed using Oracle VM VirtualBox to host the PeopleSoft DPKs. Alternatively, you can install and configure PeopleSoft environments on Microsoft Windows or Linux hardware or virtualization platforms using the DPKs.

The DPKs that are deployed using Oracle VM VirtualBox are referred to as "VirtualBox DPK," and those that are deployed directly onto Microsoft Windows and Linux operating systems are referred to as "Native OS DPK."

Task A-1-1: Reviewing the Native OS DPK Use Cases

This table lists possible deployment scenarios and operating systems (OS). The tasks listed in this table are found in *PeopleSoft Deployment Packages for Update Images Installation (PeopleSoft PeopleTools 8.55).*

Use Case	Operating System	Oracle SES Setup	Reference
PI with Native OS DPK	Linux (bare metal or virtual)	Oracle SES must be installed separately.	In the chapter "Deploying the PeopleSoft Application Deployment Packages": • Obtaining the PeopleSoft Update Images DPKs • Setting Up the PeopleSoft Virtual Machine on a Linux Host Using the PeopleSoft Application DPK Setup Script. • Deploying the PeopleTools Client in Update Manager Mode • Setting Up Oracle SES on a Microsoft Windows or Linux Host
PI with Native OS DPK	Microsoft Windows (bare metal or virtual)	Oracle SES must be installed separately.	In the chapter "Deploying the PeopleSoft Application Deployment Packages": • Obtaining the PeopleSoft Update Images DPKs • Setting Up the PeopleSoft Virtual Machine on a Microsoft Windows Host Using the PeopleSoft Application DPK Setup Script • Deploying the PeopleTools Client in Update Manager Mode • Setting Up Oracle SES on a Microsoft Windows or Linux Host

Task A-1-2: Reviewing the VirtualBox DPK Use Cases

If you choose to use VirtualBox, be aware of the following guidelines:

- If you installed Oracle VM VirtualBox on a Microsoft Windows host, you can deploy the Virtual Box DPKs either by importing the OVA shell directly into VirtualBox, or by using the delivered PeopleSoft application DPK setup script.

- If you choose to install Virtual Box on a different, non-Microsoft Windows operating system, you must import the OVA shell directly into Oracle VM Virtual using the documented procedure.

  See *PeopleSoft Deployment Packages for Update Images Installation (PeopleSoft PeopleTools 8.55)*, "Deploying the PeopleSoft Application Deployment Packages."

This table lists possible deployment scenarios for the supported operating systems (OSs). The tasks listed in this table are found in *PeopleSoft Deployment Packages for Update Images Installation (PeopleSoft PeopleTools 8.55)*.

Use Case	Operating System	Oracle SES Setup	Reference
PI with VirtualBox DPK — deploy the VirtualBox Shell using Oracle VirtualBox Manager.	Linux guest OS on Microsoft Windows or other OS host	The initialization process for the VirtualBox DPK will deploy Oracle SES. The instructions include manual steps to extract the downloaded Oracle SES file and create the VMDK file format needed for the process.	In the chapter "Deploying the PeopleSoft Application Deployment Packages": • Obtaining the PeopleSoft Update Images DPKs • Using the VirtualBox Shell to Set Up the PeopleSoft Virtual Machine • Deploying the PeopleTools Client in Update Manager Mode
PI with VirtualBox DPK — deploy using the PeopleSoft application DPK setup script.	Microsoft Windows host	The PeopleSoft application DPK setup script will set up Oracle SES.	In the chapter "Deploying the PeopleSoft Application Deployment Packages": • Obtaining the PeopleSoft Update Images DPKs • Setting Up the VirtualBox VM Using the PeopleSoft Application DPK Setup Script • Deploying the PeopleTools Client in Update Manager Mode

Task A-1-3: Setting the Network Configuration for a VirtualBox Deployment

This section discusses:

- Understanding VirtualBox Network Configuration Settings
- Setting a Host-Only Network Configuration
- Allowing Your VM to Access the External Network
- Accessing VirtualBox and Your VM from Another Host
- Using the Virtual Machine with VPN
- Using the Virtual Machine Hostname from the Host OS

Understanding VirtualBox Network Configuration Settings

This section briefly describes the network configuration settings that you can use with the VirtualBox DPKs. When you deploy the VirtualBox DPKs, you have the option to select either host-only or bridged adapter configuration.

See Oracle VM VirtualBox Users Manual for more information about VirtualBox network configurations, http://virtualbox.oracle.com.

A host-only adapter network configuration means:

- The virtual machine will be used in a machine-bound deployment. Select the host-only configuration if your environment will not need access to networked resources outside the host. This means that the virtual machine will only be used for single user or demonstration purposes and will be accessed only by users logged on to the host OS.
- Everything required of the runtime environment is contained within the virtual appliance.
- During the deployment process, a dynamic IP address is assigned to the virtual machine.

A bridged adapter network adapter means:

- The virtual machine will be able to operate in a wider network.
- If you choose to use a bridged adapter network configuration, you must provide a static IP address, DNS server IP address, gateway, and netmask during the deployment process

Oracle strongly recommends that the IP address of the VirtualBox host and the IP address of the guest be within the same subnet. Otherwise, customers will need to have their own networking experts verify that everything is set up properly, such that all virtual machines can see other machines as needed. Oracle Support will not assist customers directly with the actual network configuration of machines on different subnets.

Some of the scenarios with which you may wish to extend your virtual appliance are described in this section.

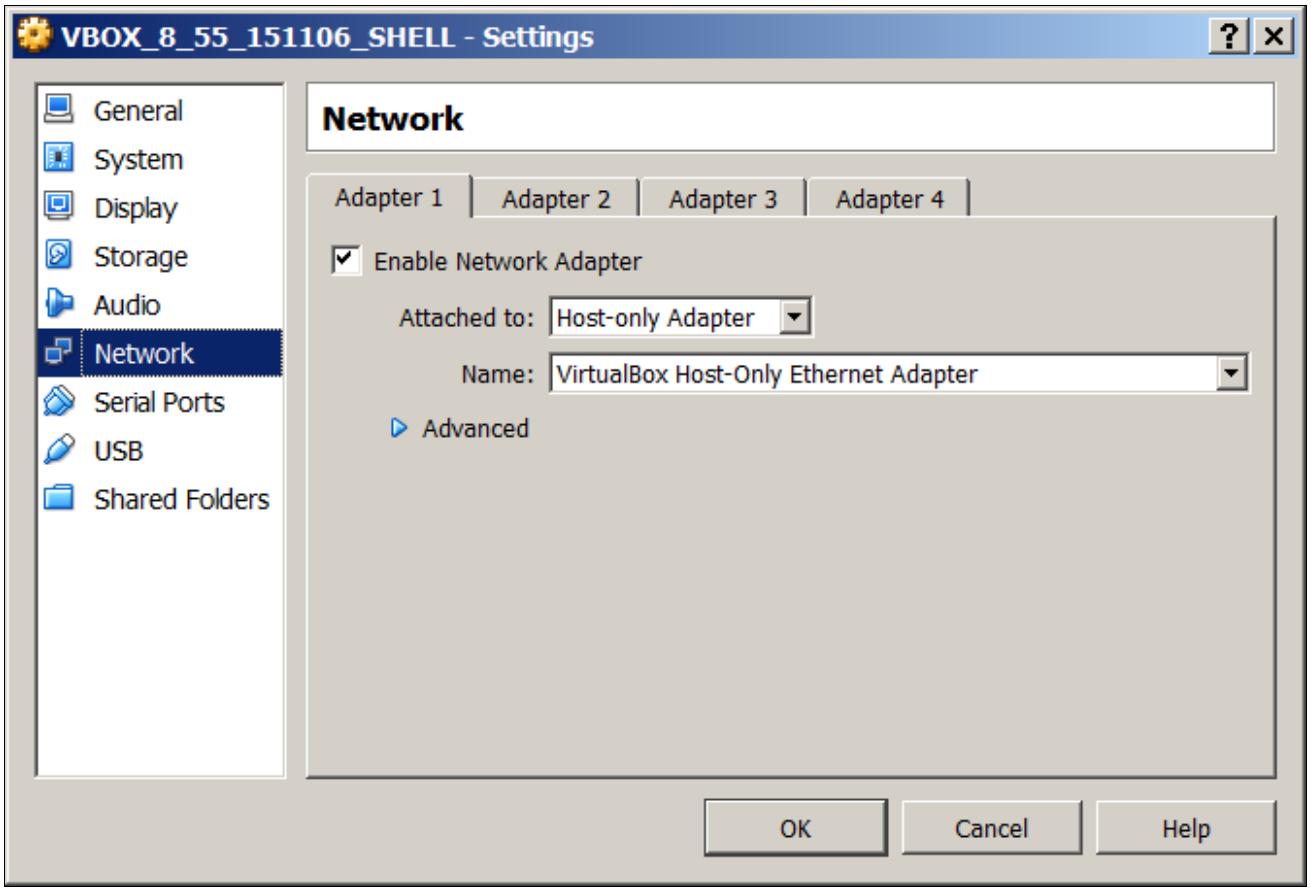
Setting a Host-Only Network Configuration

This procedure assumes that you have installed Oracle VM VirtualBox and imported the VirtualBox shell.

To set the network configuration for a host-only configuration:

1. In the Oracle VM VirtualBox Manager, highlight the virtual appliance and click Settings in the menu bar.
2. On the Settings window, select Network in the left-hand frame.

3. Select *Host-only Adapter* from the Attached to drop-down list, as shown in this example.



VirtualBox Manager Settings window: Network page with Host-only Adapter selected

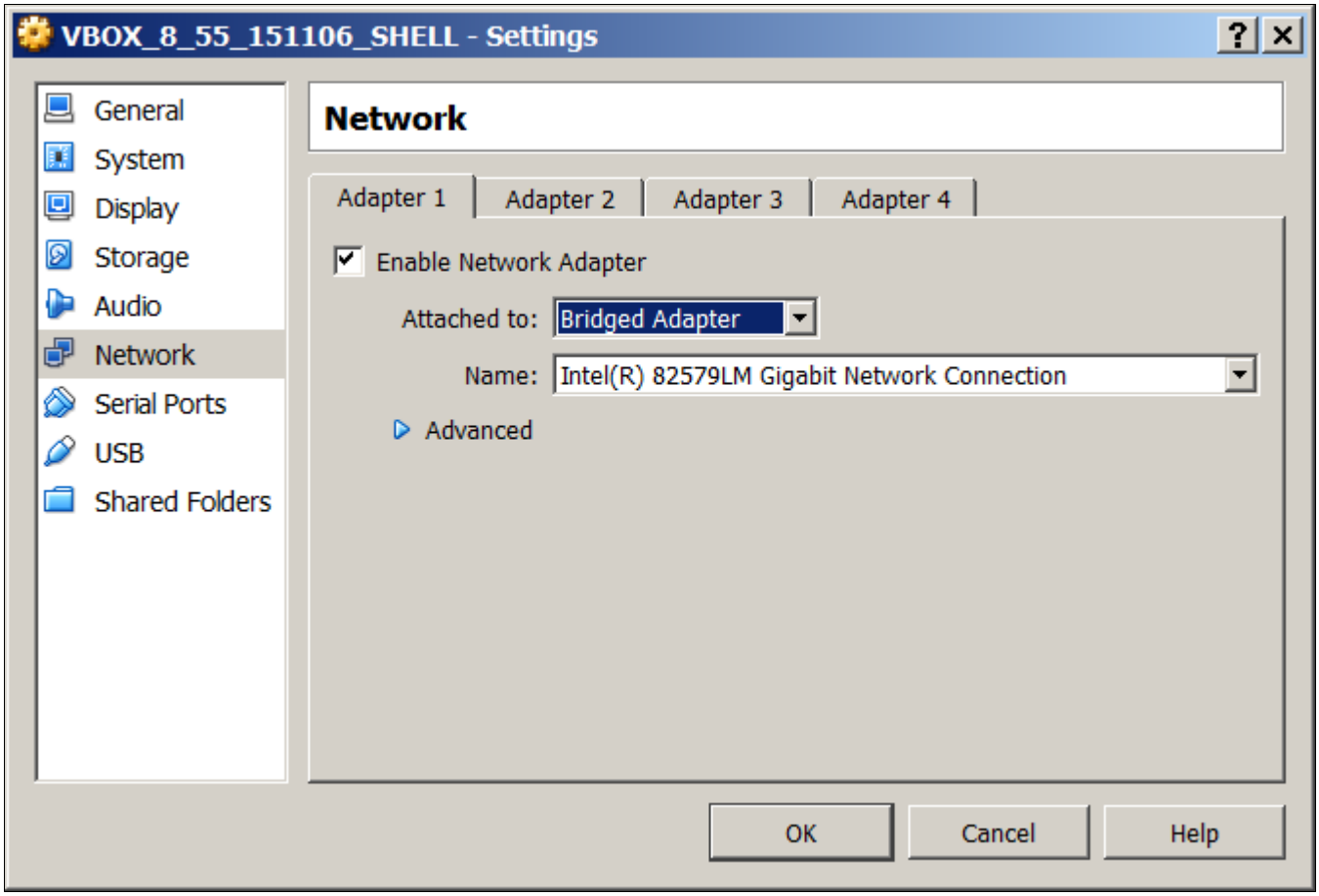
---

Note. Setting the adapter to being Host-only means that the virtual machine will be unable to access the network outside the host on which it will run. The IP and hostname of the virtual machine will be known only within the host and virtual machine OS. During the time that the virtual machine is connected to the Host-only network consider performing any security configuration you need.

Allowing Your VM to Access the External Network

This is possible if your virtual machine has a network configuration that allows it to participate in the wider network. The default instructions in the previous section, Setting a Host-Only Network Configuration, permit the virtual machine to only run within the host machine. In order for the VM to operate in the wider network it is necessary to use one of the other network configuration options offered by VirtualBox. The most common choice is to use a bridged network adapter.

To use a bridged adapter rather than a host-only adapter, access the Network page in the Settings dialog box, as described in Setting a Host-Only Network Configuration, and select Bridged Adapter from the Attached to drop-down list, as shown in this example.



VirtualBox Manager Settings window: Network page with Bridged Adapter selected

After you choose the Bridged Adapter option, you will select the correct adapter with which to connect to the network. On a single user system such as a laptop this will typically correspond to the wireless network card. If multiple adapters are listed you should consult the Microsoft Windows Control Panel to identify which network adapter to use.

Accessing VirtualBox and Your VM from Another Host

VirtualBox is not intended for use as a server product, or for multi-user access. However, it is in fact possible to access the virtual machine from outside the host on which it runs. In such a case the network configuration of the virtual machine will need to be initialized with settings that are understood by the network in which it will run. The virtual machine will be subject to any rules imposed upon conventional hosts residing on the network. This means that a valid hostname, and IP address if using static IP, will be required.

To allow multiple users to access the VM, you must change the network adapter from Host-Only to Bridged Adapter. The procedure that you follow depends upon where you are in the deployment process.

If you have just imported the VirtualBox appliance, carry out these steps:

1. In the Oracle VM Virtual Box Manager, highlight the virtual appliance and click Settings in the menu bar.
2. On the Settings window, select Network in the left-hand frame.

The Network page includes four tabs in the right-hand frame, one for each of the network adapters.

3. On the Adapter 1 tab, select *Bridged Adapter* in the Attached to drop-down list.
4. Verify that the Name drop-down list is populated with the correct network adapter.

   This will typically be the wireless or wired network adapter that is on the host computer. This can be found, for example, by examining the network configuration in the Microsoft Windows Control Panel.
5. Click OK and start the VM.

If you have already started the VM with the setting Host-Only Adapter, carry out these steps:

1. Open the VM console window and select the following command to stop the VM:

   ```
   Machine, ACPI Shutdown
   ```
2. In the Oracle VM Virtual Box Manager, highlight the virtual appliance and click Settings in the menu bar.
3. On the Settings window, select Network in the left-hand frame.

   The Network page includes four tabs in the right-hand frame, one for each of the network adapters.
4. On the Adapter 1 tab, select *Bridged Adapter* in the Attached to drop-down list.
5. Verify that the Name drop-down list is populated with the correct network adapter.

   This will typically be the wireless or wired network adapter that is on the host computer. This can be found, for example, by examining the network configuration in Microsoft Windows Control Panel.
6. Click OK and start the VM.
7. Update the hosts file on the host Microsoft Windows machine to reflect the new IP address of the VM.

Using the Virtual Machine with VPN

Your virtual machine may not work as expected if your host OS is connected to a private network using a Virtual Private Network (VPN). In particular, Application Designer, PuTTY or browser connections to PIA may fail. This is because communication to and from the virtual machine takes place through the VirtualBox Network Adapter. When a VPN connection is active, the host OS will route all network communication through the VPN network adapter. The reason that communications to and from the virtual machine will not work is that the VPN adapter does not recognize the private network that VirtualBox is using. Therefore communications from the browser, Application Designer and so forth, get stopped at the VPN adapter and do not get propagated to the virtual machine.

If you want to use VPN, you can investigate the following configurations. Set up the VPN on the host OS, and use NAT for the network adapter for the virtual machine. Alternatively, if you choose to set up the virtual machine with a bridged adapter, you need to locate a VPN client that is compatible with the Oracle Linux server.

For more information on working with VPN, consult the VirtualBox documentation.

See VirtualBox, https://www.virtualbox.org.

Using the Virtual Machine Hostname from the Host OS

If the hostname of your virtual machine is not known to the network on which your host OS is running, you will not be able to use it to access the virtual machine. Client connections such as those made by the browser to PIA will not be able to resolve the hostname.

To overcome this issue it is necessary to update the hosts file on the host OS. This file will be located in %SystemRoot%\System32\drivers\etc. The %SystemRoot% value by default maps to C:\Windows. The hosts file must be updated to contain a mapping from the virtual machine IP address to the hostname that it has been assigned. This will allow the network adapter on the host OS to route any network traffic directly to the virtual appliance.

Add an entry such as the following in order to use the virtual machine hostname rather than the IP address to establish connections:

```
192.168.1.103   hostname.example.com
```

Task A-2: Reviewing the PeopleTools Client DPK Use Case

The PeopleSoft application DPKs include DPKs for supported versions of the PeopleSoft PeopleTools Client. Deploy the PeopleTools Client DPK, for example, to install utilities such as Change Assistant or Application Designer to connect to an existing environment.

Deployment	Operating System	Reference
PeopleTools client DPKs	Microsoft Windows (physical hardware or virtual)	In the chapter "Deploying the PeopleSoft Application Deployment Packages" in this documentation: • Obtaining the PeopleSoft Update Image DPKs • Deploying the PeopleTools Client DPK in Update Manager Mode
PeopleTools VCDs	All other operating systems	PeopleTools installation guide for your database platform, on My Oracle Support

Task A-3: Reviewing the Customization Use Cases

You have the option to customize your environment using the Hiera data files that are provided as part of the Puppet implementation. The PeopleSoft PeopleTools documentation provides a few common examples, but there are a wide variety of ways to make use of the Hiera data files in customizing your environment.

See *PeopleSoft PeopleTools 8.55 Deployment Packages Installation,* "Customizing a PeopleSoft Environment."